AY 2024-2025

Strengthening Domestic and International Financial Capability to Support U.S. National Security Objectives

FINANCE INDUSTRY STUDY
GROUP PAPER

Professor William Jannace
COL Cory Young, JD, USA

SEMINAR 11

WORD COUNT: 8,291

May 13, 2025

The Dwight D. Eisenhower School for National Security and Resource Strategy
National Defense University
Fort McNair, Washington, D.C. 20319-5062

Contents

PREFACE

Seminar Members

John W. Keefe, Captain, U.S. Navy
Michael Miloszewski, Colonel, U.S. Air Force
Carter G. Deekens, Colonel, U.S. Army
Lorraine A. Foster, Colonel, Guyana Armed Forces
James S. Hirbo, Colonel, Kenyan Navy
Ramon Brigantti, Lieutenant Colonel, U.S. Army
John R. Fitzgerald, Lieutenant Colonel, U.S. Air Force
George E. Getman, Jr., Lieutenant Colonel, U.S. Marine Corps
Michael E. Ellis, Lieutenant Colonel, U.S. Air Force
Michael F. Capobianco, U.S. Agency for International Development
Shadrika Y. Witherspoon, Lieutenant Colonel, U.S. Army
Zachary J. Miller, Department of the Army
Richard R. Grimm, Defense Logistics Agency
Darren C. Woodside, Lieutenant Colonel, U.S. Air Force

Seminar Faculty

Professor William Jannace, Faculty, National Defense University
Cory Young, Colonel, U.S. Army
Professor Seth Weissman, Faculty, National Defense University
Russell Badowski, Colonel, U.S. Air Force

Field Studies Hosts and Seminar Guest Speakers

Jim Rosener – Partner, Troutman Pepper; Chairman, American Battle Monuments Foundation
Daniel N. Anziska- Partner, Troutman Pepper
Andrew Vrabel – Managing Director, CME Group
Owain Johnson – Managing Director, CME Group
Eric Aldrich – Executive Director, CME Group
Justin Durbin – Director, NYSE
Aditya Saharia – Professor, Information Systems and Director, Center for Digital Transformation Gabelli School of Business, Fordham University
Alex Shulman-Peleg – Managing Director, Ernst & Young LLP
Theodore Bunzel-Managing Director, Lazard Freres & Co. LLC
Senator Bill Bradley – Allen & Co.
Mike Brown – Partner, Shield Capital
Ernestine Fu – Founder, Brave Capital
Paul Madera – Co-Founder, Meritech Capital
Kevin McDonnell – CFO, AeroVironment
Scott Newbern – CTO, AeroVironment
Don Dixon – Managing Partner, Forgepoint Capital
Andrew McClure – Managing Director, Forgepoint Capital

Matt Ocko – Co-Founder & Managing Partner, DCVC
Alan Cohen – General Partner, DCVC
Clay Hutmacher – Operating Partner, DCVC
Earl Jones – Operating Partner, DCVC
Spencer Punter – Partner & COO, DCVC
Jeff Phaneuf – Chief of Staff, DCVC
AJ Bertone – Managing Partner, In-Q-Tel
Cullen Greenfield – Commander, USN, Defense Innovation Unit (DIU)
Justin Bernier – Executive, National Security Index (NSI)
Martin Wolf – Chief Economics Commentator, Financial Times
Sonya Branch – Executive Director, Bank of England
David Geen – Senior Technical Advisor, Bank of England
Byron McKinney – Product Management Director, S&P Global
John Neal – CEO, Lloyd's of London
James Hacket – Head of Defence & Military Analysis, International Institute for Strategic Studies
Huw Williams – Editor, International Institute for Strategic Studies
Karl Dewey – Research Associate, International Institute for Strategic Studies
Fenella McGerty – Senior Fellow, International Institute for Strategic Studies
Patrick Schneider – Sikorsky, Partner, NATO Innovation Fund
John Ridge – Chief Adoption Officer, NATO Innovation Fund
René van Vlerken – CEO, EURONEXT Amsterdam
Christine van den Bos – Listing Director, EURONEXT Amsterdam
Dirk Donker – Head of Secondary Markets, EURONEXT Amsterdam
Sébastien d'Herbès – Equity Listing Senior Manager, EURONEXT | Primary Markets
Dr. Jason Rathje (SES) – Director, Office of Strategic Capital, Department of Defense
Col Michael Murphy – Office of Strategic Capital, Department of Defense
Lt Col Connor Benedict – Office of Strategic Capital, Department of Defense
Juan Zarate- Global Co – Managing Partner and Chief Strategy Office, K2 Integrity
Elizabeth Severinovskaya – Managing Director, K2 Integrity
Katrine Steffensen – Senior Director, K2 Integrity
Maciej Makowski – Blockchain Analytics & Open-Source Intelligence Investigator, Coinbase
Hannah Clemens – Senior Consultant, Guide House

Distinguished Visitor Briefing Recipients

Alma Angotti, Senior Managing Director, FTI Consulting
Ylli Bajraktari, President and CEO, Special Competitive Studies Project.
J. Bradley Bennett, Former FINRA EVP-Managing Partner, Vernon's Gates Partners
Howard Herndon, Managing Director, Prescentus, LLC
Andrew Vrabel, Managing Director & Chief Regulatory Officer, Market Regulation Department CME Group
Major General (Ret.) William Walker, Vice President & Corporate Security Director, Allied Universal

Executive Summary

The finance industry is a large and intricate system of institutions and services (including banks, investment firms, and financial technology companies) that manage money, handle risk, and power economic activity. It is a cornerstone of the U.S. economy, facilitating capital formation, driving innovation, supporting job creation, and enabling economic growth across all sectors. The U.S. finance industry is also critical to national security because it allows the country to mobilize economic resources, fund defense initiatives, and exert geopolitical influence through financial mechanisms. This complex industry is undergoing rapid transformation, driven by technological disruption, market fragmentation and consolidation, interest rate sensitivity, the growing importance of nonbank financial institutions, and an evolving paradigm of assessing risks with an increasing focus on geopolitical and national security issues. These trends create vulnerabilities that demand examination of specific areas where disruption and strategic risk are concentrated.

The finance industry is characterized by intense competition and vulnerability to disruption. While traditional firms benefit from regulation and scale, technology, consumer empowerment, and new entrants are shifting the balance of power. At the same time, countries like China and Russia are using their financial systems to challenge the U.S. This combination of factors increases the risks to the U.S. financial system.

To address these issues, the report recommends:

- **Legislative Action:** Clarify digital asset regulation—distinguishing payment tokens, securities, and commodities—and enhance the Corporate Transparency Act (CTA) to restore comprehensive beneficial ownership disclosures.

- **Executive Measures:** Mandate the Department of Defense (DOD) blockchain logistics pilots; expand Cybersecurity and Infrastructure Security Agency's (CISA) resilience mandates; and streamline Committee on Foreign Investment in the United States (CFIUS) procedures to accommodate digital asset transactions while preserving security guardrails.
- **Public Private Partnerships:** Deepen co-investment through In-Q-Tel (IQT), Defense Innovation Unit (DIU), and allied venture initiatives; establish joint finance defense intelligence sharing forums.
- **Technological Modernization:** Deploy further artificial intelligence (AI)-driven Anti Money Laundering (AML) and anomaly detection; adopt International Organization of Standards (ISO) 20022 messaging standards for cross-border payments; codify digital asset security protocols.

The U.S. finance industry is a critical pillar of economic strength and national security, enabling innovation, capital formation, and global influence. However, it faces mounting risks from technological disruption, strategic competition, regulatory shifts, and geopolitical threats, particularly from rival financial systems like those of China and Russia. The U.S. financial system is a vital strategic asset that requires proactive measures to address emerging challenges and ensure its continued contribution to U.S. national security, economic strength, and global influence.

Introduction

In an era of accelerating technological innovation and intensifying great power competition, the U.S. finance industry stands at a strategic crossroads. As the primary allocator of capital, facilitator of complex global payments, and arbiter of financial risk, this sector is indispensable to defense procurement, logistics funding, and the enforcement of economic sanctions. Yet it also harbors latent vulnerabilities such as cyber threats, money laundering loopholes, and emerging asset classes that evade traditional oversight, that adversaries can exploit to undermine American economic and security interests.

This paper argues for a "scalpel, not cudgel" strategy: targeted regulatory refinements, precise technological defenses, and strategic investment vehicles that bolster points without stifling the innovation essential to dual-use defense technologies and global influence. Two analytical lenses guide this assessment: lines of effort (which informed some of the below policy recommendations) as well Porter's Five Forces. Porter's Five Forces reveals where financial technology firms (fintech) entrants, buyer power, crypto substitutes, supplier dependencies, and intense industry rivalry weaken or strengthen the financial ecosystem. A comparative review of rival systems, notably China's state capitalist banks and Russia's shadow finance networks, highlights how competitors weaponize finance through sanctions evasion, predatory investments, and covert funding.

Five domain studies illustrate both promise and peril. Cryptocurrency and blockchain can enhance supply chain visibility and enable micropayments in logistically challenging environments but also facilitate sanctions evasion and illicit finance. In cybersecurity, financial institutions face sophisticated threats from state-sponsored and criminal hackers; zero trust architectures, multi-factor authentication, and enhanced threat sharing under CISA offer

pathways to resilience. Money laundering analyses show how digital channels and informal networks undermine AML efforts, with implications for terrorist financing and intellectual property theft. Venture capital (VC) plays a crucial role in advancing dual-use technologies, yet structural barriers, long hardware cycles, and limited exit options hinder scale. Finally, foreign ownership and mergers reshape the defense industrial base: robust CFIUS scrutiny, transparent beneficial ownership reporting, and a potential U.S. sovereign wealth fund (SWF) can preserve strategic control over critical assets.

From these analyses there emerges a cohesive policy roadmap. Legislatively, Congress should clarify digital asset oversight and restore comprehensive beneficial ownership disclosures. From the Executive Branch, the DOD should continue pilots focused on blockchain logistics, and CISA's resilience mandates should be expanded. Public-private partnerships must be deepened through co-investment vehicles and intelligence sharing forums. Technological modernization, AI-driven AML analytics, and cross-border payment standards will further harden the system.

By combining precise regulation with innovation incentives, the U.S. can reinforce financial resilience, secure its economic and security interests, and retain its leadership in a contested global landscape.

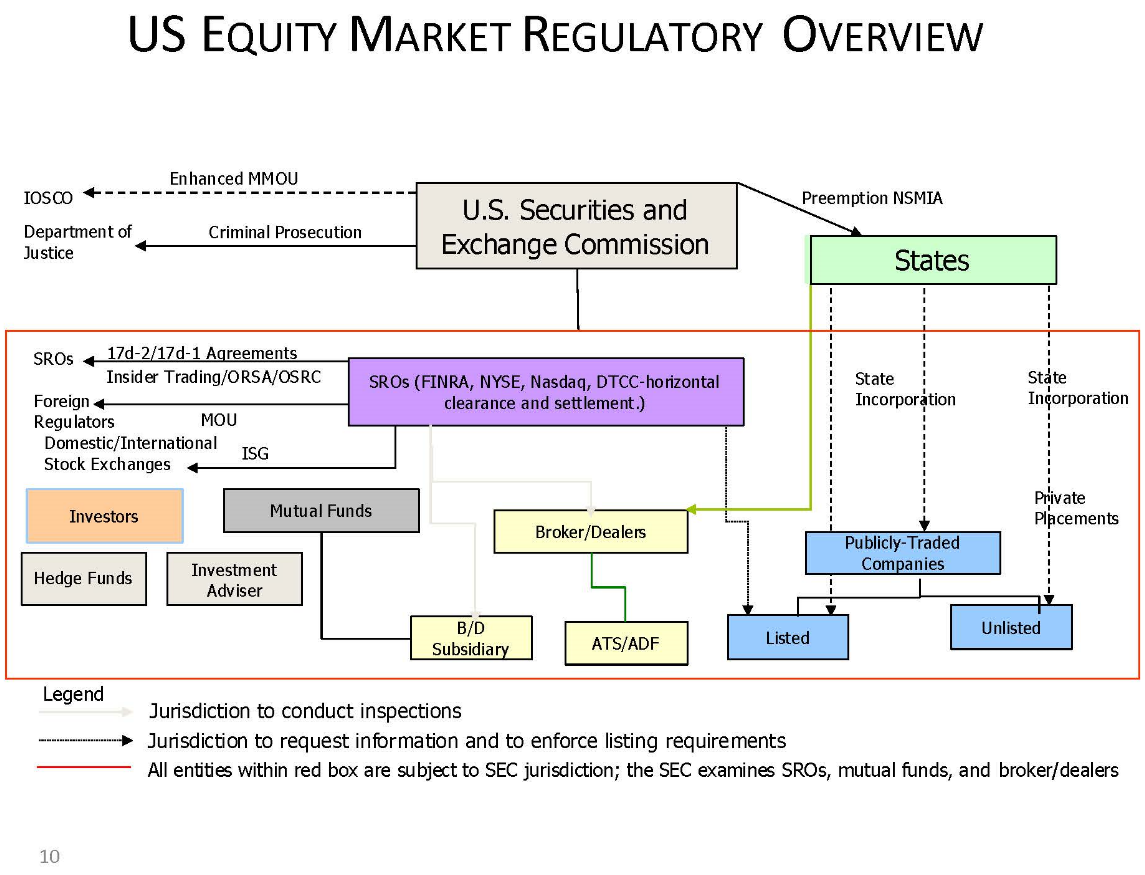
The Strategic Landscape

Before analyzing the finance industry, including why it is important to national security, and discussing the discrete topics of this paper, it is important to provide an overview of the strategic landscape. The finance industry encompasses a broad and complex ecosystem of institutions and services that facilitate the flow of capital, manage risk, and enable economic activity. It includes commercial banks, credit unions, investment firms (including investment advisers and broker-dealers), pension funds, fintech platforms, private equity (PE), hedge funds, and market infrastructure such as exchanges and clearinghouses. These entities collectively support credit intermediation, asset management, payment systems, and capital formation essential to national and global economic stability.[1] For the purposes of this paper, it excludes the insurance industries.

With its complexity, the finance industry is subject to scrupulous oversight by a fragmented system of regulators, both private and public (see below diagram displaying the regulatory scheme just for equities). Entities such as the Financial Industry Regulatory Authority (FINRA) require businesses to publish procedures and continuity planning to prepare for disruptions that would impacting the market, business health, and investors.[2] Additionally, the Securities and Exchange Commission (SEC) aims to ensure fairness and transparency for investors.[3] The Financial Stability Oversight Council (FSOC) serves as a mechanism to test, evaluate, and report on the financial industry's readiness and security.[4] CFIUS regulates foreign investment by ensuring companies factor in appropriate levels of risk relative to sensitive

[1] Office of Financial Research, *Annual Report 2024* (Washington, DC: U.S. Department of the Treasury, 2024), 5–6.
[2] "Business Continuity Planning (BCP) | FINRA.Org," accessed March 26, 2025, https://www.finra.org/rules-guidance/key-topics/business-continuity-planning.
[3] "The Role of the SEC | Investor.Gov," accessed April 29, 2025, https://www.investor.gov/introduction-investing/investing-basics/role-sec.
[4] "Financial Stability Oversight Council," U.S. Department of the Treasury, February 8, 2025, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc.

information and enforces compliance.[5] These are just some of the regulatory mechanisms that govern the finance industry.



10

Why the Finance Industry is Important to National Security

The U.S. finance industry underpins national security, providing a foundation for economic mobilization, defense spending, and preserving geopolitical influence. Financial institutions enable defense firm access to capital, execution of monetary policy, transactions essential for defense readiness and sustainment. Disruptions to this system, such as cyberattacks on clearinghouses or instability in markets, could impair defense financing and broader

[5] U. S. Government Accountability Office, "Foreign Investment in the U.S.: Efforts to Mitigate National Security Risks Can Be Strengthened | U.S. GAO," accessed February 3, 2025, https://www.gao.gov/products/gao-24-107358.

economic resilience.[6] U.S. control over global financial infrastructure allows the imposition of sanctions and disruption of adversary access to capital, bolstering deterrence.[7] The growing role of nonbank financial institutions and digital assets further expands this strategic domain, making financial system visibility and stability essential to national security.[8]

Broad Industry Trends

The finance industry is undergoing rapid structural and technological transformation marked by four dominant trends. First, technological disruption is reshaping every segment, from artificial intelligence (AI)-driven portfolio management to blockchain-based transactions, enhancing efficiency but increasing cybersecurity and operational risks.[9] Second, there is a clear trend of fragmentation and consolidation occurring simultaneously: while large firms consolidate through mergers and acquisitions (M&A) to build defensible moats, fintech and decentralized platforms are fragmenting traditional services.[10] Third, interest rate sensitivity is high across nearly all sectors, making them vulnerable to monetary policy shifts; sectors like commercial real estate lending and subprime consumer finance are especially exposed.[11] Fourth, nonbank financial institutions are gaining systemic importance but remain under-regulated and opaque, raising stability concerns.[12] These trends collectively signal an increasingly complex and interconnected financial system with evolving vulnerabilities.

---

[6] Office of Financial Research, *Annual Report 2024* (Washington, DC: U.S. Department of the Treasury, 2024), 29–31, 62–65.
[7] Office of Financial Research, *Annual Report 2024* (Washington, DC: U.S. Department of the Treasury, 2024), 23–25.
[8] Office of Financial Research, *Annual Report 2024* (Washington, DC: U.S. Department of the Treasury, 2024), 55–57, 69.
[9] Office of Financial Research, *Annual Report 2024* (Washington, DC: U.S. Department of the Treasury, 2024), 29–31.
[10] IBISWorld, *Portfolio Management and Investment Advice in the US*, April 2024, 10.
[11] Office of Financial Research, *Annual Report 2024*, 34–36.
[12] Ibid., 55–57.

Industry Analysis

As noted above, the U.S. finance industry plays a vital role in enabling economic growth, national security, and global competitiveness by facilitating capital allocation, risk management, and financial intermediation. The breadth of the industry requires the application of a comprehensive framework for effective analysis, e.g., Porter's Five Forces. Applying Porter's framework to assess the industry's competitive dynamics, structural pressures, and evolving threats allows for that analysis. The framework, detailed sector reports, and regulatory insights identify the key forces shaping the strategic landscape of finance and the implications for resilience, innovation, and systemic stability.

Threat of New Entrants – Moderate to High

While regulatory compliance and capital requirements create substantial barriers to entry, technology is eroding traditional protections. Fintech platforms, digital wallets, and decentralized finance initiatives have lowered costs of entry across payments, lending, and investment services.[13] Loan brokers and alternative lenders now compete with banks, with low market concentration in segments like loan administration and money transfers.[14] However, incumbents benefit from brand loyalty, regulatory relationships, and scale in compliance infrastructure.

Bargaining Power of Buyers – High

Buyers, whether individuals, businesses, or institutional investors, have increasing power due to transparency, digital comparability, and low switching costs. Mobile apps, online brokers, and robo-advisors allow users to shop across platforms for rates, fees, and services. In asset management, client sophistication, preference for low-cost exchange-traded funds, and passive

[13] Office of Financial Research, *Annual Report 2024* (Washington, DC: U.S. Department of the Treasury, 2024), 23–25.
[14] IBISWorld, *Loan Administration, Check Cashing & Other Services in the US Industry Report*, April 2024, 22.

strategies are reducing fees.[15] Similarly, institutional clients pressure custodians and fund managers for fee reductions and value-added analytics.[16]

Bargaining Power of Suppliers – Low to Moderate

Suppliers in finance are typically sources of capital (depositors, investors), data providers, and technology vendors. While depositors supply capital, their power is limited by Federal Deposit Insurance Corporation (FDIC) insurance and limited knowledge of alternatives. However, fintech enablers and cloud providers are gaining power.

Threat of Substitutes – High and Growing

The proliferation of fintechs, peer-to-peer (P2P) lending, crypto assets, and nonbank lenders presents growing substitute threats. Stablecoins and digital assets may supplant some aspects of money markets, while crowdfunding and private credit offer alternatives to bank loans.[17] In investment services, algorithmic trading and self-directed investing platforms allow individuals to bypass traditional full-service broker dealers.

Industry Rivalry – High

The finance industry is marked by intense rivalry across nearly all sectors. Price competition is fierce in retail banking, asset management, and insurance. (for example, BD industry due to leverage asset-management-buy-side has, i.e., Big Three Indexers, HFs order flow, etc.). Firms compete in technology, customer experience, and breadth of services. M&A activity is frequent, especially among asset managers, insurance firms, and credit

[15] IBISWorld, *Portfolio Management & Investment Advice in the US Industry Report*, April 2024, 11.
[16] IBISWorld, *Custody, Asset & Securities Services in the US Industry Report*, April 2024, 18.
[17] Office of Financial Research, *Annual Report 2024*, 23, 57.

intermediaries.[18] Additionally, nonbanks and fintech firms exert pressure on legacy players, raising capital efficiency and service expectations.[19]

Porters: Key Takeaways

The finance industry faces highly competitive intensity and rising vulnerability to disruption. While legacy firms maintain some defensive advantages through regulation and scale, technology, consumer empowerment, and nontraditional entrants are shifting the balance of power across all five forces.

Adversary Financial Systems

Analyzing the U.S. financial system provides a significant portion of the overall picture, but not the whole picture. That requires looking at the financial systems of U.S. adversaries and their respective impact on the U.S. system. The modern financial system faces mounting pressure from the rise of state capitalism, particularly as practiced by China and Russia.[20] These systems distort global financial markets by leveraging state-owned or state-controlled enterprises to achieve strategic goals, including access to capital, coercion of trading partners, and evasion of sanctions. In China, preferential lending from state-owned banks and the use of shadow banking channels advantage domestic firms and crowd out U.S. competitors.[21] In Russia, economic control is centralized under a leadership that rewards oligarchs aligned with regime goals, enabling sanctions evasion through alternative financial networks.[22] China's SWF, China Investment Corporation, plans to offload $1 billion in U.S. PE investments, a move driven by

[18] IBISWorld, *Private Equity, Hedge Funds & Investment Vehicles in the US Industry Report*, April 2024, 10.
[19] Office of Financial Research, *Annual Report 2024*, 57–59.
[20] Martin C. Spechler, "Defining State Capitalism," in *State Capitalism in Eurasia*, ed. Adam Dixon and Andrei V. Makarov (New York: Routledge, 2017), 1.
[21] Curtis J. Milhaupt and Wentong Zheng, "Beyond Ownership: State Capitalism and the Chinese Firm," *Georgetown Law Journal*, March 2015, 689–692.
[22] Daniel Satinsky, "Russia Back in Play? Lessons from business in 1990's Russia," March 14, 2025. Accessed April 15, 2025, https://russiapost.info/economy/90s_business

shifting geopolitical risk and a reassessment of overseas exposure. Like Russia's use of its National Wealth Fund to insulate its economy from Western sanctions, China's repositioning underscores how SWFs can serve as instruments of national strategy. Such distortions challenge core financial system functions—capital allocation, risk pricing, and transparency—while undermining global norms. The U.S. must enhance regulatory oversight, particularly through mechanisms like CFIUS and strengthen coordination with allies to mitigate the national security implications of these asymmetric financial behaviors. State-directed finance, when fused with geopolitical ambition, creates vulnerabilities in both economic and strategic domains that cannot be addressed solely through market competition.

Taken together, the finance industry's complexity, centrality to national security, and evolving structural trends underscore the urgency of examining specific topics where disruption and strategic risk are most concentrated. Cryptocurrency is a prime topic with which to start, followed by cybersecurity, money laundering, VC, and foreign ownership.

Cryptocurrency

Crypto and Digital Assets: Implications for National Security and Financial Strategy

The emergence of cryptocurrency and its underlying blockchain technology has initiated a transformative period for global finance and security. Characterized by decentralized structures, cryptographic safeguards, and reliance on distributed ledgers, these technologies present significant opportunities and profound challenges for individuals, institutions, and nation-states. Given their considerable growth potential, the integration of blockchain and

cryptocurrency into defense innovation and national security frameworks has become increasingly imperative.[23]

Blockchain for Secure Logistics

A novel application for blockchain technology in support of the defense industrial base (DIB) is supply chain visibility. A blockchain is an immutable, decentralized, and auditable digital ledger that offers immense value in tracking the movement of hundreds of components in complex supply chains.[24] Blockchain technology can revolutionize how DOD maintains supply chain integrity, particularly for exquisite munitions items. A Javelin missile, for instance, consists of over 250 microprocessors; a counterfeit part could compromise the system's effectiveness.[25] Blockchain registries can ensure the veracity of subcomponents, with manufacturers like Raytheon and Lockheed Martin maintaining visibility across the entire chain. From factory to battlefield, blockchain applications could provide cradle-to-grave asset visibility critical for operational planning and logistics. Each step in the manufacturing process could verify the authenticity of previous components, creating an immutable audit trail that enhances security and operational readiness.

Addressing intellectual property theft would be a side benefit of the cradle-to-grave visibility. As one European partner noted regarding the size of the issue, "Americans innovate, the Chinese duplicate, and the Europeans regulate," reflecting significant concerns over intellectual property theft.[26] The Federal Bureau of Investigation highlights intellectual property theft as a grave concern for academia, business, and national security, with estimates of losses

[23] "Convertible Virtual Currency: Meaning, Types, and Example," accessed April 16, 2025, https://www.finance4.net/convertible-virtual-currency/.
[24] "Crypto 101 Materials.Pdf," n.d.
[25] U.S. Army Acquisition Support Center, Javelin Weapon System, U.S. Department of the Army, accessed April 13, 2025, https://asc.army.mil/web/portfolio-item/ms-javelin/.
[26] Field Practicum. Author Observations and Interview Notes, Amsterdam, April 11, 2025., n.d.

ranging from $225 billion to $600 billion annually.[27] With secured logistics visibility, intellectual property theft could be mitigated for those component parts.

Cryptocurrency for Micropayments in Operational Environments

Cryptocurrencies are decentralized digital assets that rely on encryption and could revolutionize micropayments in immature theaters of war where central banks are unstable.[28] A tactical brigade in an austere environment could securely leverage cryptocurrency to procure local commodities. Using basic internet and digital wallets, local merchants could receive payments discreetly, minimizing risk in counterinsurgency environments where adversaries blend with civilian populations.[29] Reports estimate that at least 10% of logistic payments in Afghanistan went to insurgents, predating the broader use of digital assets in conflict zones.[30] In contrast, crypto donations exceeding $212 million have aided Ukraine during its conflict, showcasing digital transactions' transparent and auditable benefits.[31] More importantly, a secure digital transaction ledger ensures that taxpayer dollars are traceable and auditable, reinforcing public trust.

Threats from Cryptocurrency Exploitation

While offering benefits for secure logistics and micropayments, cryptocurrency also presents threats that adversaries may exploit. Features like transaction speed, borderless nature, irreversibility, and pseudonymity enable illicit activities, including cybercrime, sanctions

---

[27] "The China Threat," Folder, Federal Bureau of Investigation, accessed April 29, 2025, https://www.fbi.gov/investigate/counterintelligence/the-china-threat.
[28] Investopedia. "Explaining Crypto: What Is Cryptocurrency?" Accessed April 13, 2025.
[29] CoinMarketCap. "The Micropayment Economy: What It Is and Why It Matters." Academy. Accessed April 13, 2025. https://coinmarketcap.com/academy/article/the-micropayment-economy-what-it-is-and-why-it-matters.
[30] Clemente, Daniel. Afghanistan: The Logistics of Withdrawal. Chatham House, 2022. https://www.chathamhouse.org/sites/default/files/home/chatham/public_html/sites/default/files/afghanistan_clemente.pdf.
[31] World Economic Forum. "The Role Cryptocurrency Plays in Ukraine's War Effort." Accessed April 13, 2025. https://www.weforum.org/stories/2023/03/the-role-cryptocurrency-crypto-huge-in-ukraine-war-russia/.

evasion, and terrorism financing.[32] North Korea's Lazarus Group, for example, deployed ransomware globally, demanding Bitcoin payments, and has stolen cryptocurrencies to fund nuclear programs. Over the last few years, Lazarus Group and other North Korean cyber actors have stolen several billion dollars through cyberattacks aimed at bolstering their weapons programs.[33] Russia has leveraged stablecoins like Tether to bypass sanctions, while centralized exchanges remain vulnerable, as evidenced by the $1.46 billion Bybit heist attributed to North Korean actors.[34] These examples underscore the urgent need for robust security measures and policy interventions to mitigate the risks associated with cryptocurrency exploitation.

Shifting U.S. Policy

The current Administration recently announced an Executive Order prioritizing stablecoins and prohibiting the development of central bank digital currencies (CBDCs), signaling a strategic policy shift distinct from countries like China that are moving toward centralized digital currencies.[35] Stablecoins, cryptocurrencies pegged to reserve assets like fiat currencies, are critical to overcoming volatility and enabling broader, everyday use.[36] CBDCs are anathema to the decentralized philosophy underpinning cryptocurrency development.[37]

The shift toward stablecoins represents a balancing act between fostering innovation and preserving financial stability. However, ambiguity remains regarding regulatory jurisdiction.[38]

---

[32] K2 Integrity Crypto National Defense Considerations Briefing for Eisenhower School_Feb 6, 2025.Pdf," n.d.
[33] "Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies Phase II," n.d.
[34] Elliptic Research, "The Largest Theft in History - Following the Money Trail from the Bybit Hack," accessed April 29, 2025, https://www.elliptic.co/blog/bybit-hack-largest-in-history.
[35] The White House. Executive Order 14178: Strengthening American Leadership in Digital Financial Technology. January 23, 2025. The White House. https://www.whitehouse.gov/presidentialactions/
[36] "Stablecoins: Definition, How They Work, and Types," Investopedia, accessed April 17, 2025, https://www.investopedia.com/terms/s/stablecoin.asp..
[37] Brussels Diplomatic, The Digital Yuan Revolution: China's Bold Move Towards a New Financial Order, April 13, 2025, https://brusselsdiplomatic.com/the-digital-yuan-revolution/.
[38] U.S. Congress, S.954 – 119th Congress: To Establish a Framework for the Regulation of Digital Assets, introduced March 21, 2025, https://www.congress.gov/bill/119th-congress/senate-bill/954/text.

Agencies like the SEC and the Commodity Futures Trading Commission must further clarify and coordinate their roles and responsibilities to ensure a consistent regulatory framework.[39] Without clear guidelines, the risk of systemic financial vulnerabilities increases as tokenized assets gain broader acceptance in mainstream finance and commerce. The administration is signaling movement in that direction.

Financial Statecraft Risks

The increasing adoption of cryptocurrency and digital assets poses challenges to U.S. financial statecraft, particularly concerning dollarization vulnerabilities. Dollarization, using the USD as a primary currency in other countries, has long been a tool of U.S. economic and political influence.[40] However, the decentralized nature of cryptocurrency and the emergence of alternative digital currencies could erode the dollar's dominance, potentially diminishing the effectiveness of U.S. sanctions and other financial statecraft tools.[41] Rivals to the U.S. are considering the adoption of central-backed digital currencies as a way of introducing a rival to the USD's status as the reserve currency.[42] For example, China's development of the digital yuan may represent a strategic and functional challenge to the dollar's hegemony.[43] The digital yuan could enable cross-border transactions that bypass SWIFT and traditional payments systems that are influenced by the U.S. This would reduce the effectiveness of U.S. financial sanctions and could have far-reaching implications for global economic power dynamics, potentially reducing reliance on the dollar in international trade and finance. However, the digital yuan has limitations due to it not being fully convertible, and China's capital account remaining closed, thus

[39] Ibid.
[40] "De-Dollarization: The End of Dollar Dominance? | J.P. Morgan," accessed April 30, 2025, https://www.jpmorgan.com/insights/global-research/currencies/de-dollarization.
[41] Ibid.
[42] Brussels Diplomatic, The Digital Yuan Revolution: China's Bold Move Towards a New Financial Order, April 13, 2025, https://brusselsdiplomatic.com/the-digital-yuan-revolution/.
[43] Ibid.

restricting the flow of capital in and out of the country. Even though there are limitations, the ability of adversaries to use cryptocurrencies to evade sanctions and conduct illicit transactions further complicates the U.S. efforts to exert financial pressure and maintain its strategic advantage. Preserving dollar primacy will require innovative financial strategies incorporating digital assets while safeguarding U.S. economic influence**.**

Cryptocurrency: Key Takeaways

Cryptocurrency and blockchain technologies offer significant opportunities for innovation in defense logistics and financial transactions. However, adversaries exploit vulnerabilities through cyber theft and efforts to undermine dollar dominance. A balanced regulatory approach is needed to mitigate risks while enabling the strategic advantages these technologies can provide. The Administration's initial policy signals are positive; it is now incumbent on Congress and executive agencies to provide more statutory clarity to secure America's economic and security future. With prudent policy actions and strategic investments, the U.S. can harness the full potential of blockchain and cryptocurrency technologies while safeguarding its national interests.

Cybersecurity

Cybersecurity represents another topic that is critical to the finance industry, especially given the growing power of fintech firms and AI platforms. Cybersecurity is a broad term and for the purposes of this paper is used interchangeably with cyberfraud, cybercrimes, and cyber threats. Oversight and regulatory agencies are in place to prevent cyberfraud, the deliberate exploitation of digital platforms and technologies to commit fraud and related crimes that

undermine financial integrity, operational efficiency, and consumer confidence.[44] Cyberfraud covers a wide range of illicit activities, which include identity theft, phishing schemes, online bank fraud, the manipulation of stock markets, and the disruption of supply chains.[45] With the financial sector deeply intertwined with national defense, playing a fundamental role in funding and facilitating transactions, the resulting transactions make the financial industry a prime target for hackers and others with malicious intent.[46]

[44] "Cyber Fraud - Everything You Need to Know," DataDome, accessed April 17, 2025, https://datadome.co/guides/cyberfraud/what-it-is/.
[45] Aamir Lakhani, "Cyber Fraud Examples: What Threat Actors Are Doing Today | Fortinet," Fortinet Blog, February 15, 2021, https://www.fortinet.com/blog/industry-trends/why-threat-actors-continue-to-rely-on-cyber-fraud.
[46] Couplet travel. Gabelli Business School, 7 March, 2025

Business Continuity Plans, Rule 4370, and FSOC

Although many cybersecurity threats are impacting the financial industry, both FINRA and FSOC are working to mitigate these threats across the finance industry. FINRA has instituted regulatory rule 4370 for firms to establish business continuity plans that must be communicated in writing to respond effectively to unexpected disruptions or crises. FINRA provided recommendations to financial firms earlier this year to include increased training involving phishing, monitoring sites for imposter domains, increased identity verification, and subdividing networks.[47] Cybersecurity is a key focus for FINRA as attacks and intrusions are increasingly becoming more complex with the use of generative AI and cybercrime as a service. FINRA, supplementing SEC oversight, is central to the cash and equities regulatory system of the U.S. It works with other self-regulatory organizations (subject to SEC oversight) to oversee markets and support its infrastructure Its assessment of firms includes technology governance, controls, access, response to crisis, training effectiveness, and data loss mitigation measures.[48] The FSOC is an agency that assesses activity in the financial industry and reports current, emerging, and key threats to consumers, markets, and businesses to identify, mitigate, and assess the long-term impacts.[49] It also assesses the risks and benefits of third-party service providers once firms abdicate to an outside entity.[50]

Notable Attacks / Threats

Despite the work of these organizations, notable attacks are increasing. Cybercrimes are often conducted by international organizations or state actors, which include Russia, North

[47] Aaron Cheema, "Key takeaways from the 2025 FINRA Annual Regulatory Oversight Report," IQ-EQ, February 3, 2025, https://iqeq.com/insights/key-takeaways-from-the-2025-finra-annual-regulatory-oversight-report/.
[48] "Cybersecurity | FINRA.Org," accessed March 26, 2025, https://www.finra.org/rules-guidance/key-topics/cybersecurity.

Korea, and Iran. This crime costs the financial industry billions of dollars and directly relates to national security, as adversaries sometimes use the money for weapon systems and terrorist activity.[51] Additionally, Russia has a proven record of increasing cybercrimes as a response mechanism to actions such as sanctions, which occurred in response to the beginning of the Russia-Ukraine war of 2022.[52] In 2016, state-sponsored hackers (later identified as North Korea's Lazarus Group) broke into the Bangladesh Bank and sent fraudulent commands through the SWIFT system to steal $951 million from the bank's account at the New York Federal Reserve. Most of the fraudulent transactions were stopped in time, but $81 million was channeled to fund North Korea's weapons program.[53] In 2018, criminals targeted DOD vendors in a phishing and payment diversion scam where $23.5 million in payments that should have gone to DOD contractors were funneled into a shell company's bank accounts.[54]

Recent major cyberattacks have targeted financial institutions with connections to the defense sector. These include sophisticated supply chain compromises, social engineering campaigns against personnel with dual financial-defense responsibilities, and ransomware attacks against payment processors handling defense contractor transactions. One notable case documented by the Financial Crimes Enforcement Network, which is a bureau within the U.S.

---

[49] "Financial Stability Oversight Council." https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc

[50] Finextra, "Financial Stability Oversight Council Annual Report Identifies Threats and Vulnerablities," Finextra Research, December 9, 2024, https://www.finextra.com/pressarticle/103506/financial-stability-oversight-council-annual-report-identifies-threats-and-vulnerablities.

[51] "North Korean Hackers Steal Record $1.5 Billion in Single Crypto Hack, Security Firm Says | CNN Politics," accessed February 28, 2025, https://www.cnn.com/2025/02/24/politics/north-korean-hackers-crypto-hack/index.html.

[52] Charles Gasparino, "Russian Cyber Attacks against US Banks Increasing," March 2, 2022, https://nypost.com/2022/03/01/russian-cyber-attacks-against-us-banks-increasing/

[53] "Treasury Sanctions North Korean State-Sponsored Malicious Cyber Groups," U.S. Department of the Treasury, February 8, 2025, https://home.treasury.gov/news/press-releases/sm774.

[54] "Man Convicted in Phishing Scam That Cost U.S. DoD $23.5M," Decipher, May 2, 2022, https://duo.com/decipher/man-convicted-in-usd23-5m-phishing-scheme-against-u-s-DoD.

Department of Treasury shows malicious actors using generative AI to create false identities, opening financial accounts that were later used to launder the proceeds of other schemes targeting defense procurement systems.[55]

Methods to Counter Cyber Threats

There are several methods to counter the cyber threats to the financial industry, which include the following: multi-factor authentication, education, training, audits, encryption, verification, monitoring, lateral movement, zero trust security models, updates and patch management, and incident response plans. These methods focus on protecting digital assets and maintaining business operations and customer information.[56]

In addition to the conventional countermeasures to cyber threats in the financial industry, machine learning models are rapidly emerging as a solution to advancing cyber threats by predicting risks through understanding and learning from data and recognizing anomalies and patterns. These machine learning models are also very efficient in spotting intrusion techniques for bad actors already on the network and those who are planning to do so. There are drawbacks, which point to difficult implementation, interpretation, and bad actors attempting to attack the machine learning model itself.[57]

Another way to counter these threats is increasing collaboration with defense-related government bodies and allies. The Cybersecurity Information Sharing Act (CISA) serves as a crucial coordinator in the government for the protection of critical infrastructure, including the

[55] "FinCEN.Gov," FinCEN.gov, November 13, 2024, https://www.fincen.gov/news/news-releases/fincen-issues-alert-fraud-schemes-involving-deepfake-media-targeting-financial.
[56] "Cyber Security in Finance: Key Threats and Strategies," SentinelOne, accessed March 3, 2025, https://www.sentinelone.com/cybersecurity-101/cybersecurity/cyber-security-in-finance/.
[57] William Clement Aaron et al., "Machine Learning Techniques for Enhancing Security in Financial Technology Systems," International Journal of Science and Research Archive 13, no. 1 (2024): 2805–22, https://doi.org/10.30574/ijsra.2024.13.1.1965.

finance industry and the DIB.[58] It also provides legal protections for private companies that wish to share threat intelligence with the government and other private companies.[59] The DOD Cybersecurity Maturity Model Certification (CMMC) is another example and is used for rating cybersecurity in defense contractors.[60] Another example is the Federal Financial Institutions Examination Council provides guidelines for cybersecurity in the nation's financial institutions.[61] Finally, joint cyber exercises held yearly in Europe and the US, bring together several federal agencies in a series of war games using real-life scenarios and serve as a prime example of collaboration.[62]

Cybersecurity: Key Takeaways

The financial industry is in a strong position regarding the regulatory framework, oversight, and adaptation of machine learning technology to adapt to emerging and persistent cyber threats. The industry faces many threats related to the protection of individual data in the financial sector, increasing technical capability in cybercrime, and the emergence of complexities with bad actors integrating with nation-state actions. It is a critical time for oversight infrastructure like FINRA, SEC, FSOC, and CFIUS to be on high alert to prevent bad actors from succeeding by continuing to innovate on cybersecurity countermeasures. This is coupled with a continuous willingness to adjust to changing requirements.

[58] "What Is the Cybersecurity Information Sharing Act (CISA)?," What Is, accessed April 20, 2025, https://www.techtarget.com/whatis/definition/Cybersecurity-Information-Sharing-Act-CISA.
[59] "Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities under the Cybersecurity Information Sharing Act of 2015 | CISA," January 14, 2025,
[60] "About CMMC," accessed April 20, 2025, https://DoDcio.defense.gov/cmmc/About/.
[61] "Home | FFIEC," accessed April 20, 2025, https://www.ffiec.gov/.
[62] FS-ISAC, "FS-ISAC Represents Global Financial Sector in Cyber Defense Exercise Locked Shields," accessed April 20, 2025, https://www.fsisac.com/newsroom/pr-lockedshields-2024.

Money Laundering

Converging Threats in Financial Crime and National Security

Money laundering, the process of disguising illicit funds to make them appear legitimate remains a cornerstone of global financial crime and a persistent enabler of transnational threats.[63] While AML frameworks, including Know Your Customer (KYC) customer due diligence (CDD) and suspicious activity reporting (SAR), are designed to detect and disrupt these activities, they are increasingly challenged by the complex realities of a digitized, decentralized, and adversarial financial environment. Regulatory gaps in cross-border banking, commercial real estate (CRE), fintech ecosystems, and geopolitical hotspots are being exploited by hostile actors. The traditional boundaries between financial crime, terrorism financing, and geopolitical conflict have dissolved, giving rise to a converged threat environment where financial institutions serve not just as regulatory gatekeepers, but as frontline detectors of activity tied to national security, radicalization, and asymmetric warfare.

Financial Crime, Radicalization, and Lone-Actor Threats

With boundaries dissolving, as highlighted in the February 2025 Association of AML Specialists National Capital Chapter briefing, a growing number of plots in the U.S. and Europe are tied to online radicalization and ideologically motivated lone actors. These individuals often use hard-to-detect, low-cost financial tools such as P2P apps, prepaid gift cards, virtual currency, and encrypted messaging.[64] The January 1, 2025, New Orleans car-ramming attack exemplifies this trend. The perpetrator, radicalized online, used decentralized tools to fund and coordinate the attack evading detection by systems with static thresholds and rule-based monitoring. These

[63] Financial Action Task Force, International Standards on Combating Money Laundering (2023), 12.
[64] Dennis M. Lormel, Touchpoints between Geopolitics and Terrorism in 2025, presentation at the ACAMS U.S. Capital Chapter Webinar, February 18, 2025 (Washington, DC: ACAMS, 2025), 10-11, 19,23.

microtransactions highlight the need for behavioral analytics, geolocation tagging, and integrated data systems to identify high-risk activity.[65]

Conflict Zones and Informal Financial Networks

Conflict zones such as Syria and Gaza further complicate AML enforcement. These regions generate illicit financial activity involving humanitarian aid diversion, arms smuggling, and terrorism financing. Militant factions rely on hawala networks (informal, unregulated systems for transferring money), shell nonprofits, and diaspora remittances to evade sanctions. Syria-based actors have routed funds through weakly regulated jurisdictions, while the 2024–2025 conflict in Gaza triggered a surge in financial flows to politically aligned groups using crypto and front companies. Such shadow financial ecosystems blend licit and illicit activity, overwhelming outdated compliance infrastructure.[66]

Commercial Real Estate: Strategic Laundering Risks

CRE has emerged as a high-risk conduit for illicit finance due to its high transaction values, layered ownership structures, and subjective valuations which make it ideal for laundering large sums. Nearly 47% of properties near U.S. defense contractors lack clear beneficial ownership, and foreign-linked acquisitions are 3.7 times more likely to cluster near military sites.[67] One such attempt, blocked by CFIUS in 2024, sought to acquire property adjacent to a San Diego naval lab.[68]

Valuation manipulation is also widespread. In Dallas, a cartel-linked property was inflated by $34 million to obscure laundering. Cross-border CRE financing exacerbates opacity,

[65] Dennis M. Lormel, Touchpoints between Geopolitics and Terrorism in 2025, presentation at the ACAMS U.S. Capital Chapter Webinar, February 18, 2025 (Washington, DC: ACAMS, 2025), 9-11.
[66] Ibid, 20-21, 29.
[67] U.S. Attorney's Office, "Dallas Real Estate Fraud Case," March 2023.
[68] U.S. Department of the Treasury, "CFIUS Blocks San Diego Acquisition," November 1, 2024.

as multi-jurisdictional deals generate 62% fewer SARs than domestic cash transactions.[69] In one case, Sefira Capital moved $50 million through offshore lenders, avoiding scrutiny. These patterns suggest adversaries are targeting CRE to gain proximity to defense assets, obscure ownership, and apply financial leverage.[70]

National Security Risks to the DIB

AML gaps now pose a direct threat to the DIB through four critical vectors. First, proximity enablement involves foreign-controlled entities acquiring commercial CRE near military installations to conduct surveillance or exert influence.[71] Second, supply chain infiltration occurs when adversaries covertly acquire ownership stakes in defense suppliers, potentially compromising sensitive technologies and components.[72] Third, technology transfer risks arise when adversarial actors acquire defense-related tech firms or properties, enabling unauthorized access to controlled technologies.[73] Lastly, financial leverage is exploited through complex debt and financing structures, allowing foreign investors to pressure financially vulnerable subcontractors and manipulate strategic assets within the DIB. CFIUS reviews of more than 60 military-linked sites have flagged such risks, highlighting the national security consequences of financial opacity.[74] These mechanisms transform economic assets into strategic vulnerabilities. To safeguard against these threats, robust regulation with continuous review systems and aggressive mandatory implementation is necessary for all CRE property near national strategic facilities.

[69] U.S. Attorney's Office, "Dallas Real Estate Fraud Case," March 2023.
[70] U.S. Department of Justice, "Arizona Subcontractor Charged," May 15, 2022.
[71] U.S. Department of the Treasury, "CFIUS Blocks San Diego Acquisition," November 1, 2024.
[72] U.S. Department of Justice, "Arizona Subcontractor Charged," May 15, 2022.
[73] Hudson Rock, "Hack of Defense Contractors," February 21, 2025.
[74] Committee on Foreign Investment in the U.S., 2024 Annual Report, 45–48.

Fintech and BaaS: A Compliance Lag

The rapid expansion of fintech, particularly Banking-as-a-Service (BaaS) platforms has introduced additional vulnerabilities. BaaS is a financial industry concept that refers to the delivery of banking and financial services through a third-party platform. Essentially, BaaS providers allow non-banks, such as fintech companies, startups, and others, to leverage the infrastructure and capabilities of traditional banks to provide various financial services to their own customers without having to hold a full banking license themselves.

While this expands financial access, many sponsor-fintech relationships lack sufficient oversight. Castellum.AI's 2024 *BaaS Compliance Guide* found widespread failures in transaction monitoring, onboarding, and compliance role definition. Many digital-native firms, firms that were created in the digital age, have an innate understanding of digital technology, and have built their infrastructure using digital technologies, prioritize growth over compliance and lack infrastructure for real-time KYC, sanctions screening, or behavioral analytics. Sponsor banks remain legally responsible but often have limited visibility into fintech operations. Without embedded compliance tools and vendor governance, these platforms risk becoming conduits for illicit finance.[75]

Beneficial Ownership Information Loopholes and the Corporate Transparency Act Rollback

Further weakening the AML regime, the Treasury's 2025 interim revision to the CTA rolled back beneficial ownership reporting requirements for most U.S. entities. While foreign entities remain covered, many domestic firms are now exempt from reopening the door to anonymous shell companies and obstructing law enforcement efforts. The Financial

[75] Jonathan Patterson, BaaS Compliance Guide 2024 (New York: Castellum.AI, 2024), https://www.castellum.ai, 3-8.

Accountability and Corporate Transparency Coalition criticized the move, warning it undermines the CTA's original goals and facilitates the concealment of illicit funds, raising concerns that are also addressed further below. In response, some states such as New York, California, Maryland, South Dakota, and the District of Columbia have introduced and or enacted their own beneficial ownership information reporting requirements, but this fragmented response risks inconsistent enforcement, regulatory arbitrage, and diminished national oversight.[76] The sector calls for more resources to ensure continuous and vigorous enforcement and mandatory compliance.

Technology Modernization: Promise and Constraints

To respond to these escalating risks, many institutions are investing in technology modernization. AI, real-time analytics, and ISO 20022 messaging standards are central to this effort. ISO 20022 improves cross-border payment transparency through standardized, data-rich transaction messages. Large banks are aligning with the G20's 2027 roadmap for ISO adoption, but smaller institutions face implementation hurdles.[77] AI is being deployed to enhance risk modeling and reduce false positives. However, challenges remain around algorithm transparency, regulatory acceptance, and funding. Alessa's 2025 AML Trends Report noted that while nearly 50% of firms plan to use AI, only 45% of compliance professionals believe their budgets are sufficient to meet AML objectives. Smaller banks and fintechs remain particularly constrained.[78] Financial institutions can be incentivized to resource mitigations measures and invest in research and development (R&D) for software systems and remain a head of threat.

[76] The FACT Coalition, "Treasury Reopens the Floodgates to Dirty Money in the U.S.," March 3, 2025, https://thefactcoalition.org/treasury-reopens-the-floodgates-to-dirty-money-cta/
[77] Finextra Research, Cross-Border Payments: How Is the Market Addressing G20 Targets? (London: Finextra Research Ltd, 2025), https://www.finextra.com.
[78] Alessa, 2025 AML Trends Report (Ottawa: Alessa, 2025), https://www.alessa.com, 44.

Money Laundering: Key Takeaways

In today's threat landscape, AML, and counter-financing of terrorism (CFT), efforts must evolve. Financial institutions are no longer compliance intermediaries; they are frontline defenders of national security. The convergence of financial crime, terrorism financing, and geopolitical subversion demands an integrated, technology-driven response aligned with U.S. defense priorities. Illicit finance now spans traditional banking, fintech, and decentralized crypto systems. From sanctions evasion to lone-actor terrorism funded through digital channels, adversaries are exploiting regulatory blind spots. While regulators have made strides in enforcement and cross-border compliance, setbacks such as the rollback of CTA provisions threaten to reverse progress. Static rule-based systems are no longer sufficient; dynamic, intelligence-led frameworks are essential.

Venture Capital

The partnership between government and VC across the valleys of death from seed to production has rapidly grown domestically and internationally. VC's unique combination of risk tolerance, market discipline, and agile decision-making complements traditional financing pathways. A reinvigorated defense tech VC market is a true asset for national security. By harnessing the power of the VC market, the DOD, and North Atlantic Treaty Organization (NATO) can accelerate the development and deployment of innovative capabilities.

VC nurtures a culture of entrepreneurship and risk-taking, providing the necessary fuel for the engine of innovation. The Defense Advanced Research Projects Agency R&D "opened the funding floodgates" for America's fledgling VC industry.[79] In 1960, U.S. defense-related

[79] Martin Kenney, "How Venture Capital Became a Component of the U.S. National System of Innovation," *Industrial and Corporate Change* 20, no. 6 (December 2011): 1677–1723, https://academic.oup.com/icc/article-abstract/20/6/1677/883660.

R&D alone accounted for 36% global R&D.[80] After the "Last Supper" in 1993, the federal government became less reliable as a source of R&D funding, and companies needed to raise capital through private means. By 2019, DOD accounted for only 3.1% of global R&D investment.[81] Corporate R&D now comprises over 70% of total U.S. R&D spending.[82] Conversely, VC firms have steadily grown, investing $215 billion into domestic startups in 2024 alone, comprising nearly 60 percent of global venture investment.[83]

Defense Tech Venture Market

Early VC investors soured on the defense industry in the 1960s as long-cycle times and low volumes tilted investment and innovation toward the commercial sector.[84] However, defense technology has recently experienced a venture renaissance, partly due to several firms delivering significant profits for investors. There are multiple other reasons why defense technology startups have become popular VC investments, including rising geopolitical tensions, government innovation, and affordability narratives becoming more mainstream, and increasing overlap between commercial and defense technologies.[85] [86] [87] More VCs are mentioning defense technology than ever before, as one leading firm remarked that they have "never seen more

[80] John F. Sargent Jr., *The Global Research and Development Landscape and Implications for the Department of Defense*, CRS Report No. R45403 (Washington, DC: Congressional Research Service, November 8, 2018), https://www.congress.gov/crs-product/R45403.
[81] Ibid.
[82] Michael Brown et al., "Integration for Innovation," *Center for a New American Security*, September 2024, 3, https://www.cnas.org/publications/reports/integration-for-innovation.
[83] Marc Cadieux and Mark Gallagher, "State of the Markets: Innovation Economy Outlook, H12025," *Silicon Valley Bank*, 16, https://www.svb.com/trends-insights/reports/state-of-the-markets-report/.
[84] Martin Kenney, "How Venture Capital Became a Component of the U.S. National System of Innovation," *Industrial and Corporate Change* 20, no. 6 (December 2011): 1677–1723, https://academic.oup.com/icc/article-abstract/20/6/1677/883660.
[85] Jai Das et al., "Silicon Valley Meets The Department of Defense: Top Observations & Opportunities in Defense Tech," *Sapphire Ventures*, February 8, 2024, https://sapphireventures.com/blog/silicon-valley-meets-the-department-of-defense-top-observations-opportunities-in-defense-tech/.
[86] Leah Hodgson, "Appetite Wanes for VC defense-Tech Deals," *Pitchbook*, August 13, 2024, https://pitchbook.com/news/reports/2024-vertical-snapshot-defense-tech-update.
[87] Michael Sion et al., "M&A in Aerospace & Defense: How Incumbents Can Respond to Well-Funded Disrupters," *Bain & Company*, February 04, 2025, 29, https://www.bain.com/insights/aerospace-and-defense-m-and-a-report-2025/.

entrepreneurs want to be in national security."[88] The U.S. is now home to 15 active defense technology "unicorns," each with a valuation of over $1 billion and a cumulative value of more than $50 billion.[89] According to *Pitchbook*, these segments of defense technology are expected to grow at an impressive 15.9 percent compound annual growth rate over the next 2-3 years, generating above-average returns.[90]

Government programs still have a VC-like role to play. The Small Business Innovative Research (SBIR) program complements government R&D as the primary government program providing capital for small businesses and startups to spur technological innovation.[91] DOD alone contributes over half of the $4.4 billion annual SBIR budget.[92] However, only 16 percent of DOD-funded SBIR companies successfully transition, leading many venture firms to disregard SBIR grants as a demand signal for additional private investment.[93] [94]

New government organizations have been created to increase SBIR success rates and leverage private investment. For over 25 years, the Intelligence Community's venture arm, IQT, has made investments, which signal to private investors of a high potential for future government contract revenue.[95] Every dollar IQT invests in a startup has led to an additional $18 in private

[88] Interview with Shield Capital, March 31, 2025.
[89] Silicon Valley Bank (SVB), "H1 2025: State of the Markets Report" (Silicon Valley Bank, n.d.).
[90] Jai Das et al., "Silicon Valley Meets The Department of Defense: Top Observations & Opportunities in Defense Tech," *Sapphire Ventures*, February 8, 2024, https://sapphireventures.com/blog/silicon-valley-meets-the-department-of-defense-top-observations-opportunities-in-defense-tech/.
[91] Michael Brown, "How Federal Programs Affect Venture Capital Investment In Tech," *Forbes* November 17, 2024, https://www.forbes.com/sites/mikebrown/2024/11/17/how-federal-programs-effect-venture-capital-investment/.
[92] Amanda Bresler and Alex Bresler, "Assessing the Effectiveness of Defense-Sponsored Innovation Programs as a Means of Accelerating the Adoption of Innovation Force Wide," in *Twentieth Annual Acquisition Research Symposium* (Naval Postgraduate School, April 30, 2023), 271.
[93] "Defense Innovation Board. "Terraforming the Valley of Death." *Department of Defense*, July 20, 2023, 3. https://innovation.defense.gov/Portals/63/DIB_Terraforming%20the%20Valley%20of%20Death_230717_1.pdf
[94] *Hearings on Fostering American Innovation: Insights into SBIR/STTR Programs, Before the House Committee on Small Business, 119th Cong.* (February 26, 2025) (statement of Jere W. Glover, Executive Director, Small Business Technology Council).
[95] Michael Brown, "How Federal Programs Affect Venture Capital Investment In Tech," *Forbes* November 17, 2024, https://www.forbes.com/sites/mikebrown/2024/11/17/how-federal-programs-effect-venture-capital-investment/.

investment.[96] More recently, DIU was created in 2015 to focus on prototyping and fielding dual-use technologies.[97] The DIU partners with government entities, awarding prototype contracts averaging $2-5 million to companies with promising dual-use commercial capabilities.[98] Dual-use technologies reduce the risk of fragmented government investment and uncertain product-market fit, providing an exit opportunity in defense or commercial markets.[99] Each dollar of awarded prototype contract value generates 10-20 times the amount in additional equity capital and can increase valuations by two to five times.[100] Both IQT and DIU investments lead to transition rates of approximately 50%, much greater than SBIR success.[101] [102] Building off the venture success of DIU, the Office of Strategic Capital (OSC) was recently created in December 2022 to leverage strategic investments in critical supply chain technologies through loans and loan guarantees.[103]

The DOD must increasingly leverage the American private VC market to maintain its competitive edge and rapidly field transformative technologies. Public-private partnerships effectively direct venture investment into key dual-use promising tech areas that can benefit the DOD. These partnerships provide reliable demand signals that allow VC investors to take calculated risks.

---

[96] Geo Saba, "Investing in Defense: How an In-Q-Tel for DoD Can Help America Win the New Technology Race," in *On the Rise: Perspectives on Foreign Policy – Class of 2022*, ed. Aspen Institute (Washington, DC: Aspen Institute, 2022), 15–16, https://www.aspeninstitute.org/wp-content/uploads/2022/12/Investing-in-Defense.pdf.
[97] Defense Innovation Board. "Terraforming the Valley of Death." *Department of Defense*, July 20, 2023. https://innovation.defense.gov/Portals/63/DIB_Terraforming%20the%20Valley%20of%20Death_230717_1.pdf
[98] Dan Berkenstock and Helen Phillips, "The Defense Tech Playbook," *Hoover Institution*, February 19, 2025, 26, https://www.hoover.org/research/defense-tech-playbook.
[99] Michael Sion et al., "Rethinking Defense: The Role of Private Capital," *Bain and Company*, December 2024, https://www.bain.com/insights/rethinking-defense-the-role-of-private-capital/.
[100] Michael Brown, "How Federal Programs Affect Venture Capital Investment In Tech," *Forbes* November 17, 2024, https://www.forbes.com/sites/mikebrown/2024/11/17/how-federal-programs-effect-venture-capital-investment/.
[101] In-Q-Tel, "How We Work," accessed April 16, 2025, https://www.iqt.org/how-we-work/.
[102] Defense Innovation Unit, *FY23 Annual Report*, accessed April 17, 2025, https://www.diu.mil/fy23.
[103] Marcy E. Gallo, "The Defense Innovation Ecosystem," *Congressional Research Service*, January 8, 2025, https://www.congress.gov/crs-product/IF12869.

International Venture Capital Markets

The VC markets in Europe and China paint a different picture than that of the U.S. In Europe, VC-backed defense technology investment hit an all-time high of $625 million in 2024.[104] VC investment overall in Europe is only around one-third of U.S. levels, with a significant portion of those funds invested by American investors.[105] [106] A substantial percentage of European start-ups struggle to secure late-stage funding from domestic investors due partly to a European bias toward low-risk savings, with greater than 30 percent of household savings held in low-yield deposits rather than market-based investments.[107]

New government organizations have been created in Europe to leverage public-private partnerships and team with private investment. The NATO Innovation Fund (NIF) was launched in August 2023 with a primary objective to support start-ups, small and medium-sized enterprises (SMEs), and midcaps actively developing deep tech dual-use technologies.[108] NIF's initial €1 billion funding round is backed by NATO member states and is focused on investments in "deep technology" across nine emerging technology sectors.[109] The fund's initial investments

---

[104] Chris Metinko, "As US Defense Tech Surges, Europe Lags," *Crunchbase News*, April 2, 2025, https://news.crunchbase.com/defense-tech/us-venture-surges-europe-lags-anduril-helsing/.
[105] Christine Lagarde, "Follow the Money: Channelling Savings into Investment and Innovation in Europe," Speech at the 34th European Banking Congress, Frankfurt am Main, November 22, 2024, https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp241122~fb84170883.en.html
[106] Gené Teare, "European Venture in 2023 Halved from Peak, but Was Still Above Pre-Pandemic Funding," VC investment overall in Europe is only around one-third of US levels.[1]
Crunchbase News, January 9, 2024, https://news.crunchbase.com/venture/european-funding-share-eoy-2023/.
[107] Christine Lagarde, "Follow the Money: Channelling Savings into Investment and Innovation in Europe," Speech at the 34th European Banking Congress, Frankfurt am Main, November 22, 2024, https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp241122~fb84170883.en.html
[108] "EIF and NATO Innovation Fund Sign MoU to Mobilize Private Capital for Europe's Defence and Security Future," VCWire, July 3, 2024, https://vcwire.tech/2024/07/03/eif-and-nato-innovation-fund-sign-mou-to-mobilize-private-capital-for-europes-defence-and-security-future/
[109] "NATO Innovation Fund: About," NATO Innovation Fund, accessed April 20, 2025, https://www.nif.fund/about/

are to be deployed over fifteen years.[110] This pool of capital is provided by the SWFs and other vehicles of the twenty-four backing states.[111]

The Defense Innovation Accelerator for the North Atlantic (DIANA) acts as an accelerator, identifying and nurturing early-stage deep tech companies through hosting competitive industry challenges, inviting innovators to develop dual-use technologies, like DIU. DIANA enables development across nine emerging and disruptive technologies, awarding non-dilutive grants and granting access to accelerator sites, test centers, mentors, and a network of trusted investors.[112] Technologies developed through DIANA's programs may become eligible for NIF funding.[113] DIANA acceleration efforts and NIF investment focus on dual-use technology in the same nine emerging sectors.[114]

The European Investment Bank (EIB) and its European Investment Fund (EIF) are leveraging NATO's efforts towards reducing risk. EIF's central mission is to support Europe's SMEs by helping them access sources of capital. The EIB can only invest in dual-use technologies, limiting defense tech investment opportunities for European firms. Therefore, a multi-faceted approach combining the targeted investment of the NIF, the catalytic role of the EIF in mobilizing private capital, and the strategic alignment with defense needs positions the NIF as an effective instrument to address specific shortcomings within European capital markets.

[110] "Emerging and Disruptive Technologies," NATO, accessed April 20, 2025, https://www.nato.int/cps/fr/natohq/topics_184303.htm?selectedLocale=en
[111] "NATO Innovation Fund: About," NATO Innovation Fund, accessed April 20, 2025, https://www.nif.fund/about/
[112] Defence Innovation Accelerator for the North Atlantic (DIANA)," NATO, accessed April 20, 2025, https://www.nato.int/cps/en/natohq/topics_216199.htm.
[113] Ibid.
[114] John Henry Ridge, Chief Adoption Officer, NATO Innovation Fund, In-person conversation, April 9, 2025

China, the world's second-largest economy and America's pacing national security challenge, only saw $33.2 billion in VC investment in 2023.[115] This represented the lowest amount of VC investment in China since 2013.[116] Some market observers have noted that China is experiencing a "venture capital collapse."[117] A leading factor in driving this decline is the withdrawal of American VC into the Chinese economy. New American regulations and the perception of increased financial and geopolitical risks amongst investors have led to a sharp decline in American VC financing. American VC firms only invested $3.93 billion into China in 2023, a dramatic reduction from $24.80 billion in 2021.[118] One observer described the decline of American VC investment into China as "This isn't just about decoupling. It is about dying."[119]

Venture Capital Challenges

While there is significant momentum with public-private partnerships in defense tech startups, risks from a slowing initial public offering (IPO) market threaten to limit further venture defense tech investments. These risks are enhanced for middle and late-stage defense technology startups that require higher amounts of invested capital in later funding rounds. Only 25 percent of U.S. tech unicorns currently meet standard IPO financial criteria to go public and

[115] Chris Metinko, "China Leads Asia's Venture Downturn — But Other Countries Didn't Help," *Crunchbase News*, January 27, 2025, https://news.crunchbase.com/venture/china-leads-asia-downturn-ai-ev-data-centers/.
[116] Joyce Guevarra, Annie Sabater, and Karl Angelo Vidal, "US-Backed Funding Rounds in China Fall to Lowest in a Decade," *S&P Global Market Intelligence*, June 6, 2024, https://www.spglobal.com/market-intelligence/en/news-insights/articles/2024/6/us-backed-funding-rounds-in-china-fall-to-lowest-in-a-decade-81822765.
[117] Dan Primack, "China's Venture Capital Collapse," *Axios*, September 19, 2024, https://www.axios.com/2024/09/19/china-venture-capital-collapse.
[118] Joyce Guevarra, Annie Sabater, and Karl Angelo Vidal, "US-Backed Funding Rounds in China Fall to Lowest in a Decade," *S&P Global Market Intelligence*, June 6, 2024, https://www.spglobal.com/market-intelligence/en/news-insights/articles/2024/6/us-backed-funding-rounds-in-china-fall-to-lowest-in-a-decade-81822765.
[119] Dan Primack, "China's Venture Capital Collapse," *Axios*, September 19, 2024, https://www.axios.com/2024/09/19/china-venture-capital-collapse.

IPO listings dropped to the lowest amount in a decade in 2024.[120] [121] The National Venture Capital Association reported that American VC firms ended 2023 with an estimated $328 billion of "dry powder" awaiting investment, primarily delaying investment due to quiet IPO markets.[122]

Hardware-focused defense startups generally require more capital and have longer commercialization investment horizons, which generates more risk and longer timelines for exits.[123] According to data from *Pitchbook*, the average hardware-focused startup requires $200 million in capital to scale effectively.[124] Inconsistent government demand and funding are the most often cited challenges to defense technology startups, especially amongst companies with four times larger capital requirements than other less-capital-intensive sectors.[125]

Venture Capital: Key Takeaways

VC has reemerged as a vital partner in accelerating defense innovation, with public-private partnerships like DIU and IQT driving high-impact investments in dual-use technologies. However, challenges such as inconsistent government demand and a constrained IPO market threaten the long-term scalability of defense tech startups, especially those with capital-intensive business models.

---

[120] Marc Cadieux and Mark Gallagher, "State of the Markets: Innovation Economy Outlook, H12025," *Silicon Valley Bank*, 32, https://www.svb.com/trends-insights/reports/state-of-the-markets-report/.
[121] Nick Candy et al., "Innovation Economy Update." *JP Morgan Chase*, January 30, 2025, 17, https://www.jpmorgan.com/insights/outlook/economic-outlook/innovation-economy-outlook; *2025 Yearbook*, National Venture Capital Association (March 2025): 24, https://nvca.org/nvca-yearbook/.*2025 Yearbook*, National Venture Capital Association (March 2025): 24, https://nvca.org/nvca-yearbook/.
[122] Nick Candy et al., "Innovation Economy Update." *JP Morgan Chase*, January 30, 2025, 14, https://www.jpmorgan.com/insights/outlook/economic-outlook/innovation-economy-outlook
[123] Michael Brown, "How Federal Programs Affect Venture Capital Investment In Tech," *Forbes* November 17, 2024, https://www.forbes.com/sites/mikebrown/2024/11/17/how-federal-programs-effect-venture-capital-investment/.
[124] Dan Berkenstock and Helen Phillips, "The Defense Tech Playbook," *Hoover Institution*, February 19, 2025, 26, https://www.hoover.org/research/defense-tech-playbook.
[125] Marc Cadieux and Mark Gallagher, "State of the Markets: Innovation Economy Outlook, H12025," *Silicon Valley Bank*, 22, https://www.svb.com/trends-insights/reports/state-of-the-markets-report/.

Financial Strategy for Sustaining U.S. Power

As this paper has noted throughout, financial markets have evolved into critical arenas for strategic competition. The U.S., which has historically benefited from dynamic capital markets and robust legal and innovation ecosystems, must now adapt its economic strategies to harness capital as a strategic instrument of national power proactively. To that end, a forward-looking strategy must integrate M&A, foreign direct investment (FDI), sovereign wealth initiatives, and innovative financing schemes such as third-party litigation finance (TPLF) into a cohesive framework that safeguards economic and national security.

Examining the first of these components, the contemporary landscape of M&A reveals a complex interplay between opportunities and vulnerabilities within national security contexts. M&A activities have increasingly transitioned from purely financial mechanisms to strategic operations that determine control over essential technologies, supply chains, and defense capabilities. Post-Cold War consolidation in the defense sector has streamlined efficiencies, enabling significant cost reductions, resource optimizations, and strategic packaging and scaling of emerging technologies and innovations.[126] As the principal driver of consolidation, M&A activity plays a critical role by injecting capital, expertise, and operational efficiencies necessary for rapid growth, scale-up, and market penetration of technologies essential to defense and security. However, these same consolidations have also introduced vulnerabilities, creating potential single points of failure and dampening incentives for innovation. Market volatility exacerbates these pressures, as fluctuating valuations and uncertain financial environments can

[126] U.S. Government Accountability Office, *Defense Industrial Base: DOD Needs Better Insight into Risks from Mergers and Acquisitions*, GAO-24-106129 (Washington, DC: U.S. Government Accountability Office, October 2023), https://www.gao.gov/assets/gao-24-106129.pdf.

incentivize quicker exits and profit-taking.[127] VC and PE firms act as accelerators of defense industrial change—but without the right governance and incentives, they can just as easily accelerate challenges, especially with M&A involving foreign entities.[128] Addressing these challenges necessitates stringent oversight mechanisms, such as enhanced CFIUS screening, comprehensive outbound investment controls, and rigorous transparency mandates, to align private financial activities with overarching national security priorities.[129]

Beyond M&A, strategic FDI represents another crucial vector through which capital flows shape the defense industrial base—often mitigating the shortcomings that M&A-driven consolidation can create. FDI, particularly from allied nations like South Korea, provides a critical complement to U.S. VC and PE by filling structural gaps in long-term capital-intensive sectors that are vital to the DIB.[130] Whereas traditional American VC and PE firms often prioritize high-growth, asset-light models with shorter time horizons, foreign firms are more willing to invest in physical infrastructure and expand the U.S. manufacturing workforce.[131] For example, South Korea's Hanwha Group's investment in the Philadelphia Shipyard illustrates how foreign ownership of domestic manufacturing facilities can effectively address strategic

[127] Harvard Law Review. "Mergers and Acquisitions—What Awaits in 2025?" *Harvard Law School Forum on Corporate Governance*, January 22, 2025. https://corpgov.law.harvard.edu/2025/01/22/mergers-and-acquisitions-what-awaits-in-2025/#:~:text=M%26A%20activity%20shows%20optimistic%20signs,deals%20are%20not%20getting%20easier.
[128] Skadden, *Mapping the National Security Landscape for Investors*, January 2025.
[129] U.S. Government Accountability Office, *Defense Industrial Base: DOD Needs Better Insight into Risks from Mergers and Acquisitions*, GAO-24-106129 (Washington, DC: U.S. Government Accountability Office, October 2023), https://www.gao.gov/assets/gao-24-106129.pdf.
[130] Nick Wilson, "Del Toro: U.S. shipbuilding stands to benefit from foreign investment," *Inside Defense*, April 18, 2025, HYPERLINK "https://insidedefense.com/share/220433"https://insidedefense.com/share/220433.
[131] Jensen Touissaint, "New Owner of Philly Shipyard, Hanwha, Wants to Push 'Boundaries of Shipbuilding'," *Philadelphia Today*, January 2025, https://www.msn.com/en-us/money/executive-leadership-and-management/new-owner-of-philly-shipyard-hanwha-wants-to-push-boundaries-of-shipbuilding/ar-AA1wzj68?ocid=BingNewsSerp.

industrial needs, grow labor force capacity and enhance vital skills, and stimulate significant economic activity without compromising market principles.[132]

Policy lessons from recent presidential administrations underscore that the geographic location of economic activity, rather than the nationality of foreign ownership, is more important for strategic competition and economic resilience. This logic supports a more pragmatic approach to FDI in the DIB, particularly when vetted by CFIUS.[133] While some high-profile investments may face regulatory hurdles, regulatory flexibility should allow both wholly foreign-owned investments and joint ventures with the U.S. VC or PE firms, enabling capital inflows while maintaining sufficient control in strategic sectors.[134] Such flexibility is essential to accelerate revitalization of the DIB, strengthen supply chain resilience and enhance America's ability to compete with China's industrial capacity.

Beyond leveraging foreign capital through carefully managed FDI, another potent instrument for financial statecraft involves harnessing domestic resources. Recognizing strategic capital as a tool of financial statecraft, establishing a U.S. SWF represents a vital means to proactively channel national resources into critical long-term investments. Inspired by successful models such as Norway's Government Pension Fund and Singapore's GIC, a U.S. SWF could significantly stabilize domestic markets, strategically invest in essential sectors like infrastructure, advanced technology, and renewable energy, and effectively compete with

[132] Sam Lagrone, "South Korean Shipbuilder Hanwha Makes $100M Bid to Buy Philly Shipyard, SECNAV Del Toro Praises Deal," *U.S. Naval Institute News*, June 20, 2024, https://news.usni.org/2024/06/20/south-korean-shipbuilder-hanwha-makes-100m-bid-to-buy-philly-shipyard-secnav-del-toro-praises-deal.
[133] George Smith, "CFIUS & Foreign Direct Investment in Economic Development Projects," *JD Supra*, April 9, 2025, https://www.jdsupra.com/legalnews/cfius-foreign-direct-investment-in-3703807/.
[134] Bob Tita and Katherine Hamilton, "Trump Orders New Review of Nippon-U.S. Steel Merger," *The Wall Street Journal*, April 7, 2025, https://www.wsj.com/politics/national-security/trump-orders-new-review-of-nippon-u-s-steel-merger-52a6ba35?msockid=2a01c9448eea68c50214dd938fed69cb.

adversarial foreign sovereign wealth investors.[135] Unlike PE or VC funds, which are profit-driven and limited by investor timelines, a SWF can take a generational outlook and align investment decisions with national interests. This allows for patient capital deployment in areas that may be strategically critical but not immediately lucrative. Proposals such as the current Administration's incorporation of digital assets and federal resource revenues highlight the increasing acknowledgment of economic security as fundamental to national security.[136] The inclusion of digital assets further complements this forward-leaning approach, positioning the fund to engage with decentralized finance ecosystems that are expected to shape future global markets. Nonetheless, careful consideration of political feasibility, governance structures, and transparency protocols remains essential to mitigate risks and maximize the fund's strategic benefits.[137] [138]

Finally, shifting from large-scale government initiatives to specific financial innovations mentioned earlier, TPLF underscores the potential strategic implications of the finance industry's ability to innovate, demonstrating how financial mechanisms have the potential to inadvertently become vectors for economic and intellectual vulnerabilities. Malign actors could leverage the lack of transparency, potential control by funders, and a fragmented regulatory scheme for their benefit.[139] Robust KYC and AML requirements are directly imposed or adopted by financial

[135] Norges Bank Investment Management, *The Fund's History*, accessed April 2025, https://www.nbim.no/en/the-fund/history/; Government of Singapore Investment Corporation, "About Us," accessed April 2025, https://www.gic.com.sg/who-we-are/.
[136] Donald J. Trump, Executive Order 13999, "Establishing the United States Sovereign Wealth Fund," The White House, March 15, 2025.
[137] U.S. Department of Commerce, *White Paper on Blockchain Integration into Federal Investment Vehicles*, April 2025.
[138] International Working Group of Sovereign Wealth Funds, *Santiago Principles: Generally Accepted Principles and Practices (GAPP)*, October 2008, https://www.ifswf.org/santiago-principles.
[139] Klon Kitchen and Preston Golson, "Third-Party Litigation Financing: A National Security Problem," *Center for Strategic and International Studies (CSIS)*, January 30, 2024, https://www.csis.org/analysis/third-party-litigation-financing-national-security-problem.

entities, such as Registered Investment Advisers (RIAs) or indirectly when such RIAs utilize registered broker-dealers to affect securities transactions. However, requirements are predicated by various asset and/or fund triggering requirements, and the task of oversight either by the SEC for RIAs or the states for investment advisers registered under state requirements is daunting, as regulators do not have infinite resources to exam all of these entities as frequently as may be warranted. Although enforcement of these laws is not uniform, and recent signals by the current Administration suggest a pullback in enforcement efforts.[140] The complex nature of investors using shell corporations exacerbates difficulties in ascertaining beneficial ownership, thereby creating potential openings for foreign adversaries to inject capital into litigation against U.S. firms.[141] If that happens, these malign entities could finance lawsuits aimed at extracting sensitive data during discovery, distracting corporate leadership, depressing stock prices, or delaying market entries. Organizations like the U.S. Chamber of Commerce raised concerns regarding foreign SWFs from countries such as China potentially covertly funding intellectual property and patent litigation in the U.S.[142] A targeted regulatory approach is necessary to address these vulnerabilities without stifling the benefits TPLF provides.

Strategic Takeaways for Financial Resilience

These four areas offer strategic opportunities that the U.S. could leverage to better compete with peer adversaries. By proactively engaging in these strategic financial arenas, the

[140] U.S. Department of the Treasury, "Treasury Releases Request for Information on Use of Artificial Intelligence in the Financial Services Sector," press release, March 27, 2024, https://home.treasury.gov/news/press-releases/sb0038.
[141] Klon Kitchen and Preston Golson, "Third-Party Litigation Financing: A National Security Problem," *Center for Strategic and International Studies (CSIS)*, January 30, 2024, https://www.csis.org/analysis/third-party-litigation-financing-national-security-problem.
[142] U.S. Chamber of Commerce Institute for Legal Reform, *The Grim Realities of Third Party Litigation Funding* (Washington, DC: ILR, August 2024), https://instituteforlegalreform.com/wp-content/uploads/2024/08/TPLF-Research-Grim-Realities-Aug.-2024.pdf.

U.S. can secure its economic and national security future and solidify its enduring global influence.

Policy Recommendations

Having examined key dimensions of the finance industry (cryptocurrency, cybersecurity, money laundering, VC, and foreign ownership), it is now essential to propose integrated policy recommendations that address these challenges and strengthen the financial system's role in advancing national security. Critically, it is imperative to recognize that the U.S. financial system is a strategic asset and is functioning well, thus recommendations represent a scalpel, not a cudgel. These are meant to improve the system by addressing/mitigating vulnerabilities.

Cryptocurrency Policy Recommendations

1. Congress and relevant agencies must collaborate to establish statutory clarity on cryptocurrency oversight. This should balance innovation incentives with AML and counterterrorism financing safeguards, ensuring the regulatory approach enhances national security without stifling technological progress. The Genius Act, Senate 394, proposes moderate regulatory standards that are a great start to providing regulatory standards. Time will tell if this takes hold and if it will be enough.[143]
2. The DOD should initiate pilot programs applying blockchain registries to track critical weapon system subcomponents, starting with munitions like the Javelin missile.[144] These pilots would help validate the operational benefits of blockchain technologies while identifying implementation challenges.

[143] Lorena Nessi, "GENIUS Act: A Guide to the US Senate's Stablecoin Legislation," *CCN*, March 24, 2025, https://www.ccn.com/education/crypto/genius-act-us-senate-stablecoin-legislation/.
[144] U.S. Army Acquisition Support Center, Javelin Weapon System, U.S. Department of the Army, accessed April 13, 2025, https://asc.army.mil/web/portfolio-item/ms-javelin/.

3. The DOD and other relevant agencies should design and test micropayment platforms for use in viable operational environments, emphasizing transparency and secure vendor engagement while minimizing risks to local suppliers. Such systems should be resilient, auditable, and easily adaptable to different theaters of operation.
5. The Treasury Department should develop U.S. backed digital financial instruments that enhance the appeal of dollar-denominated transactions while safeguarding privacy and freedom against authoritarian alternatives. Innovation in secure, privacy-respecting digital payment methods could reinforce U.S. global financial leadership.

Cybersecurity Policy Recommendations

6. The Administration should create a reliable Joint Intelligence Sharing Platform that is secure and centralized to ensure lessons learned are passed at sufficient speed and fidelity.
7. The Administration should conduct a detailed review and strengthen current policies, such as encouraging Congress to extend the Cybersecurity Information Sharing Act of 2015, which is due to expire in September. Additionally, the Administration should encourage the SEC and FINRA to continue pushing the private sector toward more robust fortification by offering incentives for small contractors and firms.[145]
8. The Administration should hold an annual joint exercise for the finance industry involving scenarios that affect the financial and defense infrastructures simultaneously. The outcomes of these exercises should inform a joint crisis response protocol.
9. The Administration should mandate rigorous cybersecurity standards for centralized cryptocurrency exchanges and incentivize private sector investments in transaction

[145] Inceptus, "The Hidden Costs: Financial Hurdles in Cybersecurity for SMBs," Inceptus, accessed April 20, 2025, https://inceptussecure.com/inceptus-blog-1/f/the-hidden-costs-financial-hurdles-in-cybersecurity-for-smes.

security technologies. Standardized security protocols would reduce vulnerabilities and increase trust in digital asset ecosystems.

AML Policy Recommendations

10. The Treasury Department should expand beneficial ownership transparency by amending the CTA to mandate full disclosure of CRE ownership layers particularly near military installations.
11. The U.S. must strengthen global coordination by enabling real-time data sharing among financial intelligence units, as modeled by the United Kingdom's Joint Money Laundering Intelligence Taskforce to counter cross-border laundering.

Venture Capital Recommendations

12. DOD should continue to incorporate venture style practices such as adopting flexible funding vehicles, embedding innovation liaisons with VC firms, and coinvesting in dual-use startups via organizations like DIU, IQT, and OSC.
13. The U.S. should signal support for NIF and DIANA to encourage European allies to reinvigorate the defense tech VC market.

Foreign Ownership Recommendations

14. The U.S. should consider a "trusted capital" strategy that incentivizes beneficial foreign investment, tightly regulates M&A activity to maintain innovation and supply chain resilience, establishes carefully structured sovereign wealth initiatives, and rigorously oversees emerging financial innovations such as TPLF.
15. The Treasury Department must vigorously enforce existing CTA regulations mandating the identification of beneficial ownership, with the Executive Branch signaling strong support for compliance given the national security stakes.

16. The U.S. should establish and maintain a TPLF sanctions list (separate from OFAC) and modeled after frameworks like Section 889, with annual certification requirements to prevent foreign adversaries from covertly leveraging the U.S. legal system.

Conclusion

The U.S. finance industry stands as both a strategic enabler and a potential vulnerability in today's contested global environment. As adversaries exploit financial technologies for sanctions evasion, intellectual property theft, and asymmetric influence, America must treat its financial system as a critical component of national defense infrastructure. The sector's transformation—driven by fintech disruption, digital assets, cyber threats, and nonbank financial growth—requires policy responses that are agile, nuanced, and forward-looking. Rigid or sweeping regulation risks stifling innovation, while inaction leaves critical seams exposed to exploitation.

This report offers a four-part roadmap that balances resilience and dynamism: tailored legislation to clarify digital asset classification and strengthen transparency; executive action to mandate blockchain pilots and reinforce cybersecurity mandates; deepened public-private collaboration to align investment and threat intelligence; and technological modernization through AI-driven compliance tools and global payment standards. These measures are not merely financial reforms—they are elements of a broader strategy to harden U.S. economic power, protect critical infrastructure, and retain global influence. As great power competition intensifies, the ability to mobilize, secure, and project financial strength will determine more than market leadership, it will shape the nation's strategic future. The time to act is now.

Appendix A:
Artificial Intelligence and the Finance Industry

Introduction

The evolution of AI has considerably reshaped the finance sector and estimates now forecast that the AI-in-finance opportunity will turn into a $130 billion industry by 2027.[146] The transforming effects of AI manifest in several facets, such as improved efficiency, risk improvement, and navigation of regulatory challenges. Because financial systems are the lifeblood of any economy, embedding AI in these systems makes understanding the dual use of this technology crucial for policymakers, financial institutions, and national security agencies.

The Transformation of Financial Services Through AI

AI is disrupting the traditional financial sector, the established operational bonds are weakening, and innovations and business models are emerging.[147] Automation focused on AI ushered in a new era of efficiency within the financial industry. Financial institutions use AI algorithms to accelerate transaction processing, improve customer service via chatbots, and rationalize back-office operations.[148] Such automation reduces operational costs and allows institutions to reassign resources to more strategic initiatives.[149] By incorporating predictive

[146] "AI in Finance: Revolutionizing the Future of Financial Management," accessed May 1, 2025, https://www.datacamp.com/blog/ai-in-finance.
[147] "How Artificial Intelligence Is Transforming the Financial Services Industry," accessed May 1, 2025, https://www.deloitte.com/ng/en/services/risk-advisory/services/how-artificial-intelligence-is-transforming-the-financial-services-industry.html.
[148] Tobias Adrian et al., "Artificial Intelligence and Its Impact on Financial Markets and Financial Stability," IMF, accessed May 1, 2025, https://www.imf.org/en/News/Articles/2024/09/06/sp090624-artificial-intelligence-and-its-impact-on-financial-markets-and-financial-stability.
[149] David Mhlanga, "Industry 4.0 in Finance: The Impact of Artificial Intelligence (AI) on Digital Financial Inclusion," *International Journal of Financial Studies* 8, no. 3 (September 2020): 45, https://doi.org/10.3390/ijfs8030045.

analytics, finance companies can make data-driven decisions quickly, generating information that traditional methods could neglect.[150]

Enhanced Risk Management and Decision-Making

Risk management has also experienced a transformative impact due to the implementation of AI. Traditional risk assessment models have relied on historical data and human expertise, which can introduce biases or ignore emerging threats. Artificial intelligence, conversely, offers the possibility of permanently learning new data inputs, thus refining its analytical capacities.[151] Financial institutions increasingly use AI to detect fraudulent activities, as these technologies can identify irregular patterns that may indicate criminal behavior.[152] AI also analyzes transaction patterns to detect anomalies and flag suspicious activity.[153] AI applications in financial security considerably reduce the risks associated with large-scale economic changes and potential cybersecurity threats.[154] Financial institutions use AI today to manage credit risks and make better-informed credit decisions.[155]

AI in Financial Markets: Opportunities and Systemic Risks

Using AI in trading and investing has created new ways of participating in the markets. When trading with AI, one can utilize machine learning, sentiment analysis, and complex

---

[150] Peterson K. Ozili, "Big Data and Artificial Intelligence for Financial Inclusion: Benefits and Issues," in *Artificial Intelligence, Fintech, and Financial Inclusion* (CRC Press, 2023).
[151] Benjamin Cheatham, Kia Javanmardian, and Hamid Samandari, "Confronting the Risks of Artificial Intelligence," April 2019.
[152] Shailendra Mishra, "Exploring the Impact of AI-Based Cyber Security Financial Sector Management," *Applied Sciences* 13, no. 10 (January 2023): 5875, https://doi.org/10.3390/app13105875.
[153] "Banking Automation: What It Is and How It Works," accessed May 1, 2025, https://appian.com/blog/acp/finance/banking-automation-what-it-is-how-it-works.
[154] Shaip Gashi et al., "Research on the Impact of Artificial Intelligence on Financial Security in the Context of Modern Technological Challenges," *Interdisciplinary Journal of Applied Science* 8, no. 13 (October 1, 2024), https://doi.org/10.18226/25253824.v8.n13.08.
[155] "Using AI in Risk Management for Stronger Financial Services," Snowflake, accessed May 1, 2025, https://www.snowflake.com/guides/using-ai-risk-management-financial-services/.

algorithms to predict market movements and conveniently execute trades at optimal prices.[156] These tools can make the markets much more efficient, but they also introduce a higher level of risk.[157] Additionally, AI increases the market's ability to react quickly to new information, with the speed and magnitude of price movements exceeding the norm.[158] The financial system's interconnectedness and the use of AI in trading can increase systemic volatility and lead to flash crashes.[159]

However, the integration of AI into risk management is not without challenges. There is an urgent need for financial organizations to establish solid ethical directives to govern the use of AI and mitigate the biases inherent in automatic learning algorithms.

National Security Implications

AI's integration into financial systems creates multiple national security threats that demand diligent oversight.

Illicit Finance and Financial Crime

The 2024 National Strategy for Combatting Terrorist and Other Illicit Financing from the U.S. Treasury acknowledges that while both government and private sectors can use AI to enhance data analytics and improve identification of illicit finance risks, the technology can create new problems, too.[160] As the use of AI by bad actors becomes more sophisticated, new illicit risks will emerge.[161]

---

[156] "AI Trading: How AI Is Used in Stock Trading," Built In, accessed May 1, 2025, https://builtin.com/artificial-intelligence/ai-trading-stock-market-tech.
[157] "Using AI in Risk Management for Stronger Financial Services."
[158] Adrian et al., "Artificial Intelligence and Its Impact on Financial Markets and Financial Stability."
[159] SUERF Policy Brief 2024, "Financial Intelligence: Opportunities and Risks of AI in Finance," SUERF, December 19, 2024, https://www.suerf.org/.
[160] Gregg Wirth, "US Treasury's 2024 Strategy to Combat Illicit Finance Cites Importance of AI, Other Innovations," Thomson Reuters Institute, May 28, 2024, https://www.thomsonreuters.com/en-us/posts/government/treasury-illicit-finance/.
[161] Ibid.

Cybersecurity Vulnerabilities

Financial institutions increasingly face expensive cybersecurity threats and cyber-enabled fraud. As advanced AI tools become more common, cyberthreat actors may initially gain the upper hand by using them to outpace our defensive measures.[162] Financial institutions are incorporating AI-driven tools into their security infrastructure to mitigate this risk, including endpoint protection, intrusion detection and prevention, and data-loss prevention.[163]

Strategic Competition

It has become a matter of national strategic importance to ensure that the U.S. can continue to hold a position of dominance in AI applications for finance. Experts from the National Security Commission on Artificial Intelligence, formed by Congress in 2018, produced a thorough, sobering assessment of the current state of AI to ensure the US maintains a competitive advantage.[164]

Conclusion

In conclusion, the integration of artificial intelligence in finance is characterized by increased efficiency and improved risk management capacities. However, this transformation has complexities, regulatory challenges, and implications for national security and economic stability. Establishing a coherent regulatory framework while promoting innovation is essential to harness the advantages of AI while mitigating its associated risks. While the landscape of artificial intelligence continues to evolve, the finance sector must proactively engage with

[162] US Department of Treasury, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector," March 2024, https://home.treasury.gov/system/files/136/Managing-Artificial-Intelligence-Specific-Cybersecurity-Risks-In-The-Financial-Services-Sector.pdf.
[163] Ibid.
[164] "AI for National Security," accessed May 1, 2025, https://www.boozallen.com/markets/intelligence/ai-for-national-security.html.

regulatory organizations and stakeholders to navigate the challenges and opportunities this technological progress presents.

Appendix B
Wargaming / Business Planning

The U.S. finance industry has a long history of mitigating threats to its operations and reassuring investors during market shocks and periods of rapid financial innovation. This appendix explores how the industry conducts wargames to understand how strategic competition may impact their operations, including their ability to provide market liquidity in a crisis.

Although financial regulators have required large financial firms to conduct routine stress tests since the 2008 financial crisis, these computer-based simulations primarily assess traditional banking and liquidity risks—often discounting or omitting cyberattacks and geopolitical threats/risk—highlighting the need for new wargaming approaches to improve business continuity planning during a crisis. Analysis by the European Central Bank found that even a one standard deviation increases in geopolitical risk significantly reduced industrial production and heightened market volatility within one month.[165] Additionally, according to the World Economic Forum's *Global Risks Report 2025*, "geopolitical risk—and specifically the perception that conflicts could worsen and spread—tops the list of immediate-term concerns."[166] Moreover, a recent article aimed at corporate directors recommended that boards engage in geopolitical risk planning, develop in-house expertise, and integrate geopolitical threats into enterprise risk management.[167] Encouragingly, large financial firms have already begun to adopt these practices.

---

[165] Daniel Dieckelmann, Christoph Kaufmann, Chloe Larkou, Peter McQuade, Caterina Negri, Cosimo Pancaro, and Denise Rößler, "Turbulent Times: Geopolitical Risk and Its Impact on Euro Area Financial Stability," Press Release accompanying *Financial Stability Review*, European Central Bank, May 2024, https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_01~4e4e30f01f.en.html.

[166] Saadia Zahidi, "The Global Risks Report 2025" Preface to the Report, January 2025, https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf.

[167] James Lam, "The Board's Role in Navigating Geopolitical Risks," *Directors & Boards*, September 5, 2024, https://www.directorsandboards.com/risk-oversight/geopolitical-risk/the-boards-role-in-navigating-geopolitical-risks/.

Additionally, industry trade associations have played a critical role in bridging financial institutions and government agencies to evaluate collective decision-making under crisis conditions. For example, the Securities Industry and Financial Markets Association (SIFMA) sponsors *Quantum Dawn*, a series of cybersecurity exercises that "enable financial institutions and the sector as a whole to practice and improve coordination with key industry and government partners…to maintain financial markets operations."[168] These exercises help identify systemic vulnerabilities that individual financial firms may overlook in their internal wargames and tabletop exercises. Reflecting the shifting global risk environment, both advanced and emerging economies implemented over 1,500 industrial policy measures in 2023—underscoring a resurgence of protectionism and the growing role of strategic state investment in critical sectors.[169] This evolving landscape has prompted financial institutions and trade associations to deepen their collaboration with government agencies to better anticipate and respond to geopolitical disruptions. These partnerships not only yield valuable insight into the inner workings of the finance industry but also enable more effective integration into whole-of-government wargames, ultimately enhancing national coordination and crisis response efforts.

Finally, the U.S. government has taken proactive steps to engage the finance industry in wargames, tabletop exercises, and recurring briefings ahead of major geopolitical events, such as Russia's invasion of Ukraine in 2022.[170] These engagements help both public and private actors simulate systemic shocks, identify cross-sector vulnerabilities, and refine joint crisis response

[168] Press Release, "Cybersecurity Exercise: Quantum Dawn VII," *SIFMA*, May 1, 2024, https://www.sifma.org/resources/general/cybersecurity-exercise-quantum-dawn-vii/#:~:text=Quantum%20Dawn%20is%20a%20series,attack.
[169] Anna Ilyina, Ceyla Pazarbasioglu, and Michele Ruta, "Industrial Policy Is Back But the Bar to Get It Right Is High," International Monetary Fund, April 12, 2024, https://www.imf.org/en/Blogs/Articles/2024/04/12/industrial-policy-is-back-but-the-bar-to-get-it-right-is-high.
[170] Sean Lyngaas, "FBI Official Warns of Potential Ransomware Attacks in Wake of US Sanctions on Russia," *CNN*, February 22, 2022, https://www.cnn.com/europe/live-news/ukraine-russia-news-02-22-22/index.html.

strategies—ensuring greater alignment in the face of geopolitical uncertainty. This approach mirrors best practices adopted by global pension funds and PE firms, which are increasingly using geopolitical scenario analysis to stress-test investment portfolios and operational decision-making.

As the intersection of financial resilience and national security deepens, coordinated risk planning between government and industry will be essential to navigating emerging threats. These efforts lay the groundwork for sustained economic competitiveness and a more agile national response to future crises.

As the intersection of financial resilience and national security deepens, these collaborative efforts represent an essential foundation for future sovereign investment strategy and crisis preparedness planning.