America’s Cyber Crossroads: Deepening the Response to China’s Active Deterrence

Infosources™

September 1, 2025

In an era when digital networks form the backbone of national power, China’s sophisticated cyber campaign—best exemplified by the multistage Salt Typhoon operation—has exposed critical vulnerabilities in American infrastructure. From carriers’ firewalls to water-treatment controls, Beijing’s blend of pre-positioned malware and “active defense” doctrine turns civilian systems into strategic levers. This narrative explores how the United States can bridge its reactive patchwork of defenses, harness AI-driven digital twins and forge credible offensive capabilities to secure its networks and deter aggression.

The Salt Typhoon Breach

American technological leadership—from software and cloud services to AI and cybersecurity—was dealt a severe blow three years ago by “Salt Typhoon.” Chinese state-linked hackers exploited vulnerabilities in U.S. telecom firewalls and reused stolen credentials to gain administrator access to major carriers. Once inside, they copied conversations, tracked intelligence and law-enforcement movements, and spread laterally across networks. This global campaign remains only partly understood, its true scope still hidden beneath layers of covert malware implants. Salt Typhoon was not an isolated success. Analysts have since uncovered Chinese malware embedded in U.S. energy grids, water treatment plants, pipelines and transportation systems. These implants are less about data theft than sabotage: pre-positioned backdoors could be activated to trigger cascading power outages, disrupt air-traffic control or delay military mobilization. Even the threat of such attacks raises domestic political costs and serves as a powerful tool of strategic coercion.

Authoritarian Governance vs. U.S. Patchwork Defense

Beijing’s Great Firewall began as a censorship mechanism in the 1990s but evolved into a state-mandated cybersecurity shield. Its integrated filtering infrastructure screens for malicious code before it reaches critical systems, enforcing uniform protections across Chinese water, power, telecom and transport networks. By contrast, America’s critical infrastructure is owned by thousands of private operators with uneven security investments. U.S. law restricts government monitoring without explicit consent, honoring Fourth Amendment protections but leaving wide blind spots. When attackers breach networks, they are hard to evict—and often return.

A Pattern of Persistent Threats

This episode was only the most dramatic strike in a broader pattern of digital assaults on American networks. In 2020, Russian hackers weaponized SolarWinds’ software supply chain to infiltrate government and corporate systems. The following year, the DarkSide gang brought the Colonial Pipeline to its knees and an Iranian group tested water-treatment controls in Ohio. That same year, a breach at Okta exposed corporate customer support systems, and in 2023 Chinese actors exploited a Microsoft cloud vulnerability to compromise senior U.S. officials’ inboxes—so alarming that federal leaders began publicly warning of “real-world harm.”

year	Incident	Adversary $ Impact
2020	SolarWinds supply-chain compromise	Russian actors inserted spyware into government and corporate networks
2021	Colonial Pipeline ransomware attack	DarkSide criminal gang halted East Coast fuel deliveries for days
2022	Okta identity-management breach	State-linked group accessed corporate customer support systems, leading to data theft
2023	U.S. water plant control system probe	Iranian hackers gained limited access to water-treatment infrastructure
2024	Microsoft cloud vulnerability exploited	Chinese actors breached senior official email accounts, triggering “real-world harm” alerts

This timeline underscores that U.S. defenses are tested not only by China but by Russia, Iran and criminal groups—each probing gaps in pipelines, grids and hospitals.

From Censorship to Cyber Defense: The Great Firewall

China’s success rests on a dual-use evolution of the Great Firewall. What began in the late 1990s as a censorship tool has become a real-time security gateway, screening out malicious code before it ever reaches power grids, water plants, telecommunications hubs or transportation networks. Every critical system in China sits behind a uniform, state-mandated shield. By contrast, America’s infrastructure—the pipelines, rail lines and water utilities that underpin daily life—belongs to thousands of private operators with wildly varying budgets and cybersecurity expertise, and U.S. law prohibits government monitoring without explicit consent. When adversaries gain entry, they often linger unseen, primed to resurface.

Active Defense Doctrine and Dual-Use Networks

Underpinning Beijing’s strategy is the People’s Liberation Army’s doctrine of active defense, which reframes offense as the ultimate form of protection. China’s “active defense” doctrine treats offense as the best form of defense, embedding cyber-attack capabilities directly into military strategy. Units like Shanghai’s notorious 61398 and the PLA’s Strategic Support Force have grown into multi-billion-dollar cyber operations capable of embedding covert backdoors in dual-use networks.
Diplomatic efforts—from the 2015 Obama–Xi accord to Trump-era indictments and Biden-Xi election-noninterference promises—have failed to curb intrusions. In 2023, state-linked actors even exploited a Microsoft cloud flaw to access senior U.S. officials’ emails, prompting public warnings of “real-world harm.”

Rather than one-off espionage, China’s operators have:

- Gained administrative control of water treatment, power grid and rail supervisory systems
- Installed covert backdoors and stealthy malware that remain dormant until activation
- Positioned implants in dual-use networks—civilian systems that support military mobilization

These capabilities deliver both strategic deterrence and tactical leverage:

- Strategic Deterrence: Threats to disrupt rail or power networks can deter U.S. intervention in a Taiwan crisis by raising domestic political costs without kinetic strikes.
- Tactical Leverage: Disabling civilian infrastructure around U.S. bases or ports can slow reinforcement without overtly targeting military assets.
- Plausible Deniability: Civilian system failures can be passed off as technical glitches, masking China's hand and raising barriers to retaliation.

From Reactive Mandates to AI-Powered Digital Twins

Recognizing the defense gap, the Biden administration used emergency authorities to impose minimum cybersecurity standards on pipelines, rail networks, airports and water utilities—mandates that enable the TSA and other regulators to inspect and guide operators. Yet these post-incident reporting requirements and periodic checks fall far short of China's real-time monitoring and have been legally challenged in key sectors.
The United States lacks a unified view of critical defenses. Artificial intelligence offers a solution in the form of AI-generated "digital twins"—dynamic virtual replicas of physical systems that mirror performance using live sensor data. Industry and governments already deploy digital twins to enhance safety and efficiency:

- Rolls-Royce monitors jet engines
- Ford and BMW refine manufacturing processes
- Singapore and NATO simulate attacks on water and power networks

A national initiative—starting with a Department of Energy pilot on the U.S. power grid—would allow operators to:

- Simulate cyber-sabotage and DDoS scenarios safely
- Identify and prioritize the most critical vulnerabilities
- Establish behavioral baselines that flag anomalies early
- Run force-on-force cyber wargames to validate defenses

Technical hurdles (data sharing, proprietary networks) and partnership frameworks remain, but digital twins can finally bridge America's physical-digital divide, giving leaders near-real-time readiness assessments and transforming U.S. cyberpolicy from reactive patchwork into proactive deterrence. With an estimated $5 billion investment over five years, defenders could safely probe every vulnerability, establish anomaly baselines, prioritize patches and refine both defensive playbooks and offensive responses.

Beyond Defense: Offensive Capabilities and Strategic Messaging

Yet defense alone cannot restore the U.S. edge. True cyber-deterrence demands a credible offensive capability focused on Chinese military targets and logistics hubs—under international law, a more legitimate alternative to targeting civilian networks. Washington must publicly and persistently declare that it will attribute attacks rapidly, demonstrate resilient recovery, and retaliate whenever Beijing crosses clearly drawn red lines. The warning must be vivid enough to prove capability without exposing critical gaps—over-sharing only encourages adversaries to harden their weakest points, as Russia's early blackout probes taught Ukraine.

Coalition Building and Global Cyber Norms

To cement this posture, the United States should lead a coalition of democracies in sharing real-time threat intelligence via Five Eyes, embedding digital-twin exercises into NATO's annual cyber wargames, and aligning standards with Europe's NIS 2 directive. Politicians in Congress must overcome inertia, mandate continuous network monitoring, secure sustained funding for AI and offensive R&D, and establish legal guardrails for private-public data partnerships.

Conclusion: The Imperative for Action

Political inertia and private-sector resistance have stalled comprehensive reform: Congress has resisted expanding legal authorities and sustained funding, while operators balk at costly mandates. But waiting is no longer an option. Artificial intelligence will only deepen China's lead unless the United States harnesses its technical prowess, economic resources and innovative spirit.

With decisive vision and political will, America can reclaim strategic balance in cyberspace. By mandating continuous monitoring, deploying AI-powered digital twins, building forward-leaning cyberoffense and sharpening strategic messaging, the U.S. can secure its digital home front, set global norms for democratic resilience and deter authoritarian "active deterrence" for decades to come.