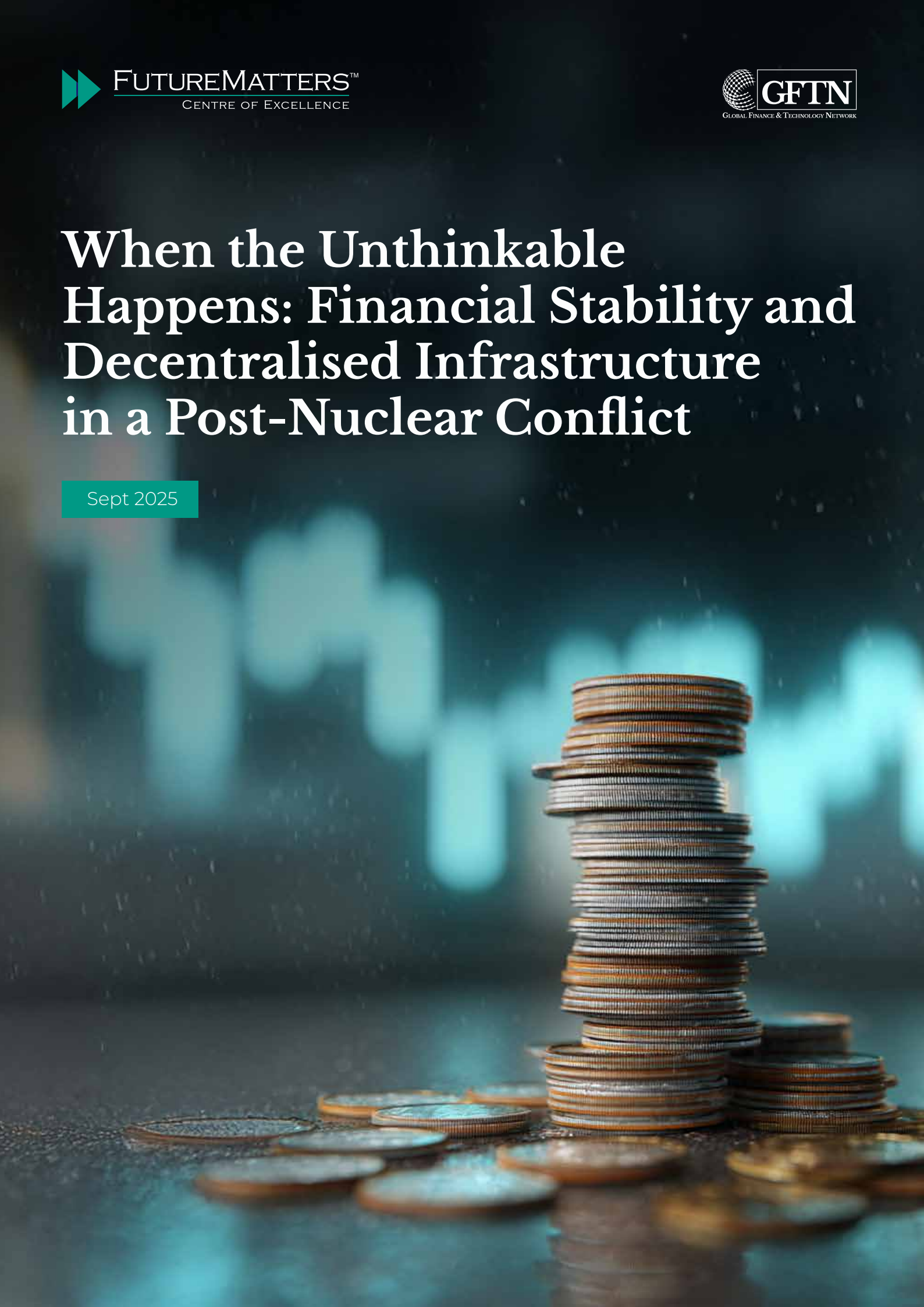
FUTUREMATTERS™
CENTRE OF EXCELLENCE

GFTN
GLOBAL FINANCE & TECHNOLOGY NETWORK

When the Unthinkable Happens: Financial Stability and Decentralised Infrastructure in a Post-Nuclear Conflict

Sept 2025



Agenda

The insight presented here is based on a nuclear-threat-scenario response discussion under Chatham Rules among world leaders in academia, industry, national public and global organisations.

1 Introduction: Confronting Systemic Risks

Today's global financial infrastructure faces escalating systemic risks, ranging from geopolitical tensions and trade disruptions to cyberattacks, pandemics, sabotage of undersea cables, and even nuclear conflict scenarios (see reference box). The vulnerabilities revealed by recent events, including military conflicts in Ukraine and Middle East, and widespread AI-enhanced cyber incidents, underscore the critical need for robust, resilient financial systems. This roundtable explored these systemic threats through an extreme yet illustrative nuclear conflict scenario, offering broader insights applicable to a wide range of disruptions.

Participants highlighted alarming gaps in preparedness among traditional financial institutions including central and commercial banks, emphasizing the urgency of developing resilient solutions.

> "Central banks and financial institutions do not currently have robust strategies for extreme systemic disruptions. Recent crises have exposed these vulnerabilities starkly."
> — Roundtable Insight.

a. Identifying Systemic Fragility in Traditional Finance

Our global financial infrastructure is primarily optimized for efficiency rather than resilience, leaving it vulnerable to systemic shocks. Key vulnerabilities include:

- **Preparedness Deficit:** Conventional financial institutions lack comprehensive plans for catastrophic disruptions, such as Electro-Magnetic Pulse (EMP) attacks, cyber incidents, or severe infrastructure failures. These risks are different to traditional financial risks and are rarely discussed in boardrooms.
- **Centralisation Risk:** Financial data and assets predominantly reside within centralized structures, creating single points of failure and increasing systemic risk exposure.
- **Wealth Inequality and Preparedness:** A pronounced divide exists in preparedness, with affluent individuals investing in private protection measures from bunkers to shielded jets, while general populations remain exposed.

b. Decentralised Finance: Building Resilience

Decentralised technologies—starting with the internet and later blockchain—were conceived as safeguards against systemic collapse. Paul Baran's 1964 proposal for a distributed communications network, designed to survive a nuclear attack, laid the foundation. Satoshi Nakamoto's 2008 work extended that logic to P2P value transfer, creating a monetary system without central points of failure.

Today, decentralised finance (DeFi) applies this principle at an increasing scale, offering not just a new model for systemic resilience but also efficiency, evident in solutions like atomic swaps.

> "Many financial institutions remain unprepared for extreme systemic disruptions. We have for long prioritised efficiency over resilience. This approach requires urgent revision in the context of current threats. I am glad we can finally have this conversation here."
> — Roundtable Insight.

2 Two Models of Resilience

Resilience can be built in two fundamentally different ways:

1. Legacy Redundancy:

- Traditional systems rely on layered backups, mirrored databases, and firewalls. But redundancy has limits—especially in cascading failures like EMPs or infrastructure attacks.
- These systems are expensive and often inaccessible to all but states and elites. Even central banks and treasuries lack full continuity strategies for extreme events like nuclear war.

2. Decentralisation by Design:

- Distributed ledgers (like Bitcoin) avoid single points of failure. If parts of the system go down, others continue to function.
- Inspired by Baran's Cold War-era designs, this approach was proven in Ukraine, where a DLT solution, specifically, the Stellar network enabled financial aid despite war-related disruptions.

> "Backups fail. But decentralised networks have higher chances of surviving by design."
> — Roundtable Insight.

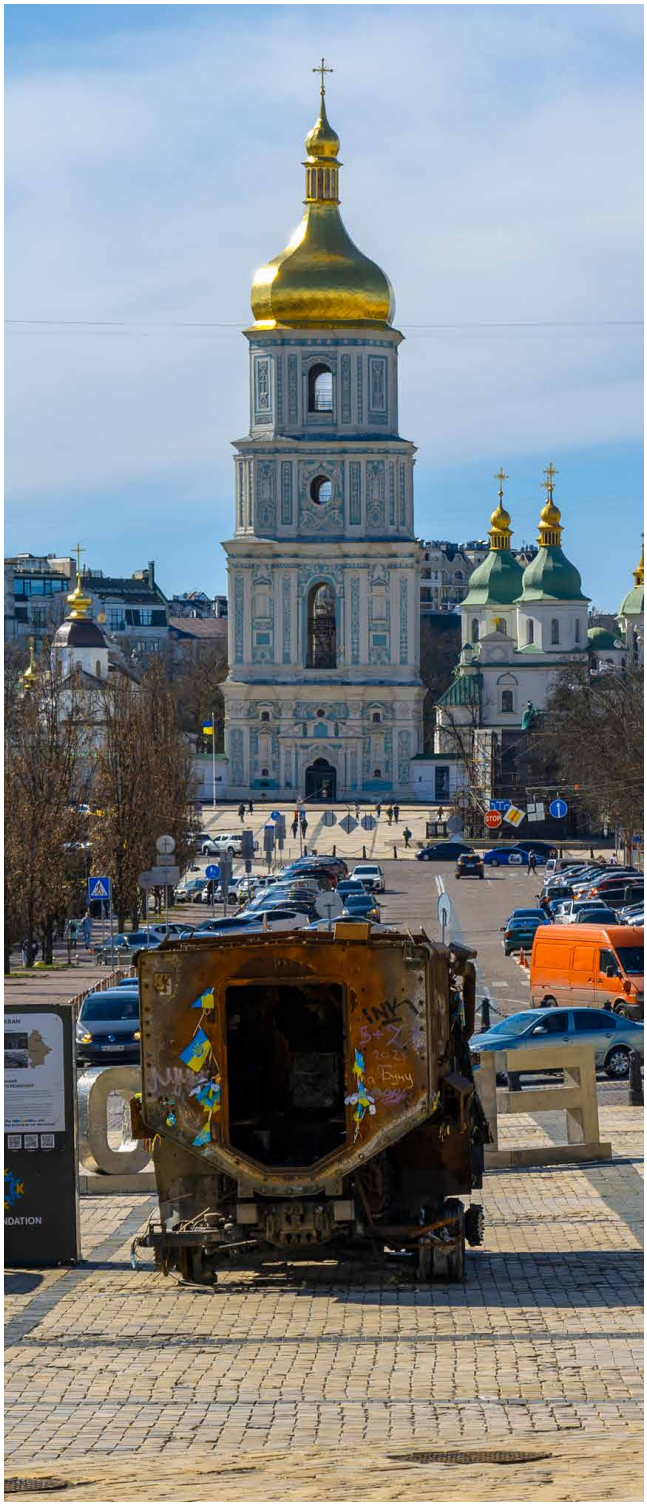
This shift reframes resilience: from protecting a central node, to ensuring system-wide survivability.

3 UNHCR Ukraine Aid via Blockchain: In Partnership with SDF, Circle (USDC), and MoneyGram

Following the start of the full-scale war in 2022 and up to 2024, UNHCR, the UN Refugee Agency, leveraged distributed ledger technology (DLT) to enable a secure, efficient digital payment solution for delivering humanitarian financial aid to war-affected and displaced people, as part of its broader assistance programmes.

Through the integration of blockchain-based digital wallets, the system connected USDC, a fully-backed stablecoin redeemable 1:1 for USD, that is issued through regulated affiliates of Circle Internet Group, Inc. with off-ramps (MoneyGram), providing direct access to Ukraine's financial ecosystem and supporting cross-border cash-out capabilities. Delivered in partnership with the Stellar Development Foundation (SDF), this solution enabled end-to-end aid delivery despite severe threats to traditional financial infrastructure. Operating securely across borders and without reliance on a single point of failure, the platform demonstrated exceptional resilience under crisis conditions. **The initiative delivered a dual benefit: it enhanced the continuity and reliability of humanitarian assistance, and significantly outperformed conventional cross-border payment systems in terms of cost savings and efficiency, ensuring full accountability for aid disbursed.**

> "What we have learned in Ukraine, was that the DLT solutions can be both more resilient and efficient."
> — Roundtable Reflection



4 Challenges to Adoption

Decentralised systems offer promise, but not without trade-offs:

- **Governance and Trust:** Decision-making in decentralised systems and even in Central Bank Digital Currencies (CBDCs) is complex and requires a debate on trust and how new tools, such as Decentralised Autonomous Organisations (DAOs) can facilitate the trust.
- **Technological innovation risks:** While new distributed technologies solve certain problems, they also introduce new systemic risks of complex interconnected systems. Not all DLTs are the same and not all are interoperable. The impact of their potential failure is yet unknown. Only several global research institutes conduct studies to understand these issues.
- **Regulation:** Legal frameworks are still catching up, leaving DeFi in uncertain territory.
- **Accessibility:** The direct access to decentralised networks is relatively rare for most people and often mediated by traditional centralised interfaces designed for convenience, hence compromising the benefits of decentralised systems.

For the system to be effective, we need more education and practice at the retail level.

5 Towards Hybrid Financial Systems: A Balanced Approach

Currently, neither purely centralised nor entirely decentralised systems alone offer a complete solution. The same applies to digital and physical asset systems. A hybrid model that strategically blends these approaches is necessary:

- **Integration of Decentralised Technologies:** Central banks recognize the efficiency and redundancy benefits of decentralised systems for cross-border transactions, remittances, and global trade.
- **Historical Lessons:** Historical societies maintained resilience by controlling and effectively governing basic resources. Modern finance could benefit from a similar strategic diversification between physical and tokenised digital assets, and centralized and decentralised systems. We should not forget that traditional assets, such as cash or gold, offer good levels of decentralisation and resilience.
- **Operational and Regulatory Integration:** Recognising decentralised technology within existing regulatory frameworks will be crucial for achieving scalable resilience and systems interoperability. DLT allows for technological proof of asset ownership, but these systems must be recognised and embedded by national legal systems to be effective. This further requires cross-border recognition and interoperability for the system to be globally resilient.

> "Successful historical societies managed resilience through diversified resource control. Similarly, hybrid financial systems blending decentralised resilience with some traditional governance structures, digital assets with physical assets, like cash, gold - and maybe even water and food in times of crises - can offer the most effective path forward."
> — Roundtable Reflection

6 Suggested Recovery Architecture: A Strategic Blueprint

A multi-layered strategy is essential for designing robust financial continuity and recovery:

Resilient Asset Layer:

- Tokenization of new value assets such as essential commodities (water, energy, food) may provide stability even if traditional fiat systems collapse.
- Multi-currency stablecoins and digital asset standards beyond legal ambiguity (e.g. not classified as securities) need to emerge and be internationally adopted.

Resilient Infrastructure Layer:

- Global nodes distribution of DLT.
- Decentralised physical infrastructure network of data centres and off-grid power solutions integrated with satellite and terrestrial communications.

Trust and Governance Layer:

- Transparent, community-driven governance models (e.g., DAOs).
- Pre-established international crisis-response protocols.

Inclusion and Humanitarian Layer:

- Portable digital identity systems and decentralised payment solutions.
- Offline and minimal-resource financial solutions for displaced populations.

7 Policy and Regulatory Recommendations

To strengthen financial stability against systemic shocks, the following actions are recommended:

- Implement mandatory resilience testing for complex, multi-system risks.
- Develop regulatory frameworks enabling hybrid financial infrastructures.
- Allocate public-private funding toward decentralised financial technology.
- Clarify regulatory frameworks for digital asset use in crisis scenarios.

8 Cross-Sector Collaboration and Immediate Actions

STAKEHOLDER	RECOMMENDED ACTION
Central Banks	Adopt hybrid (decentralised-centralised and digital-physical) financial systems and governance models and validate these via pilots.
Blockchain Platforms	Build robust, interoperable and globally decentralised infrastructures.
Humanitarian Agencies	Pilot decentralised resilient solutions during crisis scenarios.
Technology Providers	Establish geographically distributed data centre and off-grid powered infrastructure.
Investors & Innovators	Advance and invest in off-grid distributed financial and governance solutions.
Academia	Research systemic risk of both centralised and decentralised financial infrastructure system.

9 Conclusion: Proactive Resilience for Future Stability

Financial stability in the face of systemic risks demands proactive innovation and cross-sectoral cooperation. This roundtable underscored the necessity of transitioning toward hybrid systems, blending decentralised technology and traditional finance with robust governance frameworks. Emphasizing preparation over reaction will be critical to navigating and mitigating future systemic shocks. Implement mandatory resilience testing for complex, multi-system risks.

Where Next?

- Singapore FinTech Festival 2025, Insights Forum 10-11 November– Stablecoin Tsunami - Exploring the impact of a possible major stablecoin collapse.
- Black Swan Summit 2026, Perth 23-25 March – "Designing the Lifeboats and Mapping New Frontiers" Three-day foresight sprint converting extreme-scenarios insights on deep tech disruption (AI, Quantum and DLT) into digital finance policy drafts and investable prototypes.

Systemic Threat Scenarios to Digital Finance Infrastructure - Reference Box for Resilence Planning

1. Electromagnetic Pulse (EMP) Effects.
A high-altitude nuclear explosion creates an EMP capable of disabling all unshielded electronic systems across entire regions.

- Collapse of banking, telecom, and payment networks
- Fried servers, grid infrastructure, ATMs, point-of-sale systems
- Data irretrievably lost without EMP-hardened backups

Source: Glasstone & Dolan (1977)

2. Undersea Cable Disruption. Submarine cables, the silent arteries of global finance, are vulnerable to both sabotage and high-yield explosive attacks.

- Interrupted SWIFT and global FX transactions
- Settlement delays, disconnection from global markets
- Confidence loss, triggering volatility and capital flight

Source: Kavanagh (2025)

3. Cyberattack on Financial or Nuclear Infrastructure. AI-enhanced cyberweapons can simultaneously target banks, exchanges, and even nuclear deterrent systems.

- Malware on reserves, digital IDs, and payment systems
- Cascading sell-offs from false signals or forced halts
- Institutional paralysis under coordinated cyber siege

Source: Unal & Lewis (2018)

4. Global Trade Wars & Digital Sovereignty Collapse. Global trade wars affecting digital data infrastructure and connectivity expose national sovereignty issues.

- Fragmentation of cloud infrastructure as major powers ban or throttle cross-border data flows
- Disconnection from essential digital services, including cross-jurisdictional payment platforms, DNS resolution, and cloud APIs
- Weaponization of supply chains, chip embargoes, and legal bans disrupt data centre access and digital finance infrastructure

Source: WTO (2025), BCG (2025)

"The internet—and by extension global finance—was not designed for a world of economic firewalls."
— Roundtable Reflection

“Doing nothing is not an option. Preparation is cheaper than collapse.”
— Roundtable Reflection

Authors

Dr. Andrzej Gwizdalski
Global Finance & Technology Network (GFTN)

Contributor

Kaitlyn Thinn
Head of Strategy and Research, Global Finance & Technology Network (GFTN)

Production

Carol Ann Christy
Graphic Designer

**Global Finance &
Technology Network (GFTN)**

6 Battery Road, #28-01, Singapore 049909
gftn.co | hello@gftn.com