ICIT

The Hidden Infrastructure Powering America's Markets

Concentration, Interdependency, and Systemic Risk in U.S. Financial Infrastructure

Authors: Cory Simpson, Javier Nater, Hugo Holopainen, Christopher Hetner

Table of Contents

About ICIT

The Institute for Critical Infrastructure Technology (ICIT) is a nonprofit, nonpartisan, 501(c)3 think tank with the mission of modernizing, securing, and making resilient critical infrastructure that provides for people's foundational needs. ICIT takes no institutional positions on policy matters. Rather than advocate, ICIT is dedicated to being a resource for the organizations and communities that share our mission. The views and opinions expressed in this essay are solely those of the author(s) and do not necessarily reflect the official policy or position of ICIT. Any assumptions made within the analysis are not reflective of the position of any entity other than the author(s). To learn more, please visit www.icitech.org

The Institute for Critical Infrastructure Technology

I. Markets Run on More Than Just Screens

Most Americans experience financial markets through screens: prices update in real time, trades execute instantly, and portfolios adjust with a simple click of the mouse. Stakeholders ranging from major banks to anyone with a retirement savings account rely and depend on this financial system. Integral to the American way of life, this ability to execute financial decisions seamlessly and instantaneously suggests a system that is digital, distributed, and intangible.

However, modern markets actually rely on a digitally enabled but physically concentrated and operationally interdependent infrastructure layer that operates behind the scenes and expands beyond traditional institutions.

Although we often think of Wall Street as the center of U.S. markets, a significant portion of U.S. market activity is enabled inside a cluster of specialized data centers across northern New Jersey. Facilities in Secaucus, Carteret, and Mahwah serve as the physical meeting point for exchanges, trading firms, and networks. These locations form one of the most important financial infrastructure corridors in the country.

These campuses are designed to facilitate secure, high-speed connections between participants, allowing markets to function continuously, efficiently, and without delay. These locations serve as the physical meeting point for exchanges, trading firms, financial market utilities, and network providers, creating a complex and interdependent environment.

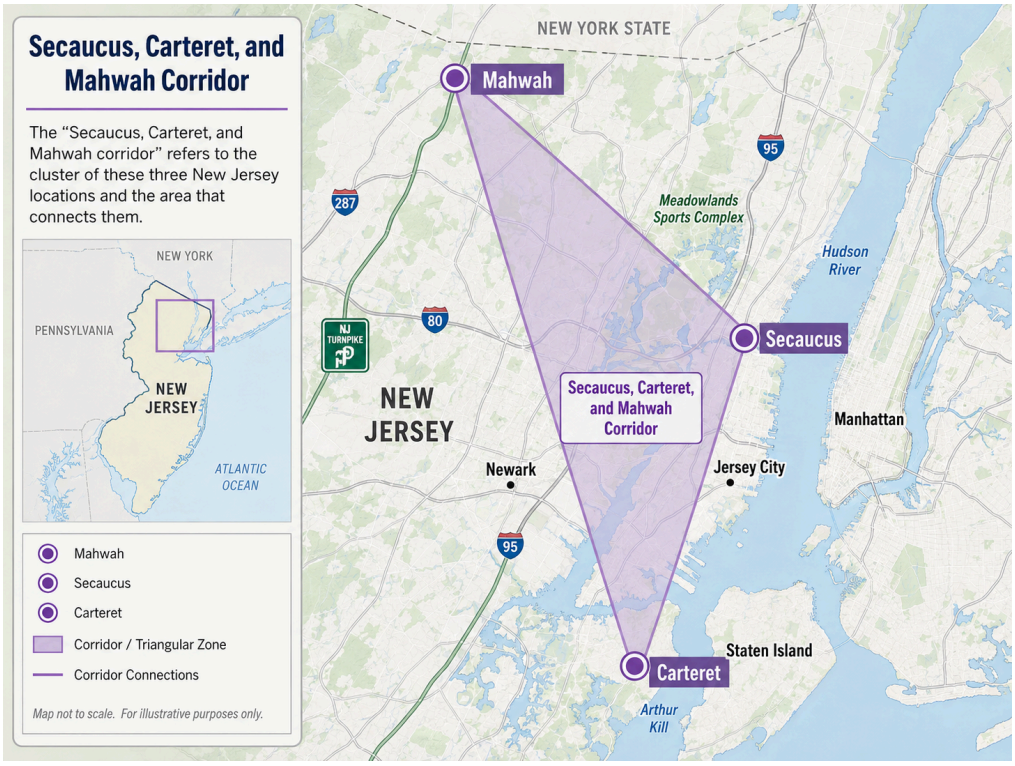
This report examines the infrastructure that underpins financial markets, how it is structured, and the risks embedded within it. It also outlines why this infrastructure is inseparable from market stability and why the investment community has a direct stake in its security and resilience. Securing and investing in this at-risk critical infrastructure must be of high priority for the institutions and investors that depend on it.

II. Critical Infrastructure and Market Stability

At their core, financial markets depend on three elements: data, connectivity, and timing. Prices must be generated and shared, buyers and sellers must be connected, and transactions must occur in a synchronized and reliable manner. The infrastructure supporting these functions operates at scale within tightly integrated physical environments.

Within these environments, firms deploy systems that connect directly both to exchanges and to one another. Networks move vast volumes of market data and orders in fractions of a second, enabling continuous price discovery and execution. This infrastructure functions as the operational foundation of modern finance, supporting liquidity, transparency, and the efficient allocation of capital.

The Secaucus, Carteret, and Mahwah corridor represents one of the most concentrated segments of this infrastructure in the United States. Core trading systems, including Nasdaq's primary data center in Carteret and the New York Stock Exchange's systems in Mahwah, operate within this corridor, interconnected through ultra-low latency networks that support continuous trading.



This geographic concentration delivers performance and efficiency. It also creates shared dependence across market participants. A disruption affecting power, connectivity, or operations within this corridor has the potential to influence trading, price formation, and liquidity across U.S. markets, with implications that extend beyond domestic markets into the global financial system.

These systems support essential economic functions and enable the flow of capital across the economy. As such, they form part of the nation's critical infrastructure and are directly tied to economic security and national stability.

III. How Financial Critical Infrastructure is Structured

Financial markets operate across a set of tightly coupled layers that together enable trading, settlement, and the underlying systems that support both.

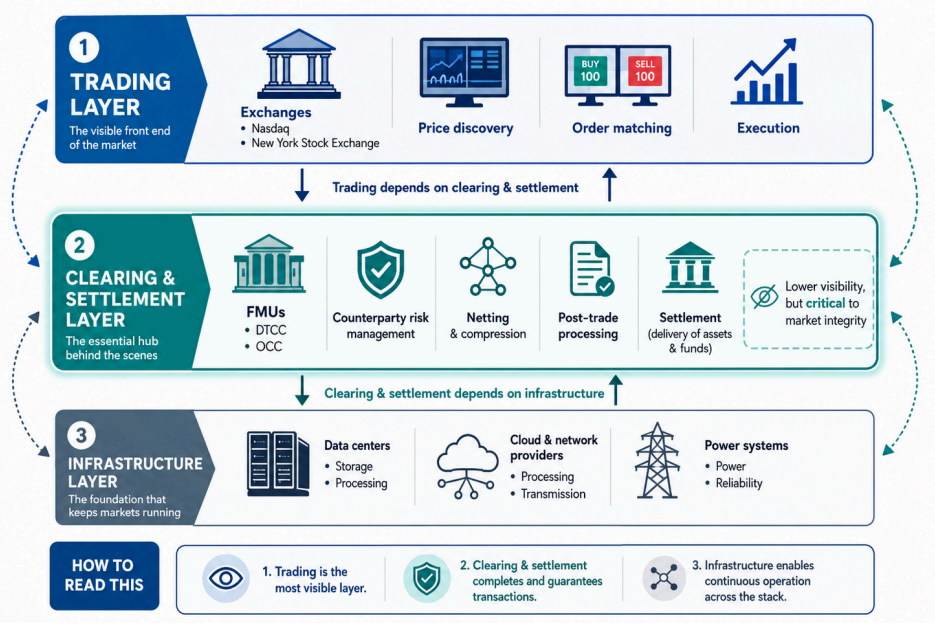
At a high level, this structure can be understood as three interconnected layers:

- **Trading Layer** – where transactions are executed through venues such as Nasdaq and the New York Stock Exchange.
- **Clearing and Settlement Layer** – where Financial Market Utilities (FMUs) such as the Depository Trust & Clearing Corporation (DTCC) and the Options Clearing Corporation (OCC) manage post-trade processes, counterparty risk, and settlement.
- **Infrastructure Layer** – the physical and digital systems that support both trading and clearing, including data centers, cloud and network providers, and power systems.

Market participants are broadly familiar with exchanges and increasingly aware of the infrastructure layer that supports them. Exchanges such as Nasdaq and the New York Stock Exchange facilitate price discovery and execution. Data centers provide the physical environments where systems are deployed and interconnected. Cloud and network providers enable data storage, processing, and transmission. Power systems ensure continuous operation of these environments.

The clearing and settlement layer, however, operates with less visibility despite its central role in ensuring that transactions are completed, netted, and honored.

Together, these layers form a tightly integrated system where each function depends on the others.



IV. Financial Market Utilities: The Core of Systemic Concentration

Beyond trading venues, the most significant concentration of risks resides within Financial Market Utilities (FMUs): entities responsible for clearing, settlement, and counterparty risk management.

The Depository Trust & Clearing Corporation serves as the backbone of U.S. post-trade infrastructure through its subsidiaries. It clears and settles the vast majority of U.S. securities transactions, manages counterparty exposure, and ensures settlement finality. A disruption at DTCC would directly affect settlement certainty, collateral flows, participant liquidity, and overall confidence in the financial system.

The Options Clearing Corporation represents a parallel concentration point as the central counterparty for all listed U.S. options markets. It clears and settles options transactions, manages margin and collateral, and supports market stability during periods of volatility.

These institutions operate as central nodes within the financial system. Their role in completing transactions makes them indispensable to market functioning.

V. What Is at Risk

The composition of financial critical infrastructure introduces a range of risks that are concentrated, interconnected, and capable of propagating across markets.

Risks Across the Three-Layer Stack

Within the **trading layer**, disruptions affecting major exchanges could interrupt order execution, impair price discovery, and reduce liquidity across equities and related markets.

Within the **clearing and settlement layer**, risks are more systemic in nature. A disruption at DTCC would affect settlement certainty, collateral movement, and participant liquidity. A disruption at OCC could impair hedging activity, amplify volatility, and transmit stress across markets through derivatives exposure.

Within the **infrastructure layer**, risks originate from failures in power systems, connectivity, data centers, or third-party providers. Because these systems are shared across multiple market participants, a localized failure has the potential to disrupt multiple institutions simultaneously.

Across all three layers, the concentration of infrastructure and limited real-time substitutability increase the potential for correlated disruption. Events affecting connectivity, cyber integrity, or physical operations within key infrastructure hubs could impact trading, settlement, and liquidity at the same time.

Sequenced, achievable steps that can be pursued within existing budgets, while tailoring communications for relevant Congressional vehicles and committees, including quantum-related legislative efforts, should be emphasized.

Just as important, messaging should reflect that PQC awareness remains uneven across sectors: the financial sector is generally farther ahead, while many critical infrastructure owners and operators may not yet be tracking these issues closely.

For that reason, outreach and education efforts should be designed to meet audiences where they are, with concrete guidance that makes clear this is a current risk requiring action now rather than a distant future problem.

Supply Chain and Hidden Concentration Risk

The resilience of financial markets also depends on a shared and often opaque supply chain. Data centers, cloud providers, telecommunications carriers, and software platforms support multiple systemically important institutions simultaneously.

These dependencies introduce hidden concentration risks. Multiple entities rely on the same vendors, physical locations, and network pathways. This structure creates the potential for a single point of failure to propagate across markets, resulting in cross-market disruption.

As threats to critical infrastructure become more sophisticated due to emerging technologies like artificial intelligence and quantum technologies (computing, sensing, networking), these interdependencies increase the potential for systemic events that affect both market functioning and confidence.

A Benchmark for Systemic Market Impact

The United States has already experienced the potential consequences of disruption to financial infrastructure. Following the September 11 attacks, U.S. markets were forced to close for nearly a week due to heavily damaged financial critical infrastructure.

When trading resumed, the Dow Jones fell more than 7% in a single day, contributing to a broader market decline that erased approximately $1.4 trillion in value within days. The disruption extended beyond equities, with sharp impacts to key sectors such as airlines and insurance, and broader volatility across commodities and global markets.

These events demonstrated how quickly market confidence can deteriorate when core systems are disrupted, and how deeply such shocks can reverberate across the financial system and economy. Digital and physical financial critical infrastructure targeted attacks pose very real risks of market closures and disruptions in the future.

VI. Stakeholders and Their Role in the Ecosystem

Government

The federal government plays a central role in identifying, protecting, and regulating financial critical infrastructure. The Department of the Treasury serves as the Sector Risk Management Agency for the financial services sector, while the Cybersecurity and Infrastructure Security Agency (CISA) supports the protection and cyber defense of critical infrastructure systems.

The Securities and Exchange Commission provides regulatory oversight of key market entities, including through Regulation Systems Compliance and Integrity (SCI).

Regulation SCI was developed in response to major market disruptions, including the Flash Crash and the Knight Capital incident. It establishes requirements for maintaining resilient and scalable systems, conducting testing and incident response, and ensuring operational integrity across covered entities such as Nasdaq, the New York Stock Exchange, DTCC, and OCC.

Its scope is focused on core market entities and does not extend across the full infrastructure and supply chain ecosystem on which these systems depend.

The Financial Community

The investment community relies directly on the consistent performance of this infrastructure. Market access, execution quality, liquidity, and overall investment outcomes depend on systems that operate reliably and securely.

This creates a clear alignment between infrastructure resilience and financial performance. Investors and institutions are positioned to influence how infrastructure is secured, funded, and prioritized. Their participation in resilience initiatives, industry coordination, and public-private engagement strengthens the systems that underpin markets.

The financial and investment community has a larger role to play in translating market dependence into resilience. Protecting the infrastructure that underpins markets requires board-level governance, alignment with enterprise risk management, regulatory coordination, financial exposure analysis, and continuous resilience testing across the systems, providers, and interdependencies that support trading, settlement, liquidity, and market confidence.

This recognition is already taking shape across the financial sector. JPMorgan Chase has announced a $1.5 trillion, decade-long Security and Resiliency Initiative focused on investing in sectors critical to economic security, including energy, advanced manufacturing, and digital infrastructure.

This level of investment reflects an understanding that resilient infrastructure supports both national security and financial system stability. It also reinforces market confidence and enables capital to move efficiently across the economy.

As geopolitical tensions rise and cyber threats increase in frequency and sophistication, the importance of securing financial critical infrastructure continues to grow. Jamie Dimon, chairman and CEO of JPMorgan Chase, has reinforced this view, noting an "increasingly complex set of risks," including geopolitical tensions, energy volatility, trade uncertainty, global fiscal pressures, and elevated asset prices, and acknowledging that how these forces ultimately unfold remains highly uncertain.

VII. Conclusion: The Foundation Beneath the Market

Financial markets operate on a foundation that is physically concentrated, operationally interdependent, and deeply connected to a broader infrastructure ecosystem.

The stability of markets is closely tied to the resilience of this foundation. Disruptions within it have the potential to affect trading, settlement, liquidity, and confidence across the financial system and the broader U.S. and global economy.

Protecting and strengthening this infrastructure is a shared responsibility across government, operators, and the financial community. As markets evolve and risks become more complex, the role of investors and financial institutions in supporting critical infrastructure will continue to expand.

Much greater engagement, sustained investment, and participation in infrastructure security is a necessesity. These efforts ensure that the systems underpinning financial markets remain resilient, secure, and capable of supporting long-term economic stability.

VIII. Bibliography

References

1. Equinix, “New York Metro - Home to the Equinix® Financial Exchange,” Equinix, n.d., https://www.equinix.com/resources/data-sheets/nyc-metro-data-sheet.
2. Nasdaq, “Nasdaq: Stock Market, Data Updates, Reports & News,” Nasdaq, n.d., https://www.nasdaq.com/.
3. New York Stock Exchange, “The New York Stock Exchange,” NYSE, n.d., https://www.nyse.com/index.
4. Equinix, Inc., 2024 Annual Report (Redwood City, CA: Equinix, Inc., April 10, 2025), https://investor.equinix.com/sec-filings/annual-reports/content/0001140361-25-013274/0001140361-25-013274.pdf.
5. Cybersecurity and Infrastructure Security Agency, “Financial Services Sector,” CISA, n.d., https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/financial-services-sector.
6. Board of Governors of the Federal Reserve System, “Designated Financial Market Utilities,” Federal Reserve Board, last updated January 29, 2015, https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm.
7. Depository Trust & Clearing Corporation, “The Depository Trust Company (DTC),” DTCC, n.d., https://www.dtcc.com/about/businesses-and-subsidiaries/dtc.aspx.
8. The Options Clearing Corporation, “The Foundation for Secure Markets,” OCC, n.d., https://www.theocc.com/.
9. Don Aviv and Sabrina Tan, “Why Cybersecurity Threats Are Growing,” TIME, February 19, 2026, https://time.com/7382979/cybersecurity-threats-are-growing/.
10. Institute for Critical Infrastructure Technology, “Entangled Migrations PQC, QKD, and US–PRC Risk Postures for Critical Infrastructure,” ICIT, March 20, 2026, https://www.icitech.org/post/entangled-migrations-pqc-qkd-and-us-prc-risk-postures-for-critical-infrastructure.
11. Michael Tait, “Exploring Quantum Potential: Computing, Sensing and Networking,” GDIT, January 8, 2025, https://www.gdit.com/perspectives/latest/exploring-quantum-potential-computing-sensing-and-networking/.
12. Roger W. Ferguson, Jr., “Implications of 9/11 for the Financial Services Sector,” speech, Conference on Bank Structure and Competition, Chicago, Illinois, Federal Reserve Board, May 9, 2002, https://www.federalreserve.gov/boarddocs/speeches/2002/20020509/default.htm.

13. Marc Davis, “How September 11 Affected the U.S. Stock Market,” Investopedia, updated September 15, 2025, https://www.investopedia.com/financial-edge/0911/how-september-11-affected-the-u.s.-stock-market.aspx.
14. U.S. Department of the Treasury, Financial Services Sector Risk Management Plan (Washington, DC: U.S. Department of the Treasury, January 2025), https://home.treasury.gov/system/files/216/Financial-Services-Sector-Risk-Management-Plan.pdf.
15. Cybersecurity and Infrastructure Security Agency, “Financial Services Sector: Council Charters and Membership,” CISA, n.d., https://www.cisa.gov/financial-services-sector-council-charters-and-membership.
16. U.S. Securities and Exchange Commission, Regulation SCI: Proposed Expansion and Updates, fact sheet (Washington, DC: U.S. Securities and Exchange Commission, March 15, 2023), https://www.sec.gov/files/34-97143-fact-sheet.pdf.
17. U.S. Commodity Futures Trading Commission and U.S. Securities and Exchange Commission, Findings Regarding the Market Events of May 6, 2010: Report of the Staffs of the CFTC and SEC to the Joint Advisory Committee on Emerging Regulatory Issues (Washington, DC: CFTC and SEC, September 30, 2010), https://www.sec.gov/news/studies/2010/marketevents-report.pdf.
18. Nathaniel Popper, “Knight Capital Says Trading Mishap Cost It $440 Million,” DealBook, The New York Times, August 2, 2012, https://archive.nytimes.com/dealbook.nytimes.com/2012/08/02/knight-capital-says-trading-mishap-cost-it-440-million/.
19. JPMorganChase, “JPMorganChase Launches $1.5 Trillion Security and Resiliency Initiative to Boost Critical Industries,” press release, October 13, 2025, https://www.jpmorganchase.com/newsroom/press-releases/2025/jpmc-security-resiliency-initiative.
20. David Hollerith, “JPMorgan and Other Big Banks See Profits Rise as Dimon Warns of ‘Increasingly Complex Set of Risks,’” MSN Money, updated April 14, 2026, https://www.msn.com/en-us/money/markets/jpmorgan-and-other-big-banks-see-profits-rise-as-dimon-warns-of-increasingly-complex-set-of-risks/ar-AA20RcZb.

Authors & Taskforce

Cory Simpson

Chief Executive Officer, Institute for Critical Infrastructure Technology (ICIT).

Cory Simpson has over twenty years of experience in government, the military, and the private sector, specializing in national security, cybersecurity, business, law, and strategy. He served in the U.S. Army Judge Advocate General's Corps from 2004 to 2016 and continues as a legal advisor to U.S. Army Cyber Command. His military career includes roles as general counsel, prosecutor, and national security law advisor, with multiple combat tours and extensive trial experience. Cory is the CEO of Gray Space Strategies, a strategic advisory firm, and the Institute for Critical Infrastructure Technology (ICIT). He also serves as a senior advisor to CSC 2.0, continuing the work of the U.S. Cyberspace Solarium Commission, and is on the Board of Directors for the Cyber Guild.

Cory holds a Master of Laws in Military Law, a Juris Doctorate, and a BA in accounting with a minor in philosophy. He is globally recognized for creating effective solutions to complex challenges.

Javier Nater

Director of Operations, Institute for Critical Infrastructure Technology (ICIT)

Javier Nater is the Director of Operations at Gray Space Strategies and ICIT, ensuring engagements are planned, coordinated, and executed with discipline.

Javier sits at the center of the organizations' operations, translating strategy into execution and ensuring that the work led by the leadership is executed consistently, precisely, and with accountability.

He brings a strong academic foundation and a practical approach to problem-solving, supporting work across cybersecurity, national security, and emerging technology. His focus is on building and managing the systems, processes, and coordination required to operate effectively in complex environments.

At both organizations, Javier works closely with leadership to manage priorities, align efforts, and maintain the pace and discipline needed to deliver. His role enables the organizations to move quickly, stay organized, and sustain a high standard of execution across engagements.

Hugo Holopainen

Senior Associate, Research & Content Development Lead, Institute for Critical Infrastructure Technology (ICIT)

Hugo Holopainen leads research and content development at ICIT and Gray Space Strategies, bringing technical depth and disciplined analysis to the organization's engagements. Hugo researches the intersections of cybersecurity, aerospace, critical infrastructure, emerging technology, and defense.

He brings experience across security and international environments, with a background spanning military service, diplomatic work, and emerging technology. His work focuses on understanding complex systems, analyzing technical developments, and translating that understanding into immediate decisions and longer-term positioning and program direction. His work bridges defense, cyber, and emerging technology to inform strategy at the nexus of security and innovation.

Christopher Hetner

Cyber Risk Advisor to the National Association of Corporate Directors (NACD)

Chris Hetner is a senior executive, board director, and cybersecurity leader recognized for advancing cyber risk, AI governance, and operational resilience across the public and private sectors.

Chris works at the intersection of cybersecurity, business strategy, regulatory compliance, and enterprise risk management, helping boards and executive leaders align cyber resilience with business objectives and protect critical infrastructure, industries, and markets.

He has held senior leadership and advisory roles across government, financial services, and critical infrastructure, including serving as Senior Cybersecurity Advisor to the Chair of the U.S. Securities and Exchange Commission and representing the SEC on the U.S. Department of the Treasury's Financial Banking Information Infrastructure Committee.

Today, Chris serves as Cyber Risk Advisor to the National Association of Corporate Directors, Chair of the Cybersecurity, AI and Privacy Council for the Nasdaq Center for Board Excellence, Senior Advisor to the Cyber Future Foundation, Research Affiliate at MIT Sloan School of Management, Fellow at the Institute for Critical Infrastructure Technology, and board member and advisor to several organizations focused on cybersecurity, resilience, and governance.

Thank you to our sponsors for making this work possible:

ICIT

www.icitech.org