International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

At the Intersection of Geopolitics And Artificial Intelligence:

Evolving Cyber Threats to Global Financial Services

A Research Paper on Cybersecurity in Financial Services
April 2026

Kishore Kandalai

Abstract:
Financial services organizations occupy a unique and perilous position in the global cyber threat landscape. As a sector whose disruption carries cascading macroeconomic consequences, banks, insurers, capital markets infrastructure, and fintech firms are simultaneously targets of criminal opportunism, geopolitical coercion, and state-sponsored sabotage. This paper examines two converging forces that are materially reshaping the threat environment: the weaponization of cyberspace as an instrument of geopolitical strategy, and the rapid evolution of artificial intelligence as both an offensive tool and a systemic vulnerability.
Drawing on threat intelligence from 2023 to early 2026, we analyze how the Russia-Ukraine conflict, US-China strategic competition, and Middle Eastern tensions have each produced distinct but increasingly overlapping attack patterns directed at financial institutions. We then examine how generative AI, large language models, autonomous bots, and automation pipelines are lowering the cost and raising the sophistication of cyber offensives, enabling threat actors ranging from nation-states to criminal syndicates to conduct operations at unprecedented scale. We conclude with actionable strategic recommendations for security leaders, boards, and regulators seeking to build durable resilience in an era where geopolitical instability and AI proliferation are not temporary conditions but permanent features of the operating environment.

Keywords: Geopolitical Cyber Risk, State-Sponsored Threats, AI-Powered Attacks, Financial Services Security, Automation, Threat Intelligence.

1. INTRODUCTION: THE CONVERGENCE OF GEOPOLITICS AND AI IN CYBER CONFLICT

In 2025, 53% of bank CEOs identified cyber-attacks as their single greatest operational risk — surpassing credit risk, regulatory change, and macroeconomic volatility for the first time in modern survey history. This is not merely a reflection of expanding digital attack surfaces. It signals a fundamental transformation in the nature of the adversary. The forces driving this transformation are deeply structural: sustained geopolitical rivalry between great powers and the democratization of sophisticated offensive cyber capabilities through artificial intelligence.
For decades, the dominant cyber threat model for financial services was financially motivated crime: account takeover, card fraud, ransomware for profit. While these threats persist, the period from 2022 to 2026 has marked a decisive inflection point. Cyberspace is now an active theater of geopolitical competition. Nation-states and their proxies deploy destructive malware, conduct espionage campaigns, and pre-position within critical financial infrastructure not merely for intelligence collection, but to create strategic leverage — a capability to be exercised when political conditions demand.

Simultaneously, artificial intelligence is compressing the skill differential between sophisticated nation-state actors and mid-tier criminal groups. Large language models craft highly convincing spear-phishing communications at scale. Autonomous bots probe and exploit vulnerabilities around the clock without human supervision. Deepfake audio and video undermine identity verification and enable social engineering at an industrial level. Reinforcement learning algorithms train credential-stuffing bots to bypass multi-factor authentication mechanisms that financial institutions invested heavily to deploy.
The interaction effect between these two forces — geopolitical threat actors adopting AI-powered offensive capabilities — creates a threat environment that is qualitatively different from anything financial services organizations have confronted before. This paper maps that environment, analyzes its implications, and proposes a framework for strategic response.

2. THE GEOPOLITICAL THREAT LANDSCAPE FOR FINANCIAL SERVICES

Financial infrastructure has long held symbolic and strategic significance beyond its economic function. The ability to disrupt payments, freeze credit markets, or undermine confidence in banking systems is a powerful instrument of coercion. Contemporary geopolitical rivals have fully recognized this, and the financial sector has become an increasingly deliberate target in hybrid conflict strategies.

2.1 Russia-Ukraine Conflict: Proxy Warfare and Financial Infrastructure Targeting

Russia's full-scale invasion of Ukraine in February 2022 catalyzed an unprecedented level of cyber activity targeting Western financial institutions. The conflict introduced a new category of adversary into the financial threat landscape: the state-sponsored hacktivist, operating as a deniable proxy with political objectives but tactically coordinated with intelligence services.

KillNet, the most prominent Russian-aligned hacktivist collective, specialized in Distributed Denial of Service (DDoS) attacks against European financial infrastructure. Operating in direct response to Western sanctions and military aid to Ukraine, KillNet and its affiliates targeted European central banks, commercial banks, and payment processors with volume-based attacks designed to degrade service availability and generate visible political effect. The group was widely assessed to operate with tacit, if not direct, coordination from Russian military intelligence (GRU). Its activities demonstrated that DDoS, often dismissed as low-sophistication nuisance traffic, can be weaponized as a tool of political signaling and operational disruption when deployed at scale against time-critical financial systems.

In June 2023, KillNet, Anonymous Sudan, and the resurrected REvil ransomware brand jointly threatened a coordinated attack against the SWIFT international messaging system — the backbone of global interbank settlements — specifically citing European financial support for Ukraine. While the threatened attack on SWIFT itself did not materialize at the scale announced, the threat demonstrated the aspirational targeting of core financial market infrastructure and the willingness of these groups to issue high-visibility declarations to maximize psychological and market impact.

ENISA's Financial Sector Threat Landscape report, covering January 2023 to June 2024, documented 301 significant cyber incidents affecting European financial institutions during this period, with peaks in DDoS activity strongly correlated with military and political escalation events in the Ukraine conflict. European credit institutions were the most affected entity type, accounting for 46% of all incidents, with hacktivists responsible for 58% of DDoS incidents directed at the sector. This represents a deliberate targeting pattern, not random opportunism.

Beyond DDoS, Russian state actors — particularly Sandworm, associated with GRU Unit 74455 — have maintained destructive malware capabilities targeting financial and critical infrastructure. The NotPetya attack of 2017, though preceding the current conflict, remains the single most financially damaging cyber

incident in history, causing over $10 billion in global losses, including significant damage to financial services firms. It established the template: malware designed with plausible deniability, deployed in conflict-adjacent conditions, causing cascading collateral damage well beyond the intended target geography.

> *Key Intelligence Assessment: Pro-Russian hacktivist groups are state-adjacent proxies, not independent actors. Their targeting patterns correlate directly with geopolitical events, and their capabilities are augmented with access to state intelligence infrastructure. Financial institutions in NATO member states should assess their DDoS resilience against sustained, politically motivated attack campaigns, not merely criminal traffic patterns.*

2.2 US-China Strategic Competition: Espionage, Pre-Positioning, and Supply Chain Risk

China's approach to cyber operations targeting financial services differs materially from Russia's in both method and strategic objective. Where Russian-aligned actors have frequently sought disruption and visibility, Chinese state-sponsored groups — operating under the broader framework of the People's Liberation Army (PLA) and the Ministry of State Security (MSS) — have pursued persistent, low-signature campaigns optimized for intelligence collection and strategic pre-positioning.

The Volt Typhoon campaign, attributed to a Chinese state actor and documented in joint advisories from CISA, NSA, FBI, and their Five Eyes counterparts, exemplifies this approach. Active since at least mid-2021 and continuing through 2024, Volt Typhoon compromised critical infrastructure networks across the United States — including financial sector entities — using a technique known as Living off the Land (LotL). Rather than deploying distinctive malware that would trigger signature-based defenses, the actors leveraged legitimate administrative tools, valid credentials harvested from prior compromises, and standard network protocols to move laterally through target environments. By exploiting short log retention periods and the lack of detailed logging for routine administrative activity in financial institutions, they maintained persistent access that evaded detection for months or years.

The DFPI (California Department of Financial Protection and Innovation) issued explicit warnings to regulated financial institutions about the Volt Typhoon threat, noting that the campaign was not designed for immediate exploitation but for pre-positioning: establishing covert footholds that could enable disruptive or destructive operations at a time of China's choosing — for instance, during a military confrontation over Taiwan. CISA Director Jen Easterly publicly stated that discovered intrusions likely represented the tip of the iceberg of Chinese presence in US critical infrastructure.

The Salt Typhoon campaign of 2024 expanded this picture further, targeting US telecommunications companies and, through them, the communications infrastructure used by financial regulators, law enforcement, and major institutions. The compromise of telecommunications infrastructure creates systemic risks for financial services: surveillance of executive communications, interception of authentication messages, and the potential to disrupt the out-of-band communication channels that firms rely upon for incident response and crisis management.

Beyond direct intrusion, the US-China competition creates significant supply chain risk for financial institutions. Chinese-origin hardware components, software libraries, and managed services represent potential vectors for pre-positioned access or data collection at scale. The growing regulatory scrutiny of Chinese technology in critical financial infrastructure — reflected in guidance from Treasury, the OCC, and European equivalents — acknowledges this risk, but the practical challenge of auditing deep supply chains remains formidable.

> *Strategic Implication: The Chinese threat model is fundamentally about strategic optionality. Compromised footholds in financial infrastructure are not activated immediately but preserved as leverage. This demands threat modeling that extends beyond current adversarial intent to future geopolitical scenarios. Financial institutions should treat pre-positioning by sophisticated APTs as a present-tense risk, not a future hypothetical.*

2.3 Middle East Tensions: Destructive Malware and Regional Financial Disruption

Iran's cyber offensive capabilities have evolved substantially over the past decade, and the financial services sector has been an explicit target of Iranian-linked threat actors during periods of heightened regional tension. Iranian operations are distinguished by a willingness to deploy destructive malware — software designed not merely to compromise or extract data, but to permanently destroy systems — a tactic with significant implications for financial institutions managing critical transactional infrastructure. The Shamoon malware family, deployed against Saudi Arabian energy and financial institutions in 2012 and again in 2016-2017, demonstrated Iran's capacity and willingness to cause irreversible operational damage. The 2012 attack against Saudi Aramco destroyed approximately 30,000 computers by overwriting master boot records, rendering them permanently inoperable. Subsequent variants have been deployed against targets across the Gulf Cooperation Council (GCC), with financial institutions, government ministries, and energy companies consistently appearing in the target set.

APT34 (OilRig), assessed to operate on behalf of Iranian intelligence, intensified its operations through 2024 in a notable evolution of its tradecraft. Beyond its historical focus on espionage and credential theft, APT34 pivoted to collaboration with ransomware operators following infrastructure compromises, obtaining revenue shares from ransom payments in what amounts to an intelligence-criminal hybrid business model. This convergence of state espionage infrastructure with financially motivated ransomware is a significant development: it allows state actors to generate hard currency while conducting intelligence operations, obscures attribution through criminal intermediaries, and exposes targeted financial institutions to both data exfiltration and operational disruption simultaneously.

The broader Middle Eastern threat landscape is shaped by escalating regional tensions, including the ongoing Israel-Gaza conflict and its reverberations across the region. Pro-Iranian and pro-Palestinian hacktivist groups have targeted financial institutions in Israel, the United States, and European countries perceived as aligned with Israel, deploying DDoS attacks and defacement campaigns. CYFIRMA's analysis of the regional cyber threat landscape notes that advanced persistent threat actors are expected to target financial institutions, energy companies, and government entities across the region with increasingly sophisticated toolsets as regional instability continues.

> *Risk Factor: Financial institutions with significant Middle Eastern operations, correspondent banking relationships, or exposure to Gulf sovereign wealth fund investments must account for the possibility that cyber operations targeting regional financial infrastructure could directly affect their operational continuity and data security, particularly during periods of military escalation.*

2.4 The Global Dimension: Spillover Effects and Systemic Financial Risk

A defining characteristic of contemporary geopolitical cyber operations is their tendency to produce collateral damage and spillover effects that transcend the intended target geography. The NotPetya attack, nominally targeting Ukrainian financial and government infrastructure, caused an estimated $10 billion in global damages across 65 countries. Pharmaceutical companies, shipping firms, and international banks

sustained significant losses as the wiper malware propagated through corporate networks connected to Ukrainian subsidiaries and supply chain partners.

The interconnected architecture of global financial services amplifies this spillover risk. Correspondent banking networks, shared payment rails, global custodian chains, and cross-border treasury operations create pathways through which a significant cyber incident affecting one jurisdiction's financial infrastructure can cascade rapidly into others. The IMF has explicitly noted that rising cyber threats pose serious concerns for financial stability, with the potential for a cyber incident to trigger confidence crises, liquidity shortfalls, and contagion effects across the financial system.

The DTCC's 2025 Systemic Risk Barometer identified geopolitical risk and cyber risk as the two dominant concerns among senior financial industry participants, noting that these two risk categories are increasingly inseparable — geopolitical tensions directly fuel the intensity and targeting of cyber operations against financial infrastructure. The financial system's role as the nervous system of the global economy means that its disruption is an attractive objective for any actor seeking to impose costs on adversarial states at scale.

Table 1: Geopolitical Threat Actor Summary — Financial Services

Actor / Region	Primary Group(s)	Preferred Methods	Financial Sector Target
Russia	KillNet, Sandworm, GRU	DDoS, destructive malware, ransomware	Banks, SWIFT, payment processors
China	Volt Typhoon, Salt Typhoon	LotL, credential theft, pre-positioning	Financial infrastructure, telco, regulators
Iran	APT34, Charming Kitten	Ransomware, data wipers, credential theft	GCC banks, US/EU institutions
Hacktivists	Anonymous Sudan, ZCrew	DDoS, defacement, data leaks	Politically aligned institutions

3. THE AI REVOLUTION IN CYBER OFFENSE

Artificial intelligence is the most significant force multiplier in offensive cyber operations since the emergence of organized cybercrime as a profession. Its impact is not confined to a single attack vector or threat actor category: AI enhances every phase of the cyber kill chain — from reconnaissance and weaponization to delivery, exploitation, persistence, and exfiltration. For financial services organizations, this translates into a step-change increase in the volume, velocity, and sophistication of attacks they must defend against.

3.1 Generative AI as an Attack Enabler

The advent of large language models and generative AI systems has fundamentally altered the economics of social engineering. Phishing — historically constrained by the telltale markers of machine-translated text, implausible sender identities, and generic lures — has been transformed into a precision instrument. Generative AI systems can synthesize highly contextual, grammatically flawless spear-phishing communications at scale, drawing on publicly available information about target individuals, their employers, their colleagues, and their recent professional activities.

By late 2024 and early 2025, over 80% of phishing emails identified by security researchers involved some form of AI assistance. The volume impact is equally dramatic: the number of reported AI-enabled cyber attacks rose by 47% globally in 2025, with financial services organizations bearing a

disproportionate share of this increase. Finance and insurance sector entities experienced 18.2% of all AI-driven incidents globally — the highest concentration of any single sector.

Beyond email, generative AI enables the automated creation of fraudulent websites, fake regulatory notifications, counterfeit customer communications, and synthetic identity documents at previously unachievable scale. The ability to generate convincing on-demand content across multiple languages and regulatory jurisdictions simultaneously is particularly significant for multinational financial institutions whose customers, counterparties, and staff operate across diverse geographies.

> *Emerging Threat Vector: AI-powered voice synthesis tools are now capable of real-time voice cloning with minimal audio samples. In 2024, multiple documented cases emerged of voice cloning being used to impersonate senior financial executives in wire transfer authorization calls, resulting in six and seven-figure losses per incident. This threat is expected to intensify significantly through 2026.*

3.2 Autonomous Attack Bots and Automated Exploitation

The automation of cyber attack infrastructure represents a qualitative shift in adversarial capability that financial institutions are not yet adequately calibrated to defend against. Machine learning-enhanced bots have moved beyond static scripted attacks to adaptive systems that learn in real-time from defensive responses, adjusting their behavior to evade detection and improve success rates.

Credential stuffing — the automated use of breached username-password pairs against financial institution login portals — has evolved dramatically through AI augmentation. In 2025, reinforcement learning-trained credential stuffing bots bypassed CAPTCHA and multi-factor authentication protections in 48% of tested scenarios. These bots do not merely replay credentials at scale; they adapt their request timing, IP rotation patterns, and device fingerprinting in direct response to the defensive signals they observe, essentially conducting autonomous red-team exercises against institutional authentication infrastructure in real-time.

AI-powered DDoS attacks reached a record 2.1 million unique incidents in 2025, with approximately 35% of botnet operations incorporating machine learning algorithms to evade detection and adapt targeting in real-time. Volumetric DDoS remains a significant threat to financial institutions' digital customer-facing services, but the emergence of application-layer DDoS — targeting specific API endpoints, authentication workflows, and transaction processing systems with legitimate-appearing traffic patterns — poses a qualitatively different challenge that requires behavioral analysis rather than simple traffic thresholding.

The automation of vulnerability discovery and exploitation represents perhaps the most concerning development in offensive AI capabilities. AI-augmented tools are demonstrably reducing the time between public disclosure of a vulnerability and the availability of working exploits. For financial institutions managing complex, multi-vendor technology stacks with significant technical debt, this compression of the patch-exploitation time window creates systemic exposure that patch management programs designed for a slower threat environment are ill-equipped to address.

3.3 Deepfake and Synthetic Identity Fraud

Deepfake technology — the AI-generated synthesis of realistic audio, video, and imagery — has emerged as a major financial crime enabler with implications spanning fraud, social engineering, market manipulation, and regulatory compliance. The technology has crossed from research curiosity to operational criminal tool in the span of fewer than three years.

In 2024, businesses lost an average of nearly $500,000 per deepfake-related incident, with financial services organizations experiencing average losses of $603,000 — 34% higher than the cross-industry average. In the first three months of 2025 alone, 179 deepfake incidents were formally reported, surpassing

the entire reported total for 2024. Generative AI-enabled fraud in the United States is projected to grow from $12.3 billion in 2023 to $40 billion by 2027, with deepfake-facilitated financial fraud accounting for a substantial and growing share of this figure.

The U.S. Treasury's Financial Crimes Enforcement Network (FinCEN) issued an alert in November 2024 specifically warning financial institutions about a surge in deepfake schemes targeting identity verification processes — the Know Your Customer (KYC) controls that serve as the first line of defense against fraudulent account opening and money laundering. AI-generated synthetic identity documents, combined with deepfake video of fabricated personas, are being deployed to systematically defeat KYC procedures designed for human document review and standard liveness detection algorithms.

A further frontier is the deployment of deepfakes for market manipulation: the generation and distribution of synthetic audio or video content falsely depicting executives of publicly traded financial firms making damaging statements, announcing material events, or conveying false regulatory information. The speed of social media propagation means that even brief exposure to credible-appearing deepfake content can trigger significant market movements before the content is identified as synthetic.

3.4 AI-Augmented Ransomware and Extortion

Ransomware targeting financial institutions has undergone a sustained evolution that AI is now accelerating. The transition from opportunistic to targeted ransomware, the adoption of double-extortion models threatening both operational disruption and data publication, and now the integration of AI capabilities across the attack lifecycle represent compounding increases in threat severity.

AI augmentation of ransomware operations is most visible in three areas: target selection, social engineering for initial access, and negotiation. Machine learning models trained on corporate financial filings, cyber insurance disclosures, and dark web intelligence enable ransomware operators to identify organizations with high revenue, cyber insurance coverage, and limited incident response capability — optimizing the expected return from each operation. AI-generated spear-phishing serves as the primary initial access vector for the majority of successful ransomware deployments, with generative AI dramatically improving the hit rate of phishing campaigns against financial institution employees.

The FBI's Internet Crime Complaint Center (IC3) reported $2.77 billion in Business Email Compromise (BEC) losses in 2024 alone, with AI augmentation consistently appearing in the most financially damaging cases. BEC attacks against financial institutions typically target treasury functions, M&A processes, and correspondent banking relationships — areas where large-value wire transfers occur routinely and where the social engineering of a single individual can yield multi-million-dollar fraud proceeds.

Iran's APT34 group demonstrated in 2024 the emerging model of state-criminal ransomware collaboration: state intelligence actors compromise target infrastructure and then engage ransomware operators to monetize the access, obtaining a portion of ransom proceeds while the criminal group handles negotiation and payment collection. This model allows intelligence services to generate revenue, complicates attribution, and aligns state and criminal incentives in a particularly dangerous combination for financial institutions that face both espionage and extortion risk from a single intrusion.

Table 2: AI-Powered Attack Vectors — Financial Services Impact

Attack Vector	AI Capability Exploited	Primary Impact	Estimated Scale (2025)
Spear phishing	LLM content generation	Initial access, credential theft	>80% AI-assisted
Credential stuffing	Reinforcement learning bots	Account takeover, fraud	48% MFA bypass rate
Deepfake fraud	Generative image/voice/video	KYC defeat, wire fraud	$40B projected by 2027
DDoS	ML-adaptive botnets	Service disruption, extortion	2.1M incidents in 2025
Ransomware / BEC	AI targeting + social eng.	Financial loss, data breach	$2.77B BEC losses (2024)

4. THE CONVERGENCE: GEOPOLITICAL ACTORS ADOPTING AI OFFENSIVE CAPABILITIES

The intersection of geopolitical cyber conflict and AI-powered offensive tools represents the most dangerous dimension of the current threat environment. Nation-state actors — previously distinguished by operational sophistication, patience, and resource depth — are now integrating AI capabilities across their offensive cyber infrastructure, potentially amplifying the scale and impact of operations by orders of magnitude.

The convergence is observable across multiple dimensions. Chinese advanced persistent threat groups have integrated AI-driven analysis into their target profiling and vulnerability research workflows, enabling more precise identification of exploitable weaknesses in specific financial institutions' technology stacks. Russian-aligned actors have demonstrated the use of AI-generated content in influence and disinformation operations designed to undermine confidence in financial systems — fabricated news reports of bank runs, synthetic audio of executive statements, and AI-generated regulatory documents are increasingly deployed in conjunction with technical attacks to amplify their psychological and market impact.

Iran's APT groups have leveraged AI-powered automation in their initial reconnaissance and credential harvesting phases, and the collaboration model between state actors and ransomware operators described in Section 3.4 represents the productization of state cyber capabilities for financial exploitation. North Korean actors, subject to increasingly severe international sanctions that create acute hard currency needs, have deployed AI-augmented cryptocurrency theft operations — targeting exchanges, DeFi protocols, and financial institutions with crypto custody operations — that resulted in estimated losses of $1.5 billion in 2024 alone.

A particularly significant development is the emerging use of AI for supply chain attack optimization. By training models on data about software dependency networks, financial institutions' vendor relationships, and the historical success rates of specific attack techniques against different vendor categories, threat actors can identify the highest-leverage supply chain nodes to compromise — the software libraries, managed services providers, or security vendors whose compromise provides the broadest access to financial institution networks.

The 2020 SolarWinds compromise — in which a Russian intelligence operation compromised a widely used IT management platform and leveraged it to gain access to thousands of organizations including financial regulators and major banks — demonstrated the systemic potential of supply chain attacks. AI-powered optimization of supply chain targeting could enable similar campaigns to be executed with greater speed, broader scope, and reduced operational security requirements.

There is also a meaningful risk that AI systems themselves become vectors for geopolitical cyber operations. Financial institutions' increasing deployment of AI for fraud detection, credit scoring, trading, and risk management creates new attack surfaces: adversarial inputs designed to manipulate AI model behavior, data poisoning attacks on training datasets, and the exploitation of model update mechanisms as intrusion vectors. These represent genuinely novel vulnerabilities that current security frameworks are only beginning to address.

5. IMPLICATIONS FOR FINANCIAL SERVICES ORGANIZATIONS

5.1 Operational Resilience Under Sustained Attack

The threat environment described in this paper demands a fundamental recalibration of how financial institutions conceptualize resilience. Traditional security frameworks, built on the assumption that well-defended perimeters would prevent most intrusions, are inadequate against adversaries with unlimited patience, AI-powered automation, and geopolitically-motivated persistence. The operative assumption for financial institutions in the current environment should be that sophisticated threat actors have achieved, or will achieve, a degree of access to their networks — and that resilience requires the ability to detect, contain, and recover from such access before material harm occurs.

The financial cost of cyber incidents reflects this reality. The average cost of an AI-powered data breach in 2025 reached $5.72 million, a 13% increase over the prior year. For institutions experiencing ransomware incidents, operational disruption costs frequently dwarf ransom demands. The reputational and regulatory consequences of significant incidents — customer notification obligations, supervisory investigations, potential enforcement action — add further dimensions to the cost calculus.

Operational resilience requires investment across the full lifecycle of cyber risk management: threat intelligence, prevention, detection, response, and recovery. The detection and response dimensions are particularly under-resourced in many institutions relative to their prevention investment, a misallocation that the current threat environment makes increasingly costly.

5.2 Regulatory Environment and Compliance Obligations

The regulatory landscape governing financial institutions' cyber resilience has expanded substantially in recent years, with significant new frameworks entering force across major jurisdictions. Understanding the compliance implications of the threat environment described in this paper is essential for both risk management and strategic planning.

The European Union's Digital Operational Resilience Act (DORA), which became enforceable on January 17, 2025, establishes comprehensive requirements for financial entities' ICT risk management, incident reporting, resilience testing, and third-party risk management. DORA represents the most comprehensive regulatory framework for financial sector cyber resilience enacted to date, explicitly addressing the systemic risk implications of ICT concentration and third-party dependencies that the threat environment has made visible.

The NIS2 Directive, with a transposition deadline of October 2024 and full implementation expected by October 2026, extends cybersecurity obligations to a broader range of entities including financial market infrastructure providers and creates senior management accountability for cybersecurity governance that aligns with international best practice. NIS2 and DORA are designed as complementary frameworks, with DORA's financial sector specificity layered on the broader baseline established by NIS2.

In the United States, the OCC, Federal Reserve, and FDIC's joint Computer-Security Incident Notification Rule requires rapid notification of significant cybersecurity incidents, while the SEC's cybersecurity disclosure rules require publicly traded firms to make material determinations about cyber incidents and to disclose material cybersecurity risks and governance in annual reports. FinCEN's November 2024 alert on deepfake fraud added AI-specific guidance to the existing BSA/AML framework.

The AI Act, enacted by the European Union in 2024, creates a risk-tiered regulatory framework for AI systems across sectors, with implications for financial institutions deploying AI in credit decisions, fraud detection, and compliance monitoring. While the AI Act's primary focus is on fairness and transparency in AI decision-making rather than cybersecurity per se, its requirements for high-risk AI systems intersect meaningfully with the security risks described in this paper, particularly regarding adversarial robustness and data integrity.

5.3 The Human Dimension: Insider Threat and Social Engineering at Scale

The AI-powered social engineering capabilities described in this paper reframe the insider threat problem in important ways. Traditional insider threat programs focus primarily on malicious insiders — employees or contractors with legitimate access who intentionally abuse it. The current threat environment adds a second dimension: the weaponized insider, an employee who is manipulated through AI-enhanced deception into performing actions that enable external threat actors. Business Email Compromise, deepfake-assisted wire transfer fraud, and AI-generated impersonation of executives all rely on this mechanism.

The scale at which generative AI can produce convincing social engineering content means that the frequency of manipulation attempts targeting financial institution employees will continue to increase. Security awareness training programs designed for a threat environment characterized by relatively low volumes of detectable phishing face a significant calibration challenge. The relevant question is not merely whether employees can identify phishing emails, but whether operational controls, authorization workflows, and verification procedures are robust enough to prevent harm even when employees are successfully deceived.

6. STRATEGIC RECOMMENDATIONS

The threat convergence described in this paper calls for a response that is equally convergent — integrating geopolitical intelligence, AI-specific security measures, and traditional cyber resilience disciplines into a coherent strategic framework. We organize recommendations across three stakeholder groups: security and risk leadership within financial institutions, boards of directors and executive management, and regulators and industry bodies.

6.1 For Security and Risk Leadership

Geopolitical threat intelligence must be integrated into security operations. Financial institutions should establish formal processes for monitoring geopolitical developments and translating their implications into specific threat assessments. The correlation between the Russia-Ukraine conflict and DDoS attack frequency, or between US-China tensions and Chinese APT activity, is not coincidental. Security teams that monitor geopolitical conditions alongside technical threat intelligence will be better positioned to anticipate attack surges, pre-deploy defensive capabilities, and brief executive leadership on emerging risks.

Threat modeling should explicitly address pre-positioned adversary access. The Volt Typhoon model — persistent but dormant access, activated at a time of adversarial choosing — is not detectable through conventional reactive security operations. Financial institutions should conduct adversary simulation exercises premised on the assumption that sophisticated state-affiliated actors may already have access to

portions of their environment and design detection and response capabilities accordingly. This includes investment in behavioral analytics, network traffic baselining, and privileged account activity monitoring. AI system security deserves dedicated architectural attention. AI models deployed for fraud detection, credit decisioning, and trading should be treated as high-value targets requiring their own threat models. This includes protection of training data integrity, monitoring of model inference behavior for signs of adversarial manipulation, and security review of the model update and deployment pipeline. The emerging discipline of ML security needs to be integrated into the financial institution's broader security architecture, not treated as an afterthought to model development.

Third-party and supply chain risk management must evolve to match the sophistication of supply chain attack techniques. Vendor security assessments focused on point-in-time certification are insufficient against adversaries who optimize supply chain targeting using AI. Continuous monitoring of vendor security posture, contractual requirements for notification of significant incidents, and architecture decisions that limit the blast radius of third-party compromises are all necessary components of an effective supply chain security program.

Deepfake-resistant verification protocols should be implemented for all high-value transactions. Financial institutions should mandate dual-channel, out-of-band verification for wire transfers, executive authorization for unusual financial instructions, and periodic review of KYC procedures in light of the demonstrated ability of AI-generated synthetic identities to defeat current liveness detection algorithms.

6.2 For Boards and Executive Management

Boards should treat geopolitical cyber risk as a board-level governance responsibility. The correlation between geopolitical events and cyber attack frequency means that boards need sufficient understanding of the geopolitical environment to ask informed questions about their institution's preparedness. Geopolitical risk briefings should be a standard component of board risk committee agendas, with explicit linkage to the institution's cyber risk posture.

Investment in cyber resilience should be proportionate to the threat environment, not to historical loss experience. Many institutions calibrate security investment based on experienced losses, a backward-looking approach that is particularly ill-suited to a threat environment where the risk is dominated by tail events — the low-frequency, high-severity incidents that geopolitical actors may execute with little warning. Stress testing of cyber resilience scenarios analogous to the financial stress testing already conducted under regulatory requirements should inform capital allocation for cyber risk management.

Incident response capabilities should be exercised regularly and realistically. Tabletop exercises premised on sophisticated, multi-vector attacks — including geopolitically motivated infrastructure disruption, AI-assisted social engineering, and supply chain compromise scenarios — provide the most value. The response to a significant cyber incident requires coordination across business continuity, communications, legal, regulatory affairs, and technology functions that benefit from rehearsal under realistic conditions.

6.3 For Regulators and Industry Bodies

Regulators should develop geopolitical cyber risk guidance that assists institutions in translating geopolitical intelligence into operational security measures. The frameworks established under DORA and NIS2 provide strong structural foundations, but the specific threat intelligence integration, geopolitical scenario stress testing, and AI system security requirements these frameworks imply deserve more granular supervisory guidance.

Cross-border regulatory coordination on cyber threat intelligence sharing needs to be strengthened. The financial system's global interconnection means that cyber threats to financial stability respect neither national boundaries nor regulatory jurisdictions. Enhanced mechanisms for sharing threat intelligence

between financial sector regulators across jurisdictions — including those who do not share common alliance frameworks — would materially improve the collective resilience of the global financial system. Industry standards for AI system security in financial applications should be developed as a priority. The EU AI Act and existing sectoral frameworks do not fully address the adversarial robustness requirements specific to high-stakes financial AI systems. Industry bodies including the Basel Committee, IOSCO, and the FSB are well-positioned to develop standards and guidance that address AI security alongside AI governance, fairness, and explainability requirements.

7. CONCLUSION

The cyber threat environment confronting financial services organizations in 2026 is characterized by a convergence of two structural forces that individually would represent serious challenges but together create a qualitatively transformed risk landscape. Geopolitical competition has made financial infrastructure a deliberate target in strategies of deterrence, coercion, and hybrid conflict. Artificial intelligence has simultaneously lowered the barriers to sophisticated offensive capability and raised the potential scale of harm that motivated actors can inflict.

This convergence is not a temporary condition created by specific geopolitical crises that will resolve. The rivalry between great powers that is driving state-sponsored cyber activity is a generation-long phenomenon. The proliferation of AI offensive capabilities to criminal groups and state actors alike is irreversible. Financial institutions and their regulators must therefore build resilience frameworks calibrated to this permanent state of heightened threat, not episodic crisis.

The recommendations in this paper are oriented toward building durable resilience: intelligence-led security operations that integrate geopolitical awareness, architectural defenses against pre-positioned adversary access, AI system security as a first-class discipline, human-resistant verification workflows for high-value transactions, and governance frameworks that bring board-level accountability to cyber risk proportionate to its systemic significance.

The financial system is too important to the functioning of modern economies — and too attractive a target to motivated adversaries — for security investment calibrated to past experience to be sufficient. The institutions and jurisdictions that recognize this reality and invest accordingly will be markedly better positioned to maintain operational continuity, protect their customers, and support the stability of the broader financial system in the face of the threats this decade will bring.

REFERENCES:

1. CISA (2024). PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Cybersecurity and Infrastructure Security Agency Advisory AA24-038A. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a
2. CISA (2025). Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System. Advisory AA25-239A.
3. DFPI (2024). Volt Typhoon Cybersecurity Threat Warning for Financial Institutions. California Department of Financial Protection and Innovation. https://dfpi.ca.gov
4. DTCC (2024). Geopolitical and Cyber Risks Remain Top Threats to the Financial Services Sector in 2025. Systemic Risk Barometer Report. December 2024.
5. ENISA (2025). Threat Landscape: Finance Sector, January 2023 to June 2024. European Union Agency for Cybersecurity. https://www.enisa.europa.eu
6. ECB (2025). Cyber Threats to Financial Stability in a Complex Geopolitical Landscape. Financial Stability Review Focus Article, May 2025. https://www.ecb.europa.eu
7. FBI IC3 (2024). Internet Crime Report 2024. Federal Bureau of Investigation Internet Crime Complaint Center.

8. FDIC (2024). 2024 Risk Review: Operational and Cyber Risks. Federal Deposit Insurance Corporation. https://www.fdic.gov
9. FinCEN (2024). Alert on Surge in Deepfake Schemes Powered by Generative AI. U.S. Treasury Financial Crimes Enforcement Network. November 2024.
10. FS-ISAC (2024). Navigating Cyber 2024: New Cyber Threats to Challenge Financial Services Sector. Financial Services Information Sharing and Analysis Center. https://www.fsisac.com
11. IMF (2024). Rising Cyber Threats Pose Serious Concerns for Financial Stability. IMF Blog, April 2024. https://www.imf.org
12. Intel 471 (2024). Pro-Russian Hacktivism: Shifting Alliances, New Groups and Risks. https://www.intel471.com
13. KELA Cyber (2024). Russia-Ukraine War: Pro-Russian Hacktivist Activity Two Years On. https://www.kelacyber.com
14. New Lines Institute (2024). 2024: When China's Salt Typhoon Made Cyberspace Tidal Waves. https://newlinesinstitute.org
15. ORX (2025). Geopolitical Uncertainty is Accelerating Cybercrime as Top Risk. https://orx.org
16. Palo Alto Networks Unit 42 (2024). Evolution of Iran Cyber Threats: From MBR Wipers to Identity Weaponization. https://unit42.paloaltonetworks.com
17. Quorum Cyber (2025). The Key Cyber Threats Facing the Financial Services Sector in 2025. https://www.quorumcyber.com
18. Stanton Chase (2025). Banking on Thin Ice: Major Threats Banks Are Already Facing in 2025. https://www.stantonchase.com
19. Trellix (2024). The Iranian Cyber Capability. https://www.trellix.com
20. Trustwave SpiderLabs (2023). KillNet, Anonymous Sudan, and REvil Unveil Plans for Attacks on US and European Banking Systems. https://www.trustwave.com
21. U.S. Treasury (2024). Treasury Sanctions Company Associated with Salt Typhoon and Hacker Associated with Treasury Compromise. https://home.treasury.gov
22. CYFIRMA (2024). Regional Stability on Shaky Ground: Cyber Threat Escalation in the Middle East. https://www.cyfirma.com