

# Financial Intelligence: A Crucial Pillar of National Security

Kevin Hk Chow

Krieger School of Arts and Sciences, Johns Hopkins University, Baltimore, USA

Email: me@scirp.org

**How to cite this paper:** Chow, K. H. (2025). Financial Intelligence: A Crucial Pillar of National Security. *Modern Economy*, 16, 2032-2043. <https://doi.org/10.4236/me.2025.1612094>

**Received:** July 24, 2025

**Accepted:** December 22, 2025

**Published:** December 25, 2025

Copyright © 2025 by author(s) and Scientific Research Publishing Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

## Abstract

Financial Intelligence (FININT) serves as a critical interface between economic systems and national security efforts, focusing on issues such as money laundering and terrorism financing. Within the national security architecture, FININT capabilities are indispensable for safeguarding national sovereignty. Specifically, FININT methodologies are deployed to investigate and interdict illicit financial networks underpinning terrorism, money laundering operations, and other transnational criminal activities that pose a direct threat to our nation's security and stability. The objective of FININT is to protect national sovereignty by proactively detecting illicit financial activities from destabilizing the economy and endangering the security of the nation. By effectively disrupting these illicit financial activities, FININT contributes directly to the integrity of the financial system and safeguards the nation's stability. Within this framework, FININT is not merely a set of tools or processes for tracing illicit flows but a dynamic, adaptive network comprising interdependent nodes (financial institutions, intelligence agencies, regulatory bodies) that collectively build systemic resilience against financial threats.

## Keywords

Financial Intelligence, Law, National Security, Policy

## 1. Financial Intelligence and Resilience of Nation's Security

Financial Intelligence (FININT) serves as a fundamental component of the national security framework, acting as a key tool for identifying and dismantling illegal financial networks. Financial intelligence plays a pivotal role in national security by safeguarding sovereignty by uncovering and addressing threats that conventional military and law enforcement agencies might overlook. Unchecked illicit finance has the potential to disrupt financial markets, compromise a country's economic

stability, and undermine national security. By identifying, examining, and interrupting unlawful transactions, authorities are able to safeguard their financial systems against exploitation for purposes such as terrorism, proliferation, and organized crime, thus enhancing national security. Financial intelligence is crucial in the endeavor to safeguard national security.

Whereas Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) regimes primarily impose obligations on financial institutions—such as customer due diligence, suspicious transaction reporting, and record-keeping—FININT operates as an intelligence discipline rather than a compliance function. It integrates data derived from AML/CFT, such as suspicious activity reports and currency transaction reports, with both classified and open-source intelligence, which encompasses Signals Intelligence (SIGINT). This multi-source integration reveals concealed patterns, beneficial ownership structures, and emerging risks that traditional law enforcement processes alone cannot detect. By converting raw transactional data into actionable intelligence, the FININT approach functions as a protective measure, enabling authorities to oversee and disrupt illicit financial transactions.

## 2. Illicit Economies and National Security

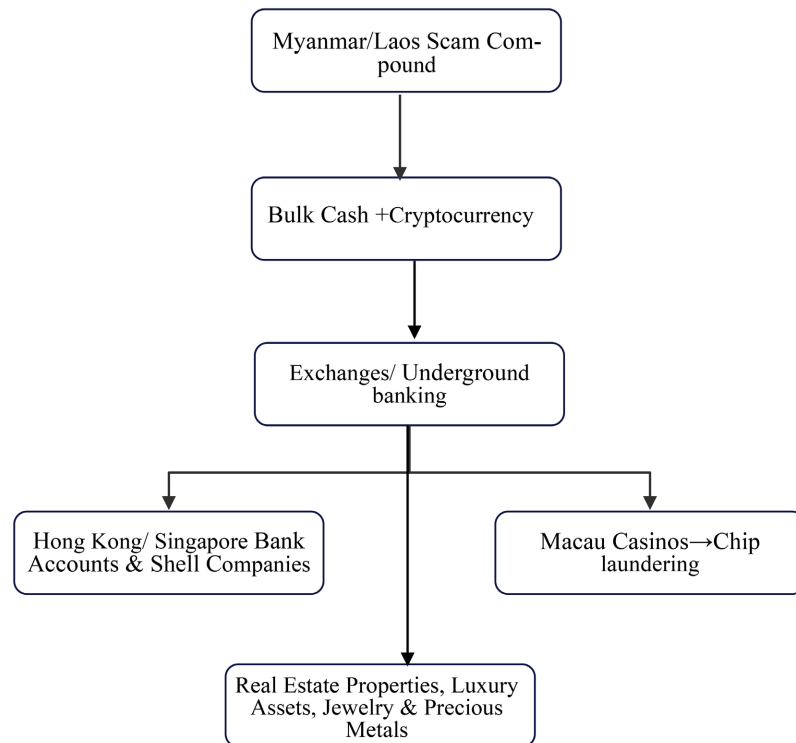
Illicit economies pose a profound threat to national security by eroding governance institutions, undermining the rule of law, and weakening state security apparatuses. Illicit economies, generated by criminal and terrorist organizations, pose a substantial threat to national security. These illegal financial flows undermine economic stability, fuel social unrest, and erode the integrity of financial systems. Over time, such financing has become the lifeblood of these groups, enabling their survival and expansion. Their deliberate diversification across a broadening spectrum of criminal enterprises. This strategic expansion of terrorist groups' illicit portfolios is one of the most dangerous developments in contemporary terrorism because it creates multiple, resilient revenue streams that are far harder for states to detect and disrupt (Shelley, 2020).

Criminal organizations operate a sophisticated, multi-layered funding architecture that combines revenue generation with resilient cross-border transfer and laundering mechanisms.

### 2.1. The Funding Architecture of Criminal Organizations

- **Cybercrime:** Cryptocurrency scams, ransomware operations, cybersecurity attacks, data breaches, darknet marketplaces
- **Drug trafficking:** Organized cartels, transnational drug trafficking operations, retail via darknet marketplaces
- **Human Exploitation Economies:** Human trafficking and migrant smuggling, forced labor and sexual exploitation networks.
- **Illegal Firearm trade:** Shell company procurement, exploitation of conflict zones, misdeclared shipments.

- **Trade-Based Money-Laundering Ecosystems:** Trade-based money laundering, Offshore shell entities and corporate vehicles for layering, Hawala, cryptocurrency exchange and other informal value transfer systems (**Figure 1**).



**Figure 1.** An example of Asia criminal organization structure—Myanmar/Laos Scam Compound.

**Figure 1** illustrates a hierarchical structure in Myanmar/Laos-based scam operations, showing how funds flow from underground exchanges to bulk cash and cryptocurrency, facilitating laundering.

## 2.2. The Funding Architecture of Terrorist Groups

Terrorism inherently necessitates substantial financial resources to maintain the operational capabilities and infrastructure of such groups. Armed insurgent and terrorist groups have successfully created autonomous economic systems that operate largely outside the control of traditional state authority. The substantial flows of illicit funds generated by these organizations are predominantly laundered and reinvested within global financial systems, thereby posing an ongoing and systemic threat to the security, integrity, and stability of economies (Napoleoni, 2004). Terrorist organizations' operation requires capacity to secure funding from a wide range of sources, including state sponsorship, criminal activities, charitable contributions, and trade-based money laundering schemes (Freeman, 2011). Terrorist groups often take advantage of financial crimes to fulfill a range of operational requirements, such as financing their activities, acquiring weapons, and supporting logistics (**Table 1**).

The strategic selection and combination of these financing methods reflects the terrorist groups' efforts to maximize their resources while minimizing the risk of detection and disruption by law enforcement and intelligence agencies. This adaptability and versatility in fundraising pose significant challenges to counterterrorism efforts, as the financial networks that underpin terrorist activities can be highly decentralized and compartmentalized. By tracking the movement of funds, identifying key nodes within financial networks, and implementing targeted interventions, authorities can significantly impair the operational capabilities of terrorist organizations and their criminal affiliates (Freeman, 2011).

**Table 1.** Source of terrorism financing.

Source Category	Methods of Financing Key Case Examples
Drug Trafficking	Opium trade funding Taliban fund \$100 - 400M/yr from opium (Azizi & Gundur, 2025)
Extortion & Kidnapping	ISIS \$20M/yr from kidnappings (Napoleoni, 2016)
Smuggling/Trafficking	Al-Shabaab funding from charcoal smuggling (U.S. Department of the Treasury, 2024)
State Sponsorship	Iran fund terrorist groups abroad (Knights et al., 2023)
Businesses and Investments	Hezbollah Real Estate Portfolio and Investments (Azani & Atiyas-Lvovsky, 2025)

In the 9/11 Commission Report, Al-Qaeda possessed significant financial resources, illustrating the importance of addressing the group's funding capabilities. Similar to al-Qaeda's operational structure, its financial network is intentionally decentralized and compartmentalized, reflecting a strategic approach designed to maintain resilience and evade detection. During the 1980s, Al-Qaeda's funding efforts comprised a sophisticated web of financial support that played a crucial role in their terrorist activities. Al-Qaeda has been known to employ various methods for funding its operations, including manipulating import and export receipts to disguise illicit financial flows, utilizing correspondent banking accounts to transfer funds across borders, and purchasing assets or commodities through suspect transactions. These methods allow the organization to evade detection while maintaining a steady stream of financial resources necessary for planning and executing terrorist activities. Understanding these techniques highlights the importance of sophisticated financial intelligence and international cooperation in uncovering and disrupting such clandestine funding networks. The effective deployment of financial intelligence and the ability to track and analyze the financial activities and fund flows of terrorist organizations have proven instrumental in uncovering their movements, operations, and planned activities (Rudner, 2006).

### 2.3. Anonymity

Wire transfers and cross-border bank accounts: Funds were transferred through

international banking channels, including wire transfers to and from overseas accounts, often utilizing shell companies and Hawala networks to mask the origin and destination of transactions. Terrorist groups have increasingly exploited cryptocurrencies as a means to facilitate financial activities and evade traditional detection mechanisms. While traditional banking systems are heavily regulated with mandatory reporting requirements, cryptocurrencies offer pseudonymity through wallet addresses that do not inherently reveal user identities, enabling rapid, low-cost cross-border transfers without intermediaries. Terrorists and criminal organizations frequently finance their activities through legitimate intermediaries. Disrupting these funds, regardless of their source, is essential to protecting national security.

### 3. Financial Intelligence Methodologies

Financial intelligence methodologies, including transaction monitoring, network analysis, and cross-border information sharing, play a pivotal role in converting raw financial data into actionable intelligence, strengthening proactive threat mitigation efforts. Transaction monitoring employs advanced algorithms to identify suspicious activities within financial systems, enabling early detection of illicit transactions linked to terrorism and money laundering. Network analysis visualizes and analyzes financial and transactional connections, facilitating the identification of complex and clandestine financial networks that support illicit activities. Cross-border information sharing enhances international cooperation by enabling real-time data exchange among Financial Intelligence Units (FIUs) and law enforcement agencies across jurisdictions, thus disrupting transnational financial flows that fund terrorism and organized crime. Collectively, these methodologies constitute an integrated approach that transforms disparate data points into strategic intelligence, crucial for preemptive security measures.

Financial intelligence involves a structured approach to the collection, analysis, and dissemination of data to mitigate the risks associated with illicit activities. When deployed strategically, financial intelligence enables the apprehension of key operatives, the dismantling of criminal infrastructures, and the recovery of illicit assets, thereby conferring a decisive advantage in managing security risks. Its applications include the prevention and disruption of money laundering, the countering of terrorist financing, and the detection of trade-based money-laundering schemes. Accordingly, financial intelligence operates not only as a reactive investigatory tool but also as a proactive instrument for preempting security breaches and enhancing the resilience of financial systems against exploitation.

#### 3.1. Financial Intelligence Mechanisms

- **Transaction Monitoring:** Employing advanced techniques to identify suspicious patterns, such as trade-based money laundering and flow of cryptocurrencies, which require sophisticated pattern recognition and anomaly detec-

tion.

- **Risk-Based Approaches:** Implementing Customer Due Diligence (CDD) and Know Your Customer (KYC) frameworks to evaluate client profiles and assess potential risks effectively.
- **Strategic Analysis:** Facilitating cross-border collaboration among Financial Intelligence Units (FIUs) for proactive threat identification, thereby enhancing dynamic threat assessments and early warning capabilities.

Financial intelligence operates at the intersection of economic systems and security imperatives, serving as a mechanism for identifying and disrupting flows of funds connected to illicit activity. At its core, this approach relies on gathering and analyzing transactional data from diverse sources, such as banks, money service businesses, or alternative financial systems, with the purpose of detecting anomalies that deviate from expected behavior. These deviations may hint at laundering operations or the financing of terrorism.

### 3.2. Planning, Direction, and Threat Prioritization in National Security Finance

Establishing clear strategic parameters within national security finance is crucial for guiding intelligence operations effectively. Central to this is the prioritization of threats, which employs risk-based methodologies such as the Financial Action Task Force (FATF)'s National Risk Assessments. These assessments rank threats based on their probability of occurrence and potential impact, allowing for resource allocation towards high-priority areas. This systematic approach ensures that intelligence efforts are both targeted and efficient, thereby maximizing their impact on national security.

### 3.3. Analysis and Evaluation of Financial Flows

The analysis and evaluation of financial flows are fundamental to maintaining the consistent movement of funds necessary for both organizational operations and the activities of entities and individuals. Financial intelligence plays a pivotal role in this process by providing critical insights into the movements of funds. Through sophisticated techniques, intelligence operations can detect irregularities, trace illicit financial transactions, and identify emerging threats to national security.

The ability to monitor and analyze these financial flows not only supports the detection of suspicious activities but also enhances the ability to preemptively address potential threats. By ensuring transparency and accountability in the financial system, nations can protect themselves against the misuse of financial channels by terrorist groups, organized crime, and other entities that threaten national stability.

The system's success should be measured not by how much money laundering it reduces, but by how effectively it curbs the underlying criminal activities that produce it (Reuter & Truman, 2005).

## 4. Actionable Intelligence and Legal Framework

### 4.1. Actionable Intelligence and Economic Sanctions

Actionable financial intelligence is precise, timely, and sufficiently detailed information that directly empowers authorities to execute specific, high-impact enforcement measures. In the realm of national security, the value of actionable intelligence lies in its capacity to enable security agencies to proactively intervene, prevent attacks, dismantle criminal networks, and safeguard critical infrastructure. The primary function of financial intelligence in the context of national security is to combat illicit economies by identifying, analyzing, and disrupting the financial networks. The integration of financial intelligence into broader national security strategies has become increasingly critical in addressing complex, multi-faceted threats to national security.

For example, a single suspicious transaction report revealing the details of a terrorist financing network can trigger an immediate account freeze or asset seizure, thereby starving the network of operational funds. Similarly, intelligence that pinpoints the wallet addresses and blockchain transactions used by a sanctions-evasion syndicate can enable law enforcement to preserve critical digital evidence, secure forfeiture orders, and dismantle the entire illicit financial chain. The integration of financial intelligence into broader national security strategies has therefore become indispensable, transforming raw financial data into decisive instruments of prevention, disruption, and accountability.

### 4.2. Example of Actionable Intelligence and Economic Sanctions

**Asset seizure:** Freeze bank accounts & assets; Seize cryptocurrency wallets; Issue restraining orders on property

**Evidence Preservation:** Search & seize devices/documents; Forensic imaging of phones/wallets; Interview witnesses under caution

**Movement restrictions:** Airport interception/no-fly addition; Border watchlist alerts; Passport cancellation or refusal

**International Cooperation:** Issue INTERPOL Red Notice/Diffusion; Mutual Legal Assistance Request (MLAR); Extradition request; Add to UN/EU/U.S. terrorist lists.

### 4.3. Asset Seizure Operations

Asset seizure presents challenges, including establishing the illicit origin of assets, legal jurisdiction issues, and protecting property rights. Effective asset seizure thus requires sophisticated financial investigations, international cooperation, and adherence to legal standards to ensure due process and preserve the legitimacy of actions taken (Lasmadi et al., 2023). To effectively neutralize the threat, authorities should promptly: issue an INTERPOL Red Notice for location and provisional arrest pending extradition; submit Mutual Legal Assistance Requests (MLARs) to relevant jurisdictions for evidence gathering, asset freezing, and searches; lodge formal extradition requests with any state of likely presence; and pursue designa-

tion of the subject and associated entities on the UN Security Council consolidated sanctions list, the EU autonomous counter-terrorism list, and the U.S. OFAC Specially Designated Global Terrorist (SDGT) list. These concurrent measures simultaneously restrict the subject's mobility, financial resources, and operational capacity, thereby significantly mitigating the security risk.

#### **4.4. Evidence Preservation**

Evidence preservation is one of the most critical principles in investigations, litigation, criminal justice, cybersecurity incidents, and regulatory compliance. Failing to preserve evidence properly can completely destroy a case or response effort, even if the underlying facts are in your favor. Preserving evidence in financial crime investigations requires protecting both physical and digital records from alteration, destruction, or loss through strict protocols that ensure their integrity. This includes securing items such as financial statements, emails, bank records, and electronic transactions. Essential measures involve immediately isolating devices, documenting a clear and unbroken chain of custody, and employing forensically sound methods to collect and store data.

#### **4.5. Movement Restrictions**

Effective implementation of the No Fly List and Selectee List requires that a subject's identifiers be proactively inserted and flagged in API and PNR transmissions. This triggers an automatic boarding denial by the airline, preventing the individual from reaching the border or immigration checkpoint.

#### **4.6. International Legal Framework and Policy Support**

The efficacy of Financial Intelligence (FININT) as a critical tool for national and international security is fundamentally dependent on a comprehensive legal and policy infrastructure. This framework empowers Financial Intelligence Units (FIUs), law enforcement agencies, and regulatory bodies to execute their mandates in Anti-Money Laundering (AML), Counter-Terrorism Financing (CTF), and counter-proliferation efforts, aligning with broader national security objectives.

FININT's legal foundation emerged in the late 20th century, primarily from international efforts to combat money laundering. The establishment of the Financial Action Task Force (FATF) in 1989 was instrumental in setting global AML and CTF standards, which continue to influence national legislation worldwide. A core principle of effective FININT is the promotion of timely information sharing, requiring real-time data feeds and prompt intelligence exchange among relevant agencies.

The legal and regulatory frameworks established to combat money laundering and the financing of terrorism enable critical functions from a national security and law enforcement perspective. These legal infrastructures facilitate the identification and tracking of illicit financial proceeds linked to criminal or terrorist activities. Through mandatory reporting requirements, information sharing pro-

tocols, and advanced analytical techniques, authorities can detect suspicious transaction patterns and map the complex money flows that underpin such illicit operations.

**Table 2.** Legal framework of financial intelligence.

Framework	Key Features	Strengths	Weaknesses
FATF Recommendations	Risk-based AML/CFT measures, mutual evaluations	Promotes global consistency	Enforcement gaps in non-compliant jurisdictions
U.S. BSA/AML	Reporting thresholds, beneficial ownership rules	Robust enforcement tools	High compliance costs for small institutions
European Union's Anti-Money Laundering Directives	Promotes transparency and accountability in financial systems, deterring illicit activities.	Risk-based approach allows resource allocation focusing on high-risk sectors while minimizing burdens on low-risk entities	Implementation variations across member states create loopholes

The three primary international and regional AML/CFT frameworks—the FATF Recommendations, the U.S. Bank Secrecy Act/Anti-Money Laundering (BSA/AML) requirements, and the European Union's Anti-Money Laundering Directives—each exhibit distinct key features, strengths, and limitations, as shown in **Table 2**. These frameworks collectively promote transparency, global consistency, and efficient resource allocation in combating money laundering.

The legal framework enables the disruption of money laundering and terrorism financing networks by providing law enforcement and intelligence agencies with the tools to interdict, seize, and forfeit these ill-gotten gains. By severing the financial lifelines of criminal and terrorist organizations, these interventions can significantly degrade their operational capabilities and resilience. The legal infrastructure supports the implementation of targeted financial sanctions, which can restrict the access of designated individuals, entities, and jurisdictions to the global financial system. Such financial coercion measures are intended to isolate and contain the threat posed by these illicit actors, denying them the resources required to fund their nefarious activities.

Collectively, these key functions enabled by the legal and regulatory frameworks play a crucial role in broader national security efforts to combat the financing of terrorism and other transnational criminal threats. The effective and responsible application of these powers must be balanced against the protection of individual civil liberties and the preservation of public trust in the financial system. At the national level, specific legislative instruments provide authorities with necessary tools.

Disrupting terrorist finance networks has become a strategic priority. Measures include targeted asset freezes and interagency coordination. Efforts to combat proliferation financing, particularly funding development of Weapons of Mass Destruction (WMD), remain critical within the global security architecture.

#### 4.7. International Intelligence Sharing

The critical role of international cooperation, comprehensive financial oversight, and robust legal frameworks in mitigating systemic vulnerabilities. By comprehending the operational mechanisms of terrorist financing—including the exploitation of charitable organizations and informal value transfer systems—targeted, evidence-based interventions can be developed. Furthermore, addressing interconnected predicate offenses such as drug trafficking, arms smuggling, and human trafficking is essential, as these activities constitute primary revenue sources for terrorist entities.

The transnational mobility of financial intelligence is far from automatic; data are not readily shared across jurisdictional boundaries. Instead, effective cross-border sharing depends on deliberate efforts to cultivate and sustain mutual trust among institutions, underpinned by robust governance practices, secure platforms, and ongoing relationship-building to ensure sensitive information can be exchanged reliably and confidentially (Lagerwaard & de Goede, 2023).

#### 4.8. Examples of International Intelligence Sharing

**Egmont Group:** The Egmont Group of Financial Intelligence Units is a global entity that promotes collaboration and the exchange of intelligence among national Financial Intelligence Units (FIUs) to combat and avert money laundering and the financing of terrorism (Amicelle & Chaudieu, 2018).

**FATF (Financial Action Task Force):** The FATF serves as the leading global institution for policy formulation and standard establishment in the realm of anti-money laundering and counter-terrorism financing. Its recommendations form the globally acknowledged normative framework that mandates jurisdictions to criminalize money laundering and terrorist financing, create financial intelligence units, carry out customer due diligence, report suspicious transactions, facilitate international collaboration, and enforce targeted financial sanctions. It conducts mutual evaluations and keeps black and grey lists.

**INTERPOL:** Facilitating immediate communication between law enforcement agencies regarding criminal intelligence, which encompasses information on terrorist financing and money laundering.

**European Union Financial Intelligence Units Platform (EU FIU Platform):** This initiative brings together the Financial Intelligence Units (FIUs) from all 27 EU Member States, with Europol and Eurojust acting as observers. It enables coordinated joint analyses and permits the rapid and secure exchange of financial intelligence among European FIUs. A decentralized information exchange network that is technically integrated into Europol's secure infrastructure (Mouzaki, 2020).

#### 4.9. Financial Intelligence Units

Financial Intelligence Units (FIUs) are specialized agencies that play a central role in the global Anti-Money Laundering and Counter-Terrorism Financing (AML/CFT) framework by receiving suspicious transaction reports from private financial institutions and passing relevant intelligence to law enforcement. Because FIUs handle large amounts of personal data, their activities must comply with data protection rules (Brewczyńska, 2021).

The structural organization of Financial Intelligence Units (FIUs) varies significantly across jurisdictions, with profound implications for national security. Some countries adopt administrative approaches, while others integrate FIUs directly within law enforcement agencies. These structural differences fundamentally influence data access protocols, retention policies, and operational agility, all of which are critical factors in a nation's ability to respond swiftly and effectively to financial threats to national security.

#### 5. Conclusion

Financial intelligence is an integral component of national security frameworks, central to preserving economic stability and state integrity. Systematic collection and analysis of financial flows enable authorities to identify and disrupt criminal organizations and terrorist networks, protecting core national interests as global financial systems grow increasingly complex and interconnected. Consequently, robust and adaptive strategies are required to address evolving financial threats and technological change. These capabilities are instrumental in degrading terrorist operational capacity, strengthening regulatory enforcement, and facilitating international cooperation. Integrating financial intelligence into broader security strategies yields actionable insights across diplomatic, economic, and military domains, supporting more nuanced and effective responses to both traditional and emergent threats. Illicit financial activities not only threaten security but also have a broader economic impact, including undermining trust in financial institutions, distorting markets, and facilitating corruption. The nexus between illicit economies, financial intelligence, and national security represents a critical area of focus for policymakers and security professionals. The evolving nature of financial threats to national security necessitates ongoing adaptation of strategies, technologies, and international cooperation frameworks. Balancing the need for robust financial intelligence capabilities with the protection of civil liberties remains a key challenge in safeguarding national security. Ultimately, the future efficacy of financial intelligence will hinge on its capacity to anticipate and counter technologically empowered adversaries while preserving the integrity and privacy expectations of the legitimate financial system.

#### Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

## References

- Amicelle, A., & Chaudieu, K. (2018). In Search of Transnational Financial Intelligence: Questioning Cooperation between Financial Intelligence Units. In C. King, C. Walker, & J. Gurulé (Eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law* (pp. 649-675). Springer International Publishing. [https://doi.org/10.1007/978-3-319-64498-1\\_27](https://doi.org/10.1007/978-3-319-64498-1_27)
- Azani, E., & Atiyas-Lvovsky, L. (2025, May 16). *Hezbollah's Financing Ecosystem-Crime Families as a Case Study: The Ahmad Clan*. International Institute for Counter-Terrorism. <https://ict.org.il/hezbollahs-financing-ecosystem-crime-families-as-a-case-study-the-ahmad-clan/>
- Azizi, H., & Gundur, R. V. (2025). The Taliban's Drug Trade Revenue and Taxation System: What the Experts Know. *Studies in Conflict & Terrorism*, 1-22. <https://doi.org/10.1080/1057610x.2025.2502924>
- Brewczyńska, M. (2021). Financial Intelligence Units: Reflections on the Applicable Data Protection Legal Framework. *Computer Law & Security Review*, 43, Article ID: 105612. <https://doi.org/10.1016/j.clsr.2021.105612>
- Freeman, M. (2011). The Sources of Terrorist Financing: Theory and Typology. *Studies in Conflict & Terrorism*, 34, 461-475. <https://doi.org/10.1080/1057610x.2011.571193>
- Knights, M., Malik, H., & Smith, C. (2023). *Iraq's New Regime Change: How Tehran-Backed Terrorist Organizations and Militias Captured the Iraqi State*. CTC Sentinel. <https://ctc.westpoint.edu/iraqs-new-regime-change-how-tehran-backed-terrorist-organizations-and-militias-captured-the-iraqi-state/>
- Lagerwaard, P., & de Goede, M. (2023). In Trust We Share: The Politics of Financial Intelligence Sharing. *Economy and Society*, 52, 202-226. <https://doi.org/10.1080/03085147.2023.2175451>
- Lasmadi, S., Usman, U., Sudarti, E., & Arfa, N. (2023). Asset Seizure of Money Laundering Crimes Arising from Corruption in the Perspective of Legal Certainty and Justice. *Pandecta Research Law Journal*, 18, 352-374. <https://doi.org/10.15294/pandecta.v18i2.48568>
- Mouzakiti, F. (2020). Cooperation between Financial Intelligence Units in the European Union: Stuck in the Middle between the General Data Protection Regulation and the Police Data Protection Directive. *New Journal of European Criminal Law*, 11, 351-374. <https://doi.org/10.1177/2032284420943303>
- Napoleoni, L. (2004). *The New Economy of Terror: How Terrorism Is Financed*. Forum on Crime and Society United Nations. [https://www.unodc.org/documents/data-and-analysis/Forum/V05-81059\\_EBOOK.pdf#page=41](https://www.unodc.org/documents/data-and-analysis/Forum/V05-81059_EBOOK.pdf#page=41)
- Napoleoni, L. (2016). *Merchants of Men: How Jihadists and ISIS Turned Kidnapping and Refugee Trafficking into Big Business*. Seven Stories Press.
- Reuter, P., & Truman, E. M. (2005). Anti-Money Laundering. *International Economy*, 56-60. [https://www.international-economy.com/TIE\\_W05\\_ReuterTruman.pdf](https://www.international-economy.com/TIE_W05_ReuterTruman.pdf)
- Rudner, M. (2006). Using Financial Intelligence against the Funding of Terrorism. *International Journal of Intelligence and CounterIntelligence*, 19, 32-58. <https://doi.org/10.1080/08850600500332359>
- Shelley, L. (2020). *Illicit Trade and Terrorism VOL*. <https://pt.icct.nl/article/illicit-trade-and-terrorism>
- U.S. Department of the Treasury (2024). *Treasury Sanctions Network Supporting Iran's Military and Autocratic Regimes*. <https://home.treasury.gov/news/press-releases/jy1499>