GFMI
GLOBAL FINANCIAL MARKETS INSTITUTE

Article **2026**

The Seventh Domain of Warfare: Fighting Asymmetric Financial Warfare Against State and State-Supported Non-State Actors

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 wish to acknowledge the contributions of Babin Dinda, Senior Consultant in the Financial Services practice of FTI Consulting's Forensic & Litigation Consulting segment, to this article.

The Seventh Domain of Warfare: Fighting Asymmetric Financial Warfare Against State and State-Supported Non-State Actors

The Character and Nature of War

"Carl von Clausewitz's treatise 'On War' theorized that the nature of war, its essence and purpose, is unchanging within the human condition. By contrast, its character, the conduct of warfare, is in constant flux."[1] In defeating the Axis Powers during WWII, the United States (U.S.), and its Allies, through sustained, coordinated, effort, leveraged in varying degrees their industrial, financial, military, and civilian resources. Particularly of note was the ability of the U.S. to unleash its vast industrial resources to serve as "The Arsenal of Democracy"[2] in support of its allies — a truly public-private partnership. In containing[3] the Soviet Union during the Cold War, the U.S. utilized an integrated approach to engage the Soviet Union militarily,[4] economically, politically, and through "soft power" — the attractiveness of its society and values. Today's multidomain threats to U.S. national security require a reassessment of an approach to counter new and evolving challenges that affect the public and private sectors and require a coordinated approach.

The Six Domains of Warfare

The U.S. Army identifies five areas covered in multi-domain operations: land, air, maritime, space, and cyberspace. Potential U.S. adversaries are challenging these areas and competing for dominance across the multi-domain environment. Space and cyberspace operations are becoming increasingly important.[5] According to a report by the Atlantic Council, the private sector is the "sixth domain" of modern warfare, and the government needs to protect it.[6]

But there is another domain of warfare that has been developing for some time. Today, the war against illicit finance traditionally viewed through the prism of compliance and law enforcement has evolved into a type of asymmetrical warfare, as its actors are no longer isolated but part of institutionalized state and non-state actor activity, i.e., Crime-as-a-Service (CAAS).[7] This trend in illicit finance has been exacerbated by geopolitical instability, financial statecraft and great power conflict,[8] the increasing use of the digital asset ecosystem[9] in that conflict,[10] and artificial intelligence (AI) being used to widen the aperture for state and non-state actors to exploit.[11] Most recently, blockchain analytics show that cryptocurrency is helping to finance the drone revolution in the context of war. Specifically, commercially available drones are enabling state and non-state actors, such as pro-Russia militias and Iran-backed terrorist organizations, to project military power in a cost-effective manner. Drone procurement networks of state-backed actors increasingly intersect with the public blockchain, while comprehensively sanctioned states, such as Iran, are using cryptocurrency to solicit and procure strategic military hardware to further insulate its arms acquisition industry from Western-led sanctions.[12]

Trends in Terrorist Financing[13]

Terrorist financing (TF) has been treated as a separate category within anti-financial crime (AFC). Unlike anti-money laundering (AML), where illicit money is moved to disguise its illicit origins, TF generally begins with lawful proceeds being directed to unlawful purposes. In addition, risk detection for money laundering (ML)[14] generally begins with a financial institution (FI) identifying transaction typologies associated with specific customers. In contrast, for many TF cases the investigative starting point is not an unusual, anomalous transaction pattern but a named subject, an individual, or organization formally designated as a terrorist by state authorities, such as the Office of Foreign Assets Control (OFAC) within the U.S. Treasury Department.[15]

The Changing Character of Illicit Finance

The International Coalition Against Illicit Economies (ICAIE) issued its latest strategic intelligence report, "Criminals Accelerating Global Illicit Trade by Exploiting Digital Assets, Trade Finance Fraud, and other Emerging Transaction Laundering Schemes" (the "2026 ICAIE Report" or "ICAIE Report").[16] The report describes how newer schemes of ML and TF, particularly in the digital world, are helping to expand the global illegal economy.[17]

The 2026 ICAIE Report also highlights that within illicit economies, digital assets and transaction "value" schemes are being leveraged by bad actors and criminal networks to finance a global ecosystem of criminality and to launder dirty profits across the international trading system, digital markets, hubs of illicit trade, risky free trade zones (FTZs), and financial safe havens.[18] This allows nation-states to avoid or evade economic sanctions and export controls,[19] and to generate revenue for weapons programs and other threats to global national security.[20]

The 2026 Global Terrorism Index (Terrorism Index) notes that AI acts as a force multiplier across the entire terrorism ecosystem, as AI-generated propaganda systems produce news bulletins, memes, and content at scale.[21] Moreover, recruitment automation employs personalized chatbots engaging potential recruits continuously, with metaverse environments enabling immersive training simulations. The Terrorism Index also noted that financing facilitation through cryptocurrency mixing and automated ML reduces traceability.[22]

A worldwide network of trade, commerce, and illicit activities is thriving, with the selling and buying of legal and illicit goods and services taking place through electronic and digital payouts across online connections, global trading systems, e-commerce marketplaces, apps, social media, and encrypted channels.[23] Globalized trade and tariff disputes have also created new arbitrage opportunities for criminals across low-tariff markets, trans-shipment points, fraudulent schemes that misuse country of origin declarations, and trade-based money laundering (TBML) that uses cryptocurrency for payment settlement.[24] As international trade and commerce are further digitized, the evolution of today's payment systems has also altered the security landscapes used to detect and fight money laundering and financial crime, particularly as markets shift toward

digital currencies and a cashless economy where "value" becomes the operative payment method for transactions.[25]

Criminals have seized on globalization that exploits digital commerce to finance an international ecosystem of criminality and illicit trade that is siphoning trillions of dollars from legal economies.[26] This criminal activity frequently enables nation-states to fund other activities like programs to develop weapons of mass destruction (WMD) and terrorism.

Geopolitical Instability and Illicit Finance[27]

Geopolitical instability and armed conflict serve as a catalyst for funds moving into and out of the regions where the conflict occurs. While some of this financial flow may be legitimate, some is likely attributable to illicit activity used to fund the conflict. Given this trend, FIs should anticipate capital flight and respond by increasing sanctions screening, expanding beneficial ownership scrutiny, additional due diligence for entities at higher risk of sanctions evasion and enhancing monitoring across higher risk regions.[28] Governments should use suspicious activity reports (SARs) filed by FIs doing business in conflict regions to help identify funding of activities that implicate their national security.[29]

2026 United States' National Proliferation Financing Risk Assessment

As noted in the 2026 National Proliferation Financing Risk Assessment (the 2026 NPFRA), the U.S. faces an elevated threat from illicit actors seeking to finance the proliferation or use of biological, chemical, nuclear, or radiological weapons or related materials. Further, global efforts to develop adequate legal frameworks and implement effective controls are insufficient to combat the proliferation financing (PF) of WMDs. Moreover, the U.S. is exposed to a higher risk of WMD PF because of the size of its economy, international prominence of the U.S. dollar, and the industrial base that produces sensitive dual-use goods and items. As a result, the U.S. implements a whole-of-government approach to mitigate WMD PF risk, including when threats target the U.S. financial system directly or indirectly.[30]

The 2026 NPFRA highlighted two broad typologies relevant to PF: the abuse of the global technology ecosystem (Typology 1) and the use of ML techniques to support proliferation activities (Typology 2). Under Typology 1, the Democratic People's Republic of Korea (DPRK) remains focused on targeting the IT worker sector to generate revenue. Also, state and non-state actors continue to use digital assets to obscure and move funds.[31]

Under Typology 2, various threat actors are enlisting intermediaries and exploiting front/shell companies to evade sanctions and circumvent export controls.[32] The 2026 NPFRA is seeking to update the national understanding of WMD PF risk. The U.S. assesses that both state and non-state actors will accelerate efforts to probe for weaknesses in CPF regimes. Because of the rise of new technologies and uneven implementation of PF-targeted financial sanctions (TFS) globally, it is also crucial that the public and private sectors[33] collaborate to address vulnerabilities in counter

proliferation financing (CPF) controls and ensure sound AML/counter terrorist financing (CFT) frameworks allow for a proactive approach to anticipate emerging risks.[34]

National Security Responses Across Various Domains

Cyber

According to a report by the Center for Strategic and International Studies, the U.S. government has no hope of deterring, defending and responding to cyber threats unless it begins to integrate cyber offense and defense into its own national security strategy. The report notes that the 2025 National Security Strategy[35] mentions offensive cyber operations as part of a comprehensive U.S. government response capability.[36] Given its global reach and complexity,[37] we believe that this offensive posture should be extended to illicit finance actors in addition to other more traditional methods of addressing cyber security risks.[38]

Artificial Intelligence

As noted above, exacerbating these problems is the use of AI.[39] According to a TRM report entitled, "2026 Crypto Crime Report," (the 2026 Report or Report) AI-enabled scam activity increased by approximately 500% in 2025, with fraud that once required significant human intervention can now scale automatically, adapt immediately, and disperses proceeds before investigators can address.[40] The 2026 Report also notes that blockchain intelligence tools, e.g., network mapping, are reactive, confirming what has happened, but not proactive, and that the next phase of defensive AI shifts the focus proactively to detecting emerging infrastructure, disrupting networks before they scale, and operating continuously rather than on a case by case basis.[41]

Building and utilizing the capabilities[42] noted above responsibly, along with adequate privacy protections and human oversight, will determine whether AI becomes a sustainable advantage for compliance and enforcement or an increasing liability.[43]

Conclusion

In a financially connected, technologically sophisticated digital world, there are additional targets, different vulnerabilities, different risks, and different weapons we need to consider to keep our country and the world safe. The U.S. continues to evolve its current defenses and approach[44] to this new threat landscape, and its broader evolving financial statecraft response.[45] While deputizing the financial industry to be at the forefront of this new challenge presents issues, its vulnerability to evolving state threats necessitates rethinking its traditional compliance-proactive-reactive approach (e.g., customer onboarding and surveillance) to a more preemptive and disruptive one[46] as these threats are no longer limited to individual actors but sanctioned by countries that are in conflict with the U.S. Whether it be kinetic or hybrid, they all fall increasingly under the Seventh Domain of Warfare.[47]

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 CIArb 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] Scott, Michael, "Back to the Basics: Why the West Should Reconsider the Nature of War," Wild Blue Yonder Online Journal, (April 15, 2022), https://www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/2980403/back-to-the-basics-why-the-west-should-reconsider-the-nature-of-war/.

[2] See generally Herman, Arthur, (2013), "Freedom's Forge: How American Business Produced Victory in World War II," Random House.

[3] George F. Kennan, a U.S. diplomat, formulated the policy of "containment," the U. S. strategy for fighting the cold war (1947–1989) with the Soviet Union. Kennan's ideas, first came to public attention in 1947 through an anonymous contribution to the journal Foreign Affairs, referred to as the "X-Article." https://history.state.gov/milestones/1945-1952/kennan.

[4] National Security Council Paper NSC-68 (entitled "United States Objectives and Programs for National Security") was a report completed by the U.S. Department of State's Policy Planning Staff in 1950. It is among the most influential documents composed by the U.S. Government during the Cold War. Its authors argued that one of the most pressing threats confronting the U.S. was the "hostile design" of the Soviet Union. Its authors concluded that the Soviet threat would soon be augmented by the addition of more weapons, including nuclear weapons, to the Soviet arsenal. They argued that the best course of action was to respond in kind with a massive build-up of the U.S. military and its weaponry. https://history.state.gov/milestones/1945-1952/NSC68.

[5] Wright, Rebecca, "Multidomain Dominance," Army AL&T, (August 14, 2024), https://www.army.mil/article/279765/multidomain_dominance.

[6] Kramer, Franklin, "The sixth domain: The role of the private sector in warfare," Atlantic Council, (October 4, 2023), https://www.atlanticcouncil.org/in-depth-research-reports/report/the-sixth-domain-the-role-of-the-private-sector-in-warfare/.

[7] https://www.europol.europa.eu/iocta/2014/chap-3-1-view1.html.

[8] Miner, Urriolagoitia (Rio), "Financial crime implications of a US-Iran war: The emotional drivers of instability & illicit flows,", Thomson Reuters, (March 10, 2026), https://www.thomsonreuters.com/en-us/posts/corporates/us-iran-war-financial-crime-implications/.

[9] Threat finance: Cryptocurrencies, covert funds and advanced detection | ACAMS

[10] See OFAC Sanctions Crypto Addresses Associated with the Central Bank of Iran, Freezes USD 344 Million | TRM Blog and How Iran's Crypto Market is Reacting to Conflict | TRM Blog. See also Stablecoins at Scale: Broad Adoption and Highly Concentrated Illicit Networks | TRM Blog and https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report.

[11] Lieutenant General (ret.) Clint Hinote, US. AirForce, Major General (ret.) Mick Ryan, Australian Army, The Character of Future War to 2030, Defense Paper Series, Special Competitive Studies Project, DPS-The-Character-of-Future-War-to-2030-.pdf. See also Blazakis, Jason, "Terrorist Financing in the Age of Large Language Models," 11 February 2026, Published as part of Project CRAAFT, https://www.rusi.org/explore-our-research/publications/external-publications/terrorist-financing-age-large-language-models.

[12] "From the Battlefield to the Blockchain: How Cryptocurrency Is Helping Finance the Drone Revolution," Chainalysis Team, (March 30, 2026), https://www.chainalysis.com/blog/cryptocurrency-drones-research/.

[13] Mikhail Karataev, "Trends in Movements in Terrorist Financing," ACAMS, (March 18, 2026), https://www.acams.org/en/opinion/hybrid-movements-terrorist-financing.

[14] It is worth noting that FinCEN issued a proposed rule intended to reform financial institutions' AML/CFT programs under the BSA. The proposed rule supports the U.S. Treasury's efforts to modernize the U.S. AML/CFT regulatory and supervisory framework, and to reduce compliance burden. The proposed rule would promote risk-based, reasonably designed programs and greater consistency in how financial institutions are evaluated for effectiveness. The proposed rule refocuses compliance obligations and expectations on effectiveness by distinguishing between deficiencies resulting from program design and implementation; reinforces Treasury's view that financial institutions are best positioned to identify and evaluate their illicit finance risks; empowers financial institutions to devote more attention and resources toward higher risks rather than toward lower risks; clarifies expectations related to certain program requirements and functions, e.g., independent testing and audit functions, to ensure that examiners and auditors do not substitute their subjective judgment in place of financial institutions' risk-based and reasonably designed AML/CFT programs; and reiterates FinCEN's central role in AML/CFT supervision, including through the introduction of a notice and consultation framework between Federal banking supervisors and FinCEN with respect to significant AML/CFT supervisory actions. https://www.fincen.gov/news/news-releases/fincen-proposes-rule-fundamentally-reform-financial-institution-programs.

[15] Mikhail Karataev, "Trends in Movements in Terrorist Financing," ACAMS, (March 18, 2026), https://www.acams.org/en/opinion/hybrid-movements-terrorist-financing.

[16] ICAIE, "Criminals Accelerating Global Illicit Trade by Exploiting Digital Assets, Trade Finance Fraud, and other Emerging Transaction Laundering Schemes," (March 9, 2026), https://icaie.com/2026/03/criminals-accelerating-global-illicit-trade-by-exploiting-digital-assets-trade-finance-fraud-and-other-emerging-transaction-laundering-schemes/.

[17] The IMF estimates that international money laundering accounts for between 2-5% of world GDP (or up to $6 trillion based on the global economy – $117 trillion in GDP – in 2025). As this report notes, new forms of ML are rapidly escalating, such as those driven by artificial intelligence and cryptocurrencies. So, the actual magnitude of money laundering could be much greater than the generally accepted $6 trillion 2026 estimate, and that has cascading negative effects and critical domestic and international policy implications. https://icaie.com/2026/03/criminals-accelerating-global-illicit-trade-by-exploiting-digital-assets-trade-finance-fraud-and-other-emerging-transaction-laundering-schemes/.

[18] See supra note 16.

[19] LegalClarity, "How Does North Korea Make Money Despite Sanctions?" (August 30, 2025), https://legalclarity.org/how-does-north-korea-make-money-despite-sanctions/?utm_source=chatgpt.com.

[20] Coindoo, "North Korea Used Fake IT Workers to Steal $800M in Crypto," (March 13, 2026), https://coindoo.com/north-korea-used-fake-it-workers-to-steal-800m-in-crypto/?utm_source=chatgpt.com.

[21] Institute for Economics & Peace. Global Terrorism Index 2026: Measuring the impact of terrorism, Sydney, March 2026. https://www.visionofhumanity.org/wp-content/uploads/2026/03/Global-Terrorism-Index-2026-Report.pdf.

[22] Ibid.

[23] See supra note 16.

[24] Ibid.

[25] Ibid.

[26] Ibid.

[27] See supra note 8.

[28] Ibid.

[29] See supra note 15.

[30] Department of the Treasury, "2026 National Proliferation Financing Risk Assessment," (March 2026), https://business.cch.com/BFLD/Treasury-2026-National-Risk-Assessment-Proliferation-Financing-03062026.pdf.

[31] Ibid.

[32] Hybrid movements in terrorist financing refer to the deliberate organization and execution of interconnected funding pathways in which terrorist actors raise, move, store and deploy value through a combination of cryptocurrency, hawala and other informal value transfer systems, cash-based activity, trade-linked mechanisms, and access points within the regulated financial sector. As noted, in FATF risk assessments and the Financial Crimes Enforcement Network (FinCEN) advisories, such hybridization is strategic rather than incidental: It is designed to fragment financial visibility across channels, exploit regulatory and jurisdictional asymmetries, and sustain operations even when individual mechanisms are disrupted. Importantly, hybrid terrorist financing does not function outside the financial system, but through repeated, adaptive intersections with it creating detection challenges that cannot be addressed through channel-specific analysis alone. Mikhail Karataev, "Trends in Movements in Terrorist Financing," ACAMS, March 18, 2026, https://www.acams.org/en/opinion/hybrid-movements-terrorist-financing.

[33] See also FINRA's Financial Intelligence Fusion Center (FIFC) is a bi-directional intelligence sharing hub for FINRA and its member firms. The FIFC utilizes FINRA's expertise and knowledge gained from its oversight of the securities ecosystem and operates in collaboration with member firms to further protect investors and safeguard the integrity of U.S. capital markets. The FIFC collects, analyzes, and disseminates cybersecurity and fraud threat intelligence to member firms through a secure portal. Its goal is to share information quicker with member firms and disrupt frauds and cyberattacks before they grow. Its benefits for member firms include curated, actionable intelligence that is specific to the broker-dealer industry, https://www.finra.org/about/finra-forward/supporting-resilience/cybersecurity-fraud-prevention.

[34] See supra note 30.

[35] The U.S. Government's relationships with its private sector helps maintain surveillance of persistent threats to U.S. networks, including critical infrastructure. This enables the U.S. Government's ability to conduct real-time discovery, attribution, and response (i.e., network defense and offensive cyber operations) while protecting the competitiveness of the U.S. economy and bolstering the resilience of the U.S. technology sector. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

[36] Congressional testimony by Emily Harding, "U.S. Cyber Capabilities to Deter and Disrupt Malign Foreign Activity Targeting the Homeland," CSIS, (January 13, 2026), https://www.csis.org/analysis/us-cyber-capabilities-deter-and-disrupt-malign-foreign-activity-targeting-homeland.

[37] The 2026 INTERPOL Global Financial Fraud Threat Assessment (INTERPOL Assessment) warns that with increased global criminal collaboration, fraud is no longer a peripheral threat, it is at the center of polycriminality, intersecting with organized crime, human trafficking, and cybercrime. The INTERPOL Assessment notes that AI-enhanced fraud is 4.5 times more profitable than traditional methods. And that "Agentic AI" systems can autonomously plan and execute complete fraud campaigns — from reconnaissance to ransom demands. https://www.interpol.int/Media/Documents/Publications/Financial-Crime/INTERPOL-Global-Financial-Fraud-Threat-Assessment-March-2026.

[38] The U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection announced an initiative to strengthen cybersecurity throughout the digital asset industry. It will provide timely, actionable cybersecurity information to eligible U.S. digital asset firms and industry organizations, helping them better identify, prevent, and respond to cyber threats targeting their customers and networks. The initiative advances an important recommendation from the President's Working Group on Digital Asset Markets report, *Strengthening American Leadership in Digital Financial Technology*. Treasury Launches Cybersecurity Information Sharing Initiative for the Digital Asset Industry.

[39] According to a recent article published in Real Clear Defense, Secretary of State Rubio observed that U.S. security and prosperity are inextricably tied to the Western Hemisphere, with it even more true in the age of AI, where the global race for supremacy will be won or lost in in the U.S.' own backyard. To prevail, it must ensure that the Americas, from Canada to South America run on American AI and U.S.-aligned AI infrastructure. The Monroe Doctrine, which barred foreign powers from encroaching in the western hemisphere, is as relevant today as it was in the past. In this regard, If China supplies Latin America's AI infrastructure, it will not just sell cloud services, it will set the technical standards, lock in long-term revenue streams, and embed political leverage into the region's digital backbone. If the U.S. leads instead, it secures markets for its companies, reinforces a rules-based digital ecosystem, and anchors the western hemisphere's economic future in American innovation. This is not just a commercial competition; it is a contest that will determine the dominant superpower of the 21st century. Carl Meacham and Kai Golden, A Monroe Doctrine for AI, Real Clear Defense, March 31, 2026. https://www.realcleardefense.com/articles/2026/03/31/a_monroe_doctrine_for_ai_1173653.html?mc_cid=68d688d67f&mc_eid=9399af183f.

[40] "Predictive Blockchain Intelligence: What Defensive AI Will Look Like in Five Years," TRM Labs, (March 26, 2026), https://www.trmlabs.com/resources/blog/predictive-blockchain-intelligence-what-defensive-ai-will-look-like-in-five-years.

[41] Ibid.

[42] See also, "Operationalizing AI in Financial Compliance and Trade Surveillance," EVENTUS whitepaper, (April 2026), https://info.eventus.com/operationalize-ai-for-better-trade-surveillance.

[43] See also, The Office of the Financial Stability Oversight Council (FSOC) and the U.S. Treasury Department's Artificial Intelligence Transformation Office (AITO) announcement launching the AI Innovation Series- a public-private initiative to support the continued strength and resilience of the U.S. financial system in an era of accelerating technological change. FSOC and the Treasury noted that AI is increasingly embedded in core financial services functions, including fraud detection and cybersecurity to operational risk management. As adoption accelerates, regulators and institutions must ensure that governance, supervisory approaches, and market practices evolve alongside technological capability. The Treasury Department noted that it will continue evaluating regulatory frameworks and enforcement policies to enable the U.S. financial sector's leadership in AI adoption while preserving national security and long-term economic resilience." https://home.treasury.gov/news/press-releases/sb0421.

[44] See also a series of articles on how the U.S. can and should wield economic power to compete, coerce, and deter in an increasingly contested global order. It is the product of a joint effort by the Potomac Institute for Policy Studies and War on the Rocks. https://warontherocks.com/category/special-series/war-by-other-ledgers/.

[45] Skipper, Georgie, "Follow the Money: Finance and the Future of Allied Economic Statecraft," War on the Rocks, (March 25, 2026), https://warontherocks.com/follow-the-money-finance-and-the-future-of-allied-economic-statecraft/. See also The U.S.-China Economic and Security Review Commission's "COMPREHENSIVE LIST OF THE COMMISSION'S 2025 RECOMMENDATIONS" which includes establishing a consolidated economic statecraft entity to address the evolving national security challenges resulting from China's systematic and persistent evasion of U.S. export controls and sanctions. This new economic statecraft entity, at a minimum, would include: the Bureau of Industry and Security, the Office of Foreign Assets Control, the Bureau of International Security and Nonproliferation's Office of Export Control Cooperation, the Defense Technology Security Administration, and other appropriate organizations across the executive branch. https://www.uscc.gov/sites/default/files/2025-11/2025_Comprehensive_List_of_Recommendations.pdf.

[46] As noted recently, future battlefields will not be defined solely by kinetic force, but by data, financial flows, and the ability to disrupt financial ecosystems proactively and in real time. See Donovan, Ray, "The Shadow War Comes to Light: How Iran's Cartel-Terror Nexus Reached a Tipping Point, https://www.linkedin.com/pulse/shadow-war-comes-light-how-irans-cartel-terror-nexus-reached-donovan-lrrbe.

[47] Threat finance: Cryptocurrencies, covert funds and advanced detection | ACAMS.