GFMI
GLOBAL FINANCIAL MARKETS INSTITUTE

Article **2026**

The Three Lines of Defense: The Financial Services Industry Role in Supporting National Security in an Era of Global Financial Crime

by Alma Angotti and William Jannace

The article expresses the personal views of the authors and does not necessarily reflect the views of any organizations with which either is affiliated.

The authors would like to thank Margaret Mizwicki and Babin Dinda for their contributions to this article.

The Three Lines of Defense: The Financial Services Industry Role in Supporting National Security in an Era of Global Financial Crime

Traditional Financial Services

The Department of Defense (DoD) recently reissued its Irregular Warfare Directive, which includes transnational organized crime and counter threat finance in the definition of irregular warfare.[1] As traditional financial crime and national security converge, a whole government approach is needed to protect the U.S. financial system's vulnerability to irregular warfare.

The Three Lines of Defense (3LOD) Model[2] was introduced by the Institute of Internal Auditors (IIA) as an approach to risk management.[3] It is an industry framework utilized to ensure that the financial services industry is complying with numerous regulations.

> "The model divides risk management responsibilities into three distinct levels, ensuring that risks are adequately identified, managed, and mitigated . . . The 3LOD model assigns specific responsibilities to three lines of defense, each playing a critical role in risk identification, management, and mitigation. The lines work together to ensure thorough oversight and avoid gaps or overlaps in risk management efforts."[4]

> "The First Line consists of operational units that are directly involved in day-to-day activities such as product development, customer interactions, and service delivery. These teams are responsible for implementing risk management controls and internal policies as part of their routine operations."[5]

> "The Second Line includes specialized teams responsible for risk management, compliance, and oversight. Their role is to support the First Line by developing policies, providing resources and guidance, and ensuring that risk management activities align with organizational goals. The Second Line also monitors the effectiveness of risk management practices and helps identify emerging risks."[6]

> "The Third Line consists of independent auditors who assess the overall effectiveness of the risk management framework. This line conducts audits, identifies gaps in the process, and provides recommendations for improvement."[7]

By encompassing the breadth of risk, the 3LOD model allows for an efficient and effective approach towards risk management. Its division of responsibility ensures that risks are not left unattended and that the compliance efforts are all-encompassing. Therefore, it plays a pivotal role in the overall risk equation and is held in high regard in both the corporate and banking

world.[8] Importantly, the financial services industry and its 3LOD framework is an important line of defense for the Unites States in its battle against illicit finance, a battle which increasingly is being fought in the digital[9] ecosystem by capable and well organized illicit actors. Although both the financial services industry and national security apparatus are beset with data overload, information silos, and related governance issues,[10] evolving public-private partnerships are emerging to address this growing concern.[11]

The 3LOD in Support of National Security

The financial services industry 3LOD supports national security concerns about illicit financing through rigorous due diligence with respect to onboarding clients and surveillance of related client activity (the First Line); subsequent compliance oversight of Line 1 activity (the Second Line); and rigorous internal audit and review of the activities conducted in Lines 1 and 2 (the Third Line).[12]

In aggregate, the financial services industry 3LOD model is the first line of the U.S.'s 3LOD against illicit finance, with the Financial Crimes Enforcement Network (FinCEN) and the Department of Justice as Lines 2 and 3, respectively. Coordinating further with various technology vendors to support, for example, digital asset seizure, can further enhance the efficacy of the 3LOD framework in support of national security.[13] As was recently noted, the U.S. should "[i]nstitutionalize tech proficiency across government and national security."[14]

Relationship Between Financial Crime and National Security

The relationship between national security and fraud has been growing closer as nation states and terrorist groups harness the revenue generation of fraud schemes.[15] For example, North Korea pulled off the largest heist in history, $1.5 billion through a cyber-attack on a crypto exchange.[16] Financial Institutions (FIs) can and should leverage these national security priorities for their cyber-security and fraud responses by integrating published intelligence assessments into their fraud and financial crime risk assessments. "Through a process of dissemination, reviews to policies and controls and incorporation into risk management procedures, this intelligence can be at the heart of an informed fraud detection strategy."[17] In addition, as noted above, law enforcement can benefit from insight into the national security connections uncovered by FIs in their fraud financial crime investigations.[18]

The National Security Implications Not Limited to the Financial Services Industry

According to the Eversheds Sutherland's 2025 U.S. National Security Compliance Risk and Readiness Report ("NSCRR Report"),[19] at least one-third of U.S. companies are not fully prepared to address key national security compliance risks facing their firms despite the legal, financial, and operational consequences. According to the NSCRR Report, "[N]early one-quarter of the

national security compliance professionals surveyed cannot fully articulate their company's national security risk profile, potentially complicating efforts to prioritize resources."[20]

Financial Crime as a National Security Threat

Financial crime continues to evolve and frequently represents a national security threat. Money laundering and its associated financial crimes are estimated at over $3.1 trillion globally,[21] exacerbating corruption, impacting economic growth and development, and providing a source of income to various malign actors, including acts of terrorism.[22] Financial crime, including cryptocurrency laundering,[23] has become an instrument of national power for certain state actors or non-state actors with a connection to a state too, impacting the efficacy of the traditional model. DIME — Diplomatic, Information, Military and Economic — is the acronym describing the instruments of traditional national power. U.S. policymakers and strategists have understood that there are many more instruments involved in national security policy development and implementation.[24] Given the scope of ML/CFT, some would argue that malign actors have reconfigured the DIME acronym by substituting the "E" with "IF" (for "illicit finance") to reflect the asymmetry of this new weapon of finance in lieu of the more traditionally understood concept of economic power. Today the evolving ecosystem of illicit finance enables countries such as Russia and North Korea to evade and withstand sanctions,[25] and to fund weapons of mass destruction. The economic power gained through illicit finance can potentially limit the impact of traditional means of financial statecraft.

Money laundering goes beyond the laundering of criminal proceeds. Transnational Criminal Organizations (TCOs) groups, state sponsored or supported sanctions evaders utilizing the digital ecosystem,[26] cryptocurrency, and professional enablers, are a growing national security problem.

> "OFAC sanctions take various forms, from blocking the property of specific individuals and entities to broadly prohibiting transactions involving an entire country or geographic region, such as through a trade embargo or prohibitions related to particular sectors of a country's economy."[27]

While AML regulators and FIs can utilize information sharing frameworks[28] and systems to combat financial crime and protect the integrity of the financial system, sharing such information may be inadequate given the rising national security threat that AML/CFT poses.[29]

A recent report entitled, "Weaponizing Artificial Intelligence: How AI Reshapes the World of Organized Crime," addressed "issues related to sophisticated crimes that are committed, automated, or enhanced using artificial intelligence tools." The report highlighted, among others, the following:

> "1. AI technologies, especially generative AI and large language models, are transforming organized crime by lowering technical barriers and enabling scalable, automated illicit activities. 2. Criminal uses of AI include enhanced

> cyberattacks (polymorphic malware, ransomware, phishing), synthetic identity fraud (deepfakes, forged documents), bypassing financial controls, money laundering and to optimize illicit trafficking routes, among others . . . 4. Financial fraud is escalating, with deepfake-based scams, crypto laundering, and stock manipulation driven by AI-generated disinformation. 5. Organized crime groups and cartels now deploy AI-controlled drones, semi-submersibles, and autonomous weapons, merging military-grade tech with illicit trade. 6. These developments industrialize crime, with 'Crime-as-a-Service' platforms and dark LLMs (e.g., WormGPT, FraudGPT) offering turnkey tools to non-experts."[30]

Exacerbating these problems is Great Power[31] competition. Geopolitical fragmentation is hindering interstate cooperation on combatting transnational organized crime (TOC), thus undermining support for international treaties designed to address such issues. "International judicial cooperation against crime is emerging as one of the casualties of current worldwide geopolitical tensions . . . [T]his directly affects states' ability to confront increasingly invasive forms of transnational organised crime such as human trafficking, environmental crime, and different forms of cybercrime . . . often considered a threat to international security."[32]

Recent Trends in Digital Financial Crime

A report by TRM Labs dealing with the growing landscape of seizable crypto assets noted the following findings:

> "Illicit entities hold nearly $15 billion in 2025, with stolen funds representing the largest category. Wallets downstream from these entities, defined as those that received funds from illicit sources in excess of 10% of total inflows, hold over $60 billion — roughly 4 times the amount held by illicit entities themselves. Darknet market administrators and vendors alone control over $40 billion in on-chain value. Bitcoin maintains dominance over other cryptocurrencies at 75% of total illicit entity balances due to its increase in value over time, but stablecoins and ether have grown substantially . . . Illicit actors are rapidly evolving their laundering methodologies and cash-out infrastructure, often leveraging more cashout addresses and using them for shorter durations. Direct transfers from illicit entities to exchanges have collapsed from a quarterly value of roughly 40% in 2021–2022 to around 15% in Q2 2025."[33]

Terrorist Financing[34]

2015 FATF Report

As far back as 2015, the Financial Action Task Force reported that "[w]hile the number and type of terrorist groups and related threats have changed over time, the basic need for terrorists to raise, move and use funds has remained the same. However, as the size, scope and structure of

terrorist organizations have evolved, so too have their methods to raise and manage funds." The 2015 report "highlight[ed] that understanding how a terrorist organisation manages its assets is critical to starving the organisation of funds and disrupting their activities in the long term. Terrorist organisations have different needs, depending on whether they are large, small, or simply constituted of a network of seemingly isolated individuals." The report noted that "[a]nti-money laundering (AML) and countering the financing of terrorism (CFT) systems and operational measures have made it more difficult for terrorist organisations to use traditional avenues to raise or move funds." The report also noted that "the adaptability of these organisations, and new threats posed by foreign terrorist fighters and small cell terror networks, require authorities to monitor how these traditional methods continue to be used. The use of national risk assessments to conduct strategic analysis of current TF risks will help inform policy makers to implement the necessary legal and operational measures."[35]

In July 2025, FATF published a new edition of its Comprehensive Update on Terrorist Financing Risks. The 2025 update presents a current analysis of current TF threats and emerging trends, as well as the effectiveness of approaches implemented by national agencies worldwide. The update also provides guidance for FIs on identifying and managing TF risk indicators.[36]

The FATF's 4th Round of Mutual Evaluations revealed that 69% of the 194 participating jurisdictions had "major or structural deficiencies in effectively investigating, prosecuting, and convicting" TF cases.[37] Among the recommendations, the FATF's report recommends the adoption of "coordinated, multilateral responses" to address the transnational dimension of TF risks.[38] It also recommends the more effective implementation of the FATF Recommendations and for stronger engagement from sectors that are not covered by the recommendations through methods including "targeted public-private partnerships."[39] For example, it recommends that the FATF should consider increasing its support for the private sector through means including "creating a centralized online repository of relevant materials, developing targeted communication strategies, and providing awareness-raising and training activities".[40]

Evolving Terrorist Financing Methodologies and Motivations

TF actors are "using various activities to generate, transfer, launder and conceal funds, complicating efforts relating to both compliance and enforcement. TF increasingly involves a combination of illegal activities, including trade and trafficking of natural resources, and other organized crime activities, such as kidnapping, extortion, human trafficking, and drug smuggling. Different types of terrorist actors have different financial needs and, therefore, adapt their 'financial management strategies' accordingly."[41] The fact that similar, or equivalent, types of terrorist actors may adopt alternative financing methods to support their needs further complicates the prospects for shutting down such illicit activity.[42] An example of "the impact of the increased intersection between TF and other forms of organized crime, is the designation by the U.S. government of eight cartels and TCOs as FTOs and SDGTs."[43]

Furthermore, terrorist groups are making use of increasingly sophisticated and decentralized methods for raising and moving funds as they continue to exploit the mainstream international financial system. This underscores how important it is for regulated firms to prioritize TF risks alongside ML and proliferation financing (PF) risks in their compliance procedures.[44]

The report "identifies numerous factors that influence the nature of TF risks, including territorial control, ***connections to armed conflict, natural resource issues, weak governance, corruption levels, the prevalence of informal financial networks and state sponsorship***.[45] The types of terrorist actors involved, such as terrorist organizations of varying scale and individual lone actors, also affect such risks."[46]

In its 2025 comprehensive update, FATF also noted that in addition to legal entities such as shell companies and trust structures, terrorist organizations exploit non-profit organizations (NPOs). Terrorist actors are not only abusing legitimate NPOs but also establishing sham organizations as vehicles to further their interests.[47] The FATF cites a 2024 paper produced by the Egmont Group that identified six methods "prevalent in the abuse of NPOs for TF purposes:"

- funds diversion;
- affiliation with terrorist entities;
- abuse of NPO programs;
- recruitment support;
- false representation; and
- fundraising through social media.[48]

The FATF report further notes that armed conflicts and humanitarian crises are being manipulated for TF purposes, as terrorists divert aid or exploit NPOs for their own purposes. In addition to exploiting traditional or "mainstream" financial systems, such as banking and prepaid cards, TF-linked actors are using e-money systems and informal value transfer systems (IVTS) and "shadow" banking services such as hawala IVTS networks to enable criminal actors to evade regulatory controls and restrictions whilst avoiding transaction fees. Offering secrecy and a general absence of record keeping, these systems are attractive to such actors. Underpinned by a movement of value, as opposed to a movement of funds, these systems render transaction tracing difficult for law enforcement agencies and firms undertaking due diligence alike. For example, FATF noted that Afghanistan-based terrorist network operatives relied on hawaladars to transfer funds internationally and store financial assets on behalf of their wider terrorist group.[49]

Furthermore, some terrorist organizations, or networks, are adopting tech-enabled methods of value transfer, such as blockchain-based systems, to promote their interests. Blockchain technology can also be used to host online crowdfunding campaigns — a popular method used by terrorist actors to reach a number of donors quickly, cheaply and with relative safety.[50]

The FATF report highlights the scale and complexity of the TF threats facing the world today, and the ways in which private sector stakeholders, including regulated firms, can contribute towards

combating these threats. The implementation of strong TF compliance procedures will not only help fight terrorism but also protect firms from incurring their own civil or criminal liability.[51]

The recommendations are important and vital to preserving the integrity of the financial system. Given the national security implications from having terrorists so integrally involved and profiting from this maligned activity, the opportunity to rethink how the existing regulatory and suspicious activity reporting system can be better leveraged to involve U.S. national security apparatus earlier to potentially degrade their abilities to raise funds and launder them in support of terrorist activities.

International Cooperation

FATF, The Egmont Group, INTERPOL and the United Nations Office on Drugs and Crime (UNODC) are advocating for stronger global collaboration among analysts, investigators, and prosecutors in connection with the issuance of Handbook on International Cooperation against Money Laundering, providing tools to help countries speed up investigations, and bringing more criminals to justice. They note that

> "[m]oney laundering almost always crosses borders, and criminals exploit gaps between national legal systems to hide their activities and avoid punishment. Yet, FATF evaluations consistently show that investigating, prosecuting and sanctioning money laundering remains one of the weakest areas worldwide. Without more effective co-operation, countries cannot stop financial crime in its tracks."[52]

> "The handbook responds to the globalization of financial systems and rapid technological advancements, which demand faster intelligence and action to keep pace with criminals. It promotes informal cooperation, such as secure communication channels, rapid response mechanisms and joint analysis, which can provide faster, more flexible, and targeted investigations, complementing formal, usually legal processes, which are often slower and procedurally complex."[53]

> "The handbook highlights real-world cases that demonstrate the impact of international cooperation: Financial Intelligence Units (FIUs) in Italy, Spain and the Netherlands uncovered a €95 million cross-border laundering scheme through joint analysis and intelligence sharing . . . U.S. and Indian authorities co-ordinated in real time to seize cryptocurrency assets worth USD 150 million linked to drug trafficking . . . The organizations warn that criminals will continue to exploit legal loopholes unless financial intelligence units, law enforcement agencies and prosecutors cooperate more effectively."[54]

Technology and Detecting Illicit Activity

The GENIUS Act "directs the Secretary of the Treasury to seek public comment on innovative or novel methods, techniques, or strategies that regulated financial institutions use, or have the potential to use, to detect illicit activity[55] involving digital assets."

The report of the President's Working Group on Digital Asset Markets also includes recommendations related to countering illicit finance and promoting a transparent and resilient digital asset ecosystem.[56] The report proposes that the ***U.S. government evaluate and consider issuing guidance on the use of digital identity verification by financial institutions and increase public-private cooperation and information sharing, including through FinCEN's 314(a) and 314(b) programs.*** Consistent with the GENIUS Act, when conducting research on these and other innovative or novel methods, techniques, or strategies, Treasury will evaluate and consider:

- ***improvements in the ability of financial institutions to detect illicit activity involving digital assets;***
- ***cybersecurity risks; and***
- ***effectiveness of the methods, techniques, or strategies at mitigating illicit finance.***[57]

In response to the Treasury's Request for Comment noted above on innovative methods to detect illicit digital asset activity, the Crypto Council for Innovation (CCI) submitted a letter urging the Department of the Treasury to promote innovation-driven approaches to combat illicit finance in the digital asset sector. The CCI letter recommended policies to encourage the adoption of advanced compliance tools using AI, emphasizing that emerging technologies can significantly strengthen AML/CFT programs when supported by clear, risk-based regulatory guidance. The CCI letter noted among other recommendations: the use of decentralized identity tools as a privacy-preserving alternative for KYC verification, and using cryptographic proofs instead of document uploads to reduce data exposure. The CCI recommended that FinCEN publish guidance confirming that decentralized identity solutions can satisfy AML/CFT and sanctions compliance requirements under the BSA and encouraged continued engagement through FinCEN's digital identity sprints.[58]

The CCI letter also emphasized the importance of blockchain analytics for tracing asset provenance and identifying illicit wallets. It also cited tools such as zero-knowledge proofs, association sets (privacy pools), and attestation tokens as ways to embed compliance tools within blockchain protocols while preserving user privacy. The CCI also noted that blockchain analysis tools are expanding their capabilities to include real-time threat detection, advanced pattern recognition, and integration with threat intelligence feeds, highlighting companies that are developing next-generation tools that can identify emerging threats such as malicious wallets and provide actionable, real-time intelligence to compliance teams.[59]

A Way Forward

Regulators and the financial services community have noted costly compliance efforts that may provide countries comfort and a feeling of security but may not make the countries and financial system safe from financial crime.[60] Rather than accepting failure, countries could opt for a whole of government approach utilizing all instruments of national power and integrating more nuanced and focused national security options to decrease the flow of funds related to the financing of terrorism and other TCOs.

Building on Private Sector Technology Capability Solutions

In the aftermath of the 2008 financial crisis, the 2010 Dodd-Frank Act established the Financial Stability Oversight Council (FSOC) to monitor the U.S. financial system for systemic risks, promote financial stability, and respond to emerging threats. The Secretary of the Treasury chairs it, and it consists of the heads of major financial regulatory agencies and an independent insurance expert, serving to improve coordination among regulators and provide transparency on financial stability risks.[61] Its 2024 Annual Report noted a myriad of threats and vulnerabilities including geopolitical, cyber, and money laundering and ransomware.[62]

Private sector vendors already provide data-centric solutions for the financial services industry. Private sector vendors can potentially leverage additional commercial reports and data to better target illicit finance risks in a more holistic manner. Ensuring that vendors integrate data from public sources such as the Crony Capitalism Index,[63] Fragile States Index Heat Map,[64] the Basel Index,[65] and the FATF Black and Gray Lists[66] can help better identify potential corruption, illicit financial activity, and the financing of terrorism. Adding data on capital flows and other types of financial statecraft flows, such as China's Belt and Road Initiative,[67] may help inform where stress points and financial largess meet to exacerbate corruption and make countries more vulnerable to illicit activity.

In addition, as noted above, crypto intelligence firms such as Chainalysis, TRM Labs, and Elliptic are supporting national security by providing blockchain analytics tools[68] and data to government agencies to detect, investigate, and disrupt criminal and illicit activities involving cryptocurrency.[69] Most recently, TRM Labs announced the establishment of the Beacon Network (Beacon), the First Real-time Crypto Crime Response Network."[70] Beacon was built in collaboration with law enforcement, exchanges, and stablecoin issuers, and is designed to prevent illicit funds from leaving the blockchain.[71]

Conclusion

The increased integration of national security priorities in money laundering and sanction guidance gives financial institutions the opportunity to think creatively. The 3LOD model viewed as a partnership between financial institutions, regulators, and the Department of Justice's National Security Division, among others, can be a powerful tool to prevent state actors abuse of the

global financial system. Advances in technology to support threat identification, threat mitigation, and digital asset seizure can further enhance the efficacy of the 3LOD framework in support of national security.[72] We all have our roles to play in keeping our nation safe. Together we can enhance the efficacy of the Three Lines of Defense to foster national security. A new way forward by harnessing the power of all our lines of defense is worthy of further consideration.[73]

About the Author: Alma Angotti

Alma Angotti is a recognized expert in financial crime compliance and economic sanctions with more than 30 years of experience in both regulatory enforcement and global consulting. Alma has held senior enforcement roles at the U.S. Securities and Exchange Commission (SEC), the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the Financial Industry Regulatory Authority (FINRA). She brings deep subject matter expertise in regulatory compliance, including Bank Secrecy Act/Anti-money Laundering (BSA/AML), sanctions, and counter-terrorist financing (CFT).

At FTI Consulting, Alma advises clients on compliance risk assessments, remediation strategies, enforcement preparedness and regulatory investigations. Her clients include global and mid-sized financial institutions; global fintech firms; digital assets and payments institutions; stablecoins and cryptocurrency platforms; broker-dealers; hedge funds; casinos; and multinational corporations.

Alma serves on the advisory boards of the Global Digital Asset and Cryptocurrency Association and the Digital Dollar Project. At FinCEN and FINRA, she designed and led the AML enforcement programs and regularly trains regulators and government officials worldwide on AML and financial crime compliance matters. Additionally, she has been approved to be an independent compliance monitor by federal and state regulatory agencies, including the SEC, the Office of the Comptroller of the Currency (OCC) and the New York State Department of Financial Services (NYDFS).

About the Author: William Jannace

William Jannace is an Associate Professor at the Dwight D. Eisenhower School for National Security and Resource Strategy/National Defense University, where he teaches courses on economics and finance and national security. He has also served as an expert witness for The Bates Group on securities litigation matters. He is also an adjunct professor/lecturer at Fordham School of Law, Global Financial Markets Institute, and Metropolitan College, where he teaches courses covering Capital Markets/Digital Assets/Securities Regulation and Corporate Governance; State Capitalism, AML/Cybersecurity; Geopolitics/Geo-Economics, and U.S. Foreign Policy/International Relations, and Grand Strategy.

Mr. Jannace had previously worked at the American and New York Stock Exchanges, FINRA and several investment banking firms. He was also an account executive at Georgeson and D.F. King where he worked on proxy fights and tender offers. He has also served as a consultant for The World Bank and the Asian Corporate Governance Association. He has also lectured at the U.S. Army War College.

Mr. Jannace has also conducted overseas training programs for the: Russian Securities Commission/Stock Exchange; The Capital Markets Authorities in: Uganda, Burundi, Tanzania and Kenya; Saudi Arabian Capital Markets Authority; Securities and Exchange Board of India;

Ukrainian Securities Commission/Stock Market; Romanian Securities Commission; Jordanian Securities Commission; Capital Markets Authority of Turkey; Albanian Financial Supervisory Authority; New York Institute of Finance- Beijing/China, the Taiwan Stock Exchange and for IOSCO in Spain.

He is a member of the faculty advisory group of Board Intelligence. He is also a ClArb Fellow, a member of the Association of Certified Anti Money Laundering Specialists, International Institute for Strategic Studies, New York International Arbitration Center, and Bretton Woods Committee. He is also a supporter of the National World War II Museum, American Battle Monuments Foundation, and National D-Day Memorial. Mr. Jannace received his JD from New York Law School, and his LL.M. in Corporate, Banking, and Finance Law from Fordham Law School.

The views expressed herein are those of the author(s) and not necessarily the views of the Dwight D. Eisenhower School for National Security and Resource Strategy/National Defense University, The Department of Defense, and FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm. FTI Consulting is an independent global business advisory firm dedicated to helping organizations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centers throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities. www.fticonsulting.com.

23 Maytime Court
Jericho, NY 11753
+1 516 935 0923
www.GFMI.com

[1] DOD INSTRUCTION 3000.07 - Irregular Warfare at page 3. "Irregular Warfare is a joint force activity conducted by conventional forces and special operations forces (SOF). (1) The DoD can conduct IW using space and cyber capabilities as part of integrated campaigning. (2) DoD IW operations and key enablers can include, but are not limited to: (a) Unconventional warfare. (b) Foreign internal defense. (c) Counterterrorism. (d) Counterinsurgency. (e) Stabilization activities. (f) DoD support to counter-threat finance and counter-transnational organized crime efforts." DOD INSTRUCTION 3000.07 - Irregular Warfare

[2] "Understanding the Three Lines of Defense Model in Risk Management," V-Comply (April 3, 2025), https://www.v-comply.com/blog/three-lines-defense-risk-management/.

[3] Ibid.

[4] Ibid.

[5] Ibid.

[6] Ibid.

[7] Ibid.

[8] "AML-CFT Compliance: The Three Lines of Defense Explained," Sanctions.io (November 4, 2024) https://www.sanctions.io/blog/the-three-lines-of-defence-explained.

[9] In its 2025 Crypto Adoption and Stablecoin Usage Report, TRM Labs recently noted that "[b]etween 2024 and 2025, sanctions drove illicit volume growth for non-stablecoin digital assets, while sanctions-related activity in stablecoins fell by 60%, indicating a potential shift away from stablecoins for sanctions evasion." https://www.trmlabs.com/reports-and-whitepapers/2025-crypto-adoption-and-stablecoin-usage-report (October 21, 2025).

[10] "Controlling and managing the deluge of data in the Army could require the service to establish new formations dedicated to the task. . . ." Data "has become the Army's ammunition," which begs the question of whether there is an organization designed to oversee data across the

U.S. Army. "[T]he Army is exploring — but hasn't decided on — whether it needs a dedicated formation to manage and integrate data across the entire Army, that spans from within the U.S. to outside the nation's borders, from garrison to the tactical edge. The formation would allow the Army to deliberately focus on standardizing data formats, ensuring interoperability, applying artificial intelligence and machine learning for insights, and ultimately enabling data-centric operations across the force, regardless of location . . ." Pomerleau, Mark, "If data is the new ammo, Army may need dedicated data formations: General," Breaking Defense (October 10, 2025), https://breakingdefense.com/2025/10/if-data-is-the-new-ammo-army-may-need-dedicated-data-formations-general/.

[11] "With the establishment of a Strategic Bitcoin Reserve (SBR) and a Digital Assets Stockpile (DAS), the United States declared that it intends to add to its pool of digital capital through additional asset seizures. And indeed, the cryptocurrency ecosystem presents law enforcement with an unprecedented opportunity: billions of dollars in illicit proceeds are sitting on public blockchains and are theoretically seizable if authorities can coordinate action. To date, Chainalysis has helped law enforcement agencies worldwide seize more than $12.6 billion in illicit funds through [its] data, software, and services. Building on this proven history of successful seizures, [Chainalysis has] conducted a comprehensive analysis of potentially seizable assets currently sitting on public blockchains." "The Growing Landscape of Seizable Crypto Assets: On-Chain Balances Linked to Criminal Activity Exceed $75 Billion," Chainalysis (October 9, 2025), https://www.chainalysis.com/blog/landscape-of-seizable-crypto-assets-2025/.

[12] For example, broker -dealers "must comply with the Bank Secrecy Act and its implementing regulations ("AML rules"). The purpose of the AML rules is to help detect and report suspicious activity including the predicate offenses to money laundering and terrorist financing, such as securities fraud and market manipulation. FINRA reviews a firm's compliance with AML rules under FINRA Rule 3310, which sets forth minimum standards for a firm's written AML compliance program. The basic tenets of an AML compliance program under FINRA 3310 include the following: The program has to be approved in writing by a senior manager; It must be reasonably designed to ensure the firm detects and reports suspicious activity; It must be reasonably designed to achieve compliance with the AML Rules, including, among others, having a risk-based customer identification program (CIP) that enables the firm to form a reasonable belief that it knows the true identity of its customers. It must be independently tested to ensure proper implementation of the program . . . The program must include appropriate risk-based procedures for conducting ongoing customer due diligence, including (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and, (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information, including information regarding the beneficial owners of legal entity customers." https://www.finra.org/rules-guidance/key-topics/aml.

[13] See, for example, "Remarks by Under Secretary for Terrorism and Financial Intelligence John K. Hurley at the Association of Certified Anti-Money Laundering Specialists Assembly

Conference," U.S. Department of the Treasury (September 17, 2025), https://home.treasury.gov/news/press-releases/sb0251.

[14] "Tech Diplomacy 2040 Event Report: Tech Diplomacy is Now," Krach Institute for Tech Diplomacy (September 30, 2025), https://techdiplomacy.org/news/tech-diplomacy-2040-event-report-tech-diplomacy-is-now/ (delineating "how governments, industry, and academia can[,]" among other things, "[i]nstitutionalize tech proficiency across government and national security. . . [and] [s]cale trusted technologies through joint ventures, financing mechanisms, and cross-border R&D."

[15] "2024 National Strategy for Combating Terrorist and Other Illicit Financing," U.S. Department of the Treasury (May 2024), https://home.treasury.gov/system/files/136/2024-Illicit-Finance-Strategy.pdf.

[16] Martz, Drew, "North Korea Just Pulled Off The Biggest Heist In World History," Money Digest, (February 28, 2025), https://www.moneydigest.com/1801396/north-korea-worlds-biggest-heist/.

[17] Carpenter, Joby, "Leveraging national security priorities for an enhanced counter-fraud response, " ACAMS (July 30, 2025), https://www.acamstoday.org/leveraging-national-security-priorities-for-an-enhanced-counter-fraud-response/.

[18] Chainalysis, supra note 12.

[19] Mayer, Marina, "1 in 3 Companies Unprepared to Tackle National Security Compliance Risks: Study," Supply & Demand Chain Executive (October 2, 2025), https://www.sdcexec.com/safety-security/risk-compliance/news/22951604/eversheds-sutherland-1-in-3-companies-unprepared-to-tackle-national-security-compliance-risks-study.

[20] Ibid. According to the NSCRR Report, "84% of organizations report cybersecurity and data protection present moderate or high degrees of compliance risk for their organizations, but only 66% are 'very prepared' to address them today. U.S. organizations with international operations were more active across all areas of national security compliance over the past year compared to their U.S.-only counterparts, with notable disparities in economic sanctions and export controls (59% vs. 30%), anti-bribery and corruption (48% vs. 20%), and outbound investment screening (39% vs. 18%). Even though companies are deploying a range of tactics when it comes to mitigating or remediating national security compliance risks, many have opted not to increase board or executive oversight of these issues (72%), add budget to support compliance efforts (56%) or engage external legal or compliance advisors (55%)."

[21] "A $3.1 Trillion Financial Crime Epidemic," Nasdaq Verafin (February 5, 2024), https://verafin.com/2024/02/a-3-1-trillion-financial-crime-epidemic/.

[22] "AML Trends & Technology: Navigating the Future of AML in 2025,"Nasdaq Verafin (January 16, 2025), https://verafin.com/2025/01/aml-trends-technology-navigating-the-future-of-aml-in-2025/.

[23] The Multilateral Sanctions Monitoring Team (MSMT) reported that "[f]ollowing a heist, [Democratic People's Republic of Korea (DPRK)] hackers have been observed to use a variety of money laundering tools including cryptocurrency mixers, bridges, swaps, and decentralized exchanges to obfuscate the source of stolen funds and evade tracking by regulators. Once laundered, stolen assets are typically cashed out by DPRK-affiliated operatives overseas who use private brokers to convert the crypto assets into fiat currency." "The DPRK's Violation and Evasion of UN Sanctions through Cyber and Information Technology Worker Activities," Multilateral Sanctions Monitoring Team (October 22, 2025), https://msmt.info/Publications/detail/MSMT%20Report/4221.

[24] Rodriguez, Cesar Augusto, Timothy Charles Walton, and Hyong Chu, "Putting the 'FIL' into 'DIME'," JFQ 97 (2nd Quarter 2020), https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-97/jfq-97_121-128_Rodriguez-Walton-Chu.pdf.

[25] Examples of traditional sanctions evasion methods include: "shell companies and front companies; false documentation; transshipment; barter trade; use of Intermediaries. Digital currency sanctions evasion methods include: privacy coins (e.g., Monero, Zcash); mixers and tumblers; decentralized exchanges (DEXs); stablecoins (e.g., Ruble-backed A7A5); and cryptocurrency mining."

[26] According to TRM Labs, "since 2023, at least USD 47 billion in cryptocurrency has been sent to fraud-related addresses . . . Additionally, 2025 has been a record-setting year for hacks with over USD 2.3 billion stolen from the cryptocurrency ecosystem . . . Funds from the USD 1.5 billion Bybit hack earlier this year moved through over 10,000 transactions in the first month after the attack, triggering an urgent need for faster detection, response, and coordination across the crypto ecosystem." "TRM Labs Launches Beacon Network, the First Real-time Crypto Crime Response Network," TRM Labs (August 20, 2025), https://www.trmlabs.com/resources/blog/trm-labs-launches-beacon-network-the-first-real-time-crypto-crime-response-network.

[27] Office of Foreign Assets Control, "Frequently Asked Questions: Sanctions," U.S. Department of the Treasury, https://ofac.treasury.gov/faqs/all-faqs.

[28] "Financial Crime Enforcement Network ("FinCEN") regulations under Section 314(a) enable U.S. federal, state, local, and foreign (European Union) law enforcement agencies, through FinCEN, and FinCEN on its own behalf and on behalf of appropriate components of the U.S. Department of the Treasury, to reach out to U.S. financial institutions to locate accounts for, and recent transactions with, subjects—which may include persons or entities—that may be involved in terrorism or money laundering." https://fiportal.fincen.gov/.

[29] "AML Trends & Technology: Navigating the Future of AML in 2025," Nasdaq Verafin (January 16, 2025), https://www.verafin.com/2025/01/aml-trends-technology-navigating-the-future-of-aml-in-2025/.

[30] Velasco, Cristos et al., "Weaponizing Artificial Intelligence: How AI Reshapes the World of Organized Crime," EU Partnership on justice and security (October 2025), https://zenodo.org/records/17281249.

[31] "Great Power competition (GPC) is a framework for understanding global interstate relations that dominated global political affairs for centuries prior to World War II. Many past GPC eras have featured multiple powerful states jockeying for relative status and position. During the Cold War (1945–1991), GPC played out as a two-state competitive dyad between the United States and the Soviet Union. After lying dormant during a relatively short two-decade period of post–Cold War globalization and American international ascendance, the construct of GPC returned to the vocabulary of international relations and security studies in earnest during the late 2010s." Lynch, Thomas F. III, National Defense University Press (November 4, 2020), https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2404286/1-introduction/.

[32] Betti, Stefano, "Are geopolitical fractures jeopardising cross-border justice?" International Institute for Strategic Studies (September 11, 2025), Are geopolitical fractures jeopardising cross-border justice?

[33] "The Growing Landscape of Seizable Crypto Assets: On-Chain Balances Linked to Criminal Activity Exceed $75 Billion," Chainalysis (October 9, 2025), https://www.chainalysis.com/blog/landscape-of-seizable-crypto-assets-2025/.

[34] "Terrorist financing refers to the process of fundraising, through both licit and illicit means, and financially sustaining terrorist groups. Other illicit financial threats span a wide range of global concerns, including proliferation finance, tax evasion, sanctions evasion, and the financial facilitation of other state or nonstate threat actors." https://www.congress.gov/crs-product/IF11064.

[35] "Emerging Terrorist Financing Risks," Financial Action Task Force (October 2015), https://www.fatf-gafi.org/content/dam/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf, p. 5.

[36] "Comprehensive Update on Terrorist Financing Risks," Financial Action Task Force (July 8, 2025), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html.

[37] Ibid., p. 6.

[38] Ibid., p. 9.

[39] Ibid.

[40] Ibid.

[41] Ibid.

[42] Ibid.

[43] Effective February 20, 2025, the U.S. Designated Eight Cartels and Transnational Criminal Organizations (TCOs) as Foreign Terrorist Organizations (FTOs) and Specially Designated Global Terrorists (SDGTs). https://public-inspection.federalregister.gov/2025-02004.pdf. See also, https://www.justice.gov/ag/media/1388546/dl?inline, and https://www.state.gov/designation-of-international-cartels.

[44] "Comprehensive Update on Terrorist Financing Risks," Financial Action Task Force (July 8, 2025), https://www.fatf-gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html.

[45] "In conflict-affected contexts, widespread corruption, breakdown in the rule of law, limited government oversight and opportunities to infiltrate as well as collude with state-based actors all offer opportunities for different types of criminal actors to expand their economic ambitions through violent means. Many non-state armed groups profit from illicit activities to finance their armed struggle, gaining political power to 'protect and expand their economic rackets,' while in other situations, criminal organisations enter the formal political space." "States of Fragility 2025," OECD (2025), https://www.oecd.org/en/publications/2025/02/states-of-fragility-2025_c9080496.html, p. 78.

[46] Financial Action Task Force, Comprehensive Update on Terrorist Financing Risks (Paris: FATF, 8 July 2025), accessed 12 November 2025, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html?utm_source=chatgpt.com

[47] "Comprehensive Update on Terrorist Financing Risks," Financial Action Task Force (July 8, 2025), https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html, p. 8.

[48] Ibid. at p. 103.

[49] Financial Action Task Force (FATF). Comprehensive Update on Terrorist Financing Risks, 2025. Paris: FATF, July 8, 2025. Accessed November 12, 2025, https://www.fatf-

gafi.org/en/publications/Methodsandtrends/comprehensive-update-terrorist-financing-risks-2025.html

[50] Ibid.

[51] Ibid.

[52] "FATF, Egmont Group, INTERPOL and UNODC call for stronger co-operation between countries as they launch handbook to fight money laundering," FATF (September 5, 2025), https://www.fatf-gafi.org/en/publications/Methodsandtrends/international-cooperation-against-money-laundering.html.

[53] Ibid.

[54] Ibid.

[55] Presently, business entities dealing with Convertible Virtual Currency operate as money transmitters. As money transmitters, persons accepting and transmitting CVC are required, like any money transmitter, to register with FinCEN as Money Service Bureaus and comply with AML/CFT program, recordkeeping, and reporting requirements. These requirements apply equally to domestic and foreign-located CVC money transmitters doing business in whole or substantial part within the United States, even if the foreign-located entity has no physical presence in the United States. See "Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies," Financial Crimes Enforcement Network (May 9, 2019), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models; see also "Sanctions Compliance Guidance for the Virtual Currency Industry," Office of Foreign Assets Control (October 2021), https://ofac.treasury.gov/media/913571/download?inline.

[56] "Strengthening American Leadership in Digital Financial Technology," The White House (2025), https://www.whitehouse.gov/wp-content/uploads/2025/07/Digital-Assets-Report-EO14178.pdf.

[57] Ibid.

[58] "Comment Letter in response to Request for Comment on Innovative Methods To Detect Illicit Activity Involving Digital Assets, Document Number–2025-15697," Crypto Council for Innovation (October 17, 2025), https://cryptoforinnovation.org/wp-content/uploads/2025/10/59a1f6a1-715c-4dd9-accd-ebf205e31d42-TICKET.hs_file_upload-CCI-Comment-on-Treasury-RFC-on-AML-Innovation.pdf.

[59] Ibid.

[60] Pol, Ronald F., "The global war on money laundering is a failed experiment," The Conversation (October 21, 2019), https://www.theconversation.com/the-global-war-on-money-laundering-is-a-failed-experiment-125143. See also, Krecké, Elisabeth, "Why anti-money laundering policies are failing," GIS Reports (February 15, 2024), https://www.gisreportsonline.com/r/why-anti-money-laundering-policies-are-failing/.

[61] "Financial Stability Oversight Council," U.S. Department of the Treasury (accessed November 12, 2025), https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc.

[62] "2024 Annual Report," Financial Stability Oversight Council (December 6, 2024), https://home.treasury.gov/system/files/261/FSOC2024AnnualReport.pdf.

[63] "The 2023 Crony-Capitalism Index," The Economist (May 2, 2023), https://www.economist.com/international/2023/05/02/the-2023-crony-capitalism-index.

[64] "Fragile States Index Heat Map," The Fund for Peace (accessed November 12, 2025), https://fragilestatesindex.org/analytics/fsi-heat-map/.

[65] "The Basel AML Index is an independent ranking and risk assessment tool for money laundering and related financial crime risks" around the world. It provides risk scores for countries and jurisdictions based on data from 17 publicly available sources such as the Financial Action Task Force (FATF), Transparency International and the Global Initiative against Transnational Organized Crime. The risk scores cover five domains considered to contribute to a high money laundering risk: Quality of AML/CFT/CPF framework; Corruption and fraud risks; Financial transparency and standards; Public transparency and accountability; and Legal and political risks. The Basel AML Index is developed and maintained by the Basel Institute on Governance through its International Centre for Asset Recovery (ICAR). https://index.baselgovernance.org/ (accessed November 12, 2025).

[66] "Black and grey" lists," Financial Action Task Force (accessed November 12, 2025), https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html.

[67] "Mapping the Belt and Road Initiative: this is where we stand," Mercator Institute for China Studies (June 7, 2018), https://merics.org/en/tracker/mapping-belt-and-road-initiative-where-we-stand.

[68] The New York State Department of Financial Services (NYDFS) issued guidance explicitly extending expectations around the use of blockchain analytics tools by banking organizations in NY that are considering or already doing virtual currency-related business. The NYSDF emphasized that as more banks enter or expand virtual currency activity, their compliance programs must adapt to mitigate new or evolving risks. Specifically, NYDFS expects banking organizations to consider incorporating blockchain analytics as an additional risk management

tool that compliments and augments existing control programs. Some specific use cases it highlighted include: customer wallet screening and source of funds verification to assess risk exposure for customers with a material nexus to virtual currency activity and wealth; holistic monitoring for illicit activity exposure, including risk coming via third party transactional activity; and augmenting due diligence controls to compare expected vs. actual customer behavior (thresholds, volumes, etc.) for crypto activity. https://www.dfs.ny.gov/industry-guidance/industry-letters/il20250917-blockchain.

[69] "As global national security threats continue to grow in scale and sophistication, the United States must invest in resilient, future-ready technologies to protect its critical infrastructure. Best known for its role in cryptocurrencies, blockchain can also protect data integrity, increase transparency, and reduce centralized vulnerabilities in computing networks underpinning our critical infrastructure." "Blockchain and National Security: A Strategic Imperative," The Digital Chamber (July 2025), https://digitalchamber.org/national-security-report/, p. 4.

[70] "Founding members include Coinbase, Binance, PayPal, Robinhood, Stripe, Kraken, Ripple, Crypto.com, Zodia Custody, Blockchain.com, Anchorage Digital, Bitfinex, HTX, Poloniex, OKX, LFJ, 1inch, Rhino.fi, Coinspot, and ChangeNow, among others, creating an unprecedented level of industry collaboration to block off-ramps for criminal funds. Leading federal law enforcement agencies globally are actively contributing to the network, flagging addresses linked to critical threats and triggering alerts that help stop illicit actors before they can cash out. Security researchers and firms — including ZachXBT, Security Alliance (SEAL), zeroShadow, Hypernative, Operation Shamrock, and CryptoForensics Investigators — are providing continuous monitoring to identify and track threats." "TRM Labs Launches Beacon Network, the First Real-time Crypto Crime Response Network," TRM (August 20, 2025), https://www.trmlabs.com/resources/blog/trm-labs-launches-beacon-network-the-first-real-time-crypto-crime-response-network.

[71] Beacon operates as follows: "Flagging and propagation: Verified investigators flag addresses linked to financial crime. Beacon Network automatically propagates those labels across related wallets. Real-time alerts: When tagged funds arrive at a participating exchange or issuer, Beacon Network triggers an instant alert; Rapid response: Crypto platforms can proactively review and hold flagged deposits before withdrawal, stopping illicit cash-outs in their tracks; Accessible by design: Affiliate membership is free for verified exchanges and law enforcement partners." Ibid.

[72] See "Remarks by Under Secretary for Terrorism and Financial Intelligence John K. Hurley at the Association of Certified Anti-Money Laundering Specialists Assembly Conference," U.S. Department of the Treasury (September 17, 2025), https://home.treasury.gov/news/press-releases/sb0251.

[73] In 2022, the Center for a New American Security announced the launch of the CNAS Task Force to "develop pragmatic and innovative national security policy recommendations for the rapidly evolving ecosystem of financial technologies, crypto, digital assets, and decentralized

finance (DeFi) . . . [It] will define U.S. strategic interests and opportunities in pursuing leadership of this technology area, as well as advance the policy conversation for managing its unique risks." CNAS Task Force on FinTech, Crypto, and National Security.