Critical Insights Series

The Silent Storm:
Why Our Cybersecurity Strategy Must Evolve

**David Mussington,
Ph.D, CISSP, DDN.QTE**

Professor of the Practice
University of Maryland
School of Public Policy

Advisor and Fellow
Mission Critical

MISSION CRITICAL
Collaborative Critical Infrastructure
Cybersecurity Research

About Mission Critical

Mission Critical facilitates collaboration between academia, industry, and government to develop proactive, nonpartisan, and peer-reviewed research that improves critical infrastructure security and resilience.

About the Critical Insights Series

This Critical Insights Series showcases the unparalleled perspectives of Critical Infrastructure Information Security Thought Leaders from across the public and private sectors. All thoughts expressed belong solely to the author and may not reflect those of their employer, affiliated organization(s), or Mission Critical.

About the Author

David Mussington, Ph.D, CISSP, DDN.QTE

Professor of the Practice,
University of Maryland's School of Public Policy,

Former Executive Assistant Director for Infrastructure Security,
US Cybersecurity & Infrastructure Security Agency (CISA)

Advisor & Fellow,
Mission Critical

Dr. David Mussington is Professor of the Practice at the University of Maryland's School of Public Policy. Prior to rejoining UMD in January 2025, David served as the Executive Assistant Director for Infrastructure Security at the Cybersecurity and Infrastructure Security Agency, US Department of Homeland Security. At CISA, David was one of three Presidentially appointed officials charged with implementing the nation's critical infrastructure security and resilience strategies and plans across 16 critical infrastructures. He also led interagency efforts on counter- and anti- terrorism efforts, playing a leading role in reducing the risks of domestic targeted violence, school safety, and physical infrastructure security standards. He was also a founding member of CISA's Cyber Safety Review Board.

David has extensive public and private sector experience in cyber and infrastructure security. He was selected for the Senior Executive Service and assigned to the Office of the Secretary of Defense in the role of Senior Advisor for Cyber Policy, later joining the NSC staff as Director for Surface Transportation Security Policy. As a researcher at RAND Corporation, and later at the Institute for Defense Analyses, David directed cybersecurity studies for the Department of Homeland Security (DHS), the Office of the Director of National Intelligence (ODNI), the Federal Communications Commission (FCC), the Bank of Canada, and NATO. David has a Ph.D in Political Science from Canada's Carleton University, and MA and BA degrees from the University of Toronto. He undertook post-doctoral study at Harvard's Belfer Center, and at the UK's International Institute for Strategic Studies.

In 2021, David was elected a life member of the Council on Foreign Relations. In 2023, David was awarded Homeland Security Today's Mission Award for contributions to the US Critical Infrastructure Security and Resilience mission. In 2024, he received the Impact Award from the Institute for Critical Infrastructure Technology (ICIT) for leadership in critical infrastructure policy and strategy.

The Silent Storm: Why Our Cybersecurity Strategy Must Evolve

Cyber activities conducted by or at the direction of the People's Republic of China have long been the topic of public comment by federal officials. Bemoaning the theft of intellectual property and sensitive data is a commonplace in Washington among those concerned or responsible for protecting critical infrastructures and sensitive data. So, what is the renewed urgency about? What has changed since the early 2010s to introduce a qualitatively different dimension to cyber defense and international stability discussions? Improvements in analytics and detection techniques have allowed for the drawing of refined and alarming conclusions from years of research.

Volt Typhoon and Salt Typhoon are not just “hacking” – they are pre-positioning inside civilian lifelines to enable coercion of democratic societies in a crisis, which demands treating their activity as battlespace preparation across utilities, telecom, lawful intercept, and cloud control channels rather than garden-variety espionage [1][2].

What Has Changed?

U.S. and Five Eyes agencies now assess with high confidence that PRC operators have quietly embedded themselves in U.S. communications, energy, transportation, and water systems for years using living-off-the-land tradecraft – a posture designed for potential disruption under geopolitical stress rather than mere collection [1][2].

CISA, NSA, FBI, and allied partners elevated the warning in late 2025 with a joint advisory describing a global compromise ecosystem feeding a broader espionage system and urging standardized mitigations across sectors, underscoring the structural—not episodic—nature of the threat [1][3].

Volt Typhoon’s Evolution

Recent joint analyses document Volt Typhoon's long-dwell access in combined electric and water environments, harvesting OT-relevant data and exploiting IT-to-OT seams that could be flipped from access to effects to generate outsized societal panic during crises [2][4].

Defenders are urged to prioritize identity hardening, network segmentation, and verbose authentication and command-line logging because the actor leans on valid credentials and poor segmentation to persist invisibly across enterprise and OT boundaries [1][2].

Salt Typhoon's Escalation

Allied threat assessments highlight that even when direct impacts appear concentrated in the United States, highly integrated North American and transatlantic infrastructure means cascading effects would propagate across borders in a crisis, making this a geopolitical infrastructure vulnerability rather than a single-country problem [1][8].

Microsoft's actor taxonomy clarifies that multiple PRC clusters—Volt, Salt, and others—are concurrently adapting toward supply chain, cloud identity planes, and telecom signaling, accelerating the shift from enclave intrusions to ecosystem-level pre-positioning [9][10].

How This is Different

Allied threat assessments highlight that even when direct impacts appear concentrated in the United States, highly integrated North American and transatlantic infrastructure means cascading effects would propagate across borders in a crisis, making this a geopolitical infrastructure vulnerability rather than a single-country problem [1][8]. Cloud identity and remote management tools are now the preferred initial access vectors for PRC clusters targeting downstream services, making control-plane security and supply-chain hygiene decisive for national resilience [10][14].

Microsoft's actor taxonomy clarifies that multiple PRC clusters—Volt, Salt, and others—are concurrently adapting toward supply chain, cloud identity planes, and telecom signaling, accelerating the shift from enclave intrusions to ecosystem-level pre-positioning [9][10]. Salt Typhoon's focus on telecom and cloud lawful intercept and signaling systems exposes a privileged attack surface where compromise yields strategic visibility and coercive potential, demanding Tier-0 treatment, separated credential domains, and continuous auditing at carriers [1][7].

Some Digital Sovereignty Fault Lines

Europe's Cyber Diplomacy Toolbox formalizes coordinated diplomatic, legal, and restrictive measures—including sanctions—to respond to malicious cyber activity, offering a model for allied action when extraterritorial cloud and telecom stacks become vectors of strategic risk [11].

The EU's IRIS² secure connectivity program further codifies a sovereignty-minded approach to satellite connectivity and government communications resilience, an emerging template for allied space-to-ground governance amid rising cyber and hybrid threats [12].

A Division of Labor That Works

A partnership between federal, state, and local agencies and the private sector has long been the bedrock of U.S. critical infrastructure security and resilience efforts. This arrangement needs to be extended to include better structuring of information sharing and response – a requirement for the more severe threat environment in which we find ourselves.

CISA and Sector Risk Partners	Department of War (USCYBERCOM, Service Cyber, CMF)	Law Enforcement (FBI and Partners)
Lead civilian critical infrastructure defense, publish LOTL-focused hunting guidance, drive identity-first mitigations and IT/OT separation, and convene joint advisories to raise baseline telemetry and segmentation across sectors [1][2].	Treat PRC pre-positioning as battlefield preparation and counter with defend-forward campaigns synchronized with domestic resilience to protect decision-making and mobilization pathways under duress [1][13].	Investigate intrusions, attribute, impose consequences, and surge incident response with carriers and utilities, turning joint advisories into legal actions and operational disruptions at scale [3][14].

What To Do Now

Urgent implementation of recommended practices – both on a pilot and readily scalable and sustainable basis – is required. Some specifics are listed below, but an even greater sense of urgency is necessary.

1

Make Identity, Segmentation, and Logs Boringly Perfect

Phishing-resistant MFA for admins, unique local admin credentials, IT/OT DMZs with bastion-only access, and SIEM-centralized verbose logging to surface LOTL behavior without tipping intruders [1][2].

2

Prioritize Telecom Lawful Intercept and Signaling Security

Classify lawful intercept platforms as Tier-0, isolate credentials, and red-team cross-connects and signaling gateways, assuming adversary lateral movement from MSP/RMM footholds [1][7].

3

Align Ally Playbooks to Sovereignty Reality

Operationalize the EU's cyber diplomacy framework for coordinated responses to carrier abuses and cloud extraterritorial risks while preserving rapid joint hunts so PRC gains in one jurisdiction cannot be parlayed across the alliance [1][11].

The Bottom Line

Volt Typhoon transformed essential services into a glass shelf that can be shattered at Beijing's discretion, and Salt Typhoon extends that choreography to lawful intercept and force-support networks. Conflating campaigns such as Volt Typhoon and Salt Typhoon with conventional espionage misses the point and invites strategic surprise at scale [2][6].

Volt Typhoon, Salt Typhoon, and similar emerging campaigns do not solely rely on the manipulation or exfiltration of data. They are adaptable, multi-faceted, and multi-pronged. In information security, risk is defined as the potential for loss or damage that may occur if a threat exploits one or more vulnerabilities in the context of the assessed likelihood of exploitation and the potential impacts. Effective security strategies depend on identifying, prioritizing, and mitigating critical risks. The necessity to mitigate the risks posed campaigns like Volt Typhoon and Salt Typhoon is urgent and unglamorous, but addressing the underlying exploitable weaknesses is possible: identity real IT/OT choke points, conduct Tier-0 treatment for telecom LI and cloud control planes, and adopt a CISA-DoW-FBI playbook that fuses domestic resilience with defend-forward and legal consequences, amplified by allied sovereignty tools to deny sanctuary and signaling leverage [1][3].

References

[1] “Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System | CISA,” Cybersecurity and Infrastructure Security Agency CISA, Aug. 27, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a

[2] CISA, “PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure | CISA,” www.cisa.gov, Feb. 07, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a

[3] “Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System,” Internet Crime Complaint Center (IC3), Sep. 2025. https://www.ic3.gov/CSA/2025/250827.pdf

[4] C. Snow, “(TLP:CLEAR) Joint Cybersecurity Advisory – Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System | WaterISAC,” Waterisac.org, Aug. 28, 2025. https://www.waterisac.org/tlpclear-joint-cybersecurity-advisory-countering-chinese-state-sponsored-actors-compromise-of-networks-worldwide-to-feed-global-espionage-system (accessed Oct. 22, 2025).

[5] D. DiMolfetta, “Salt Typhoon hacks into National Guard systems a ‘serious escalation’, experts warn,” Nextgov.com, Jul. 16, 2025. https://www.nextgov.com/cybersecurity/2025/07/salt-typhoon-hacks-national-guard-systems-serious-escalation-experts-warn/406765/

[6] D. DiMolfetta, “Salt Typhoon hackers targeted over 80 countries, FBI says,” Nextgov.com, Aug. 27, 2025. https://www.nextgov.com/cybersecurity/2025/08/salt-typhoon-hackers-targeted-over-80-countries-fbi-says/407719/

[7] C. Jaikaran, “Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications,” Congress.gov, Jan. 23, 2025. https://www.congress.gov/crs-product/IF12798

[8] Government of Canada, “National Cyber Threat Assessment 2025-2026 - Canadian Centre for Cyber Security,” Canadian Centre for Cyber Security, Oct. 30, 2024. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

[9] “How Microsoft names threat actors - Unified security operations,” Microsoft.com, Aug. 11, 2025. https://learn.microsoft.com/en-us/unified-secops/microsoft-threat-actor-naming

[10] Microsoft Threat Intelligence, “Silk Typhoon targeting IT supply chain | Microsoft Security Blog,” Microsoft Security Blog, Mar. 05, 2025. https://www.microsoft.com/en-us/security/blog/2025/03/05/silk-typhoon-targeting-it-supply-chain/

[11] Council of the EU, “EN CYBER 98 RELEX 554 POLMIL 77 CFSP/PESC 557 OUTCOME OF PROCEEDINGS From: General Secretariat of the Council,” Council of the European Union, Brussels, Jun. 2017. Available: https://data.consilium.europa.eu/doc/document/ST-10474-2017-INIT/en/pdf

References

[12] “Regulation - 2023/588 - EN - EUR-Lex,” European Union, Mar. 15, 2023. https://eur-lex.europa.eu/eli/reg/2023/588/oj/eng (accessed Oct. 22, 2025).

[13] R. Doshi, “Threats from PRC Cyber Actors and Transnational Criminal Groups for the hearing on “Countering Threats Posed by the Chinese Communist Party to U.S. National Security,” United States House Committee on Homeland Security, Mar. 05, 2025. https://homeland.house.gov/wp-content/uploads/2025/03/2025-03-05-HRG-Testimony.pdf

[14] CISA, “People’s Republic of China Cyber Threat | CISA,” www.cisa.gov, 2024. https://www.cisa.gov/topics/cyber-threats-and-advisories/nation-state-cyber-actors/china

[15] NSA CSS, “NSA and Others Provide Guidance to Counter China State-Sponsored Actors Targeting Critical,” National Security Agency/Central Security Service, Aug. 27, 2025. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4287371/nsa-and-others-provide-guidance-to-counter-china-state-sponsored-actors-targeti/

[16] CISA, “CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization | CISA,” Cybersecurity and Infrastructure Security Agency CISA, Jul. 31, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-212a

[17] CISA and USCG, “CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization,” CISA.gov, Jul. 31, 2025. https://www.cisa.gov/sites/default/files/2025-08/joint-advisory-cisa-identifies-areas-for-cyber-hygiene-improvement-after-conducting-proactive-threat-hunt-508c.pdf

Additional Sources Consulted

[18] A. Costis, “Response to CISA Advisory (AA25-212A) - AttackIQ,” AttackIQ, Aug. 01, 2025. https://www.attackiq.com/2025/08/01/response-to-cisa-advisory-aa25-212a/

[19] A. Costis, “Response to CISA Advisory (AA25-212A): CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization,” Security Boulevard, Aug. 2025. https://securityboulevard.com/2025/08/response-to-cisa-advisory-aa25-212a-cisa-and-uscg-identify-areas-for-cyber-hygiene-improvement-after-conducting-proactive-threat-hunt-at-us-critical-infrastructure-organization/

[20] C. Sivesind, “U.S. CISA, Coast Guard Issue Wake-Up Call for Critical Infrastructure,” Secureworld.io, Aug. 04, 2025. https://www.secureworld.io/industry-news/cisa-coast-guard-critical-infrastructure (accessed Oct. 22, 2025).

[21] J. Kulesza, “Space Diplomacy Toolbox and Digital Sovereignty: Lessons from European Cyber Diplomacy :: EU Cyber Direct,” EU Cyber Direct, Jul. 09, 2025. https://eucyberdirect.eu/blog/space-diplomacy-toolbox-and-digital-sovereignty-lessons-from-european-cyber-diplomacy (accessed Oct. 22, 2025).

[22] A. Rozenshtein, S. Seymour, B. Wales, and J. Patja, “Lawfare Daily: Sezaneh Seymour and Brandon Wales on Private-Sector Cyber Operations,” Lawfare, Aug. 29, 2025. https://www.lawfaremedia.org/article/lawfare-daily--sezaneh-seymour-and-brandon-wales-on-private-sector-cyber-operations (accessed Oct. 22, 2025).

[23] CISA, “CISA and USCG Issue Joint Advisory to Strengthen Cyber Hygiene in Critical Infrastructure | CISA,” Cybersecurity and Infrastructure Security Agency CISA, Jul. 31, 2025. https://www.cisa.gov/news-events/alerts/2025/07/31/cisa-and-uscg-issue-joint-advisory-strengthen-cyber-hygiene-critical-infrastructure (accessed Oct. 22, 2025).

[24] “The EU Cyber Diplomacy Toolbox,” www.cyber-diplomacy-toolbox.com. https://www.cyber-diplomacy-toolbox.com

[25] Center for Global Studies, “Daily Digest on AI and Emerging Technologies (17 July 2025) – Cgs Pam,” Cgspam.org, Aug. 17, 2025. https://www.cgspam.org/governance-and-legislation-3/ (accessed Oct. 22, 2025).

[26] D. Cerda, “Lessons from the CISA and USCG Joint Advisory: What ‘No Breach’ Still Reveals,” CommandPrompt Inc., Sep. 09, 2025. https://commandprompt.com/blog/lessons-from-the-cisa-and-uscg-joint-advisory-what-no-breach-still-reveals/ (accessed Oct. 22, 2025).

[27] “Lawfare Daily: Sezaneh Seymour and Brandon Wales on Private-Sector Cyber Operations | The Lawfare Podcast,” Lawfare, Jul. 29, 2025. https://shows.acast.com/lawfare/episodes/lawfare-daily-sezaneh-seymour-and-brandon-wales-on-private-s (accessed Oct. 22, 2025).

Additional Sources Consulted

[28] CISA and USCG, “CISA and USCG Identify Areas for Cyber Hygiene Improvement After Conducting Proactive Threat Hunt at US Critical Infrastructure Organization | CISA,” Cybersecurity and Infrastructure Security Agency CISA, Jul. 31, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-212a

[29] L. Sadoian, “The EU Cyber Diplomacy Toolbox: Shaping Global Cybersecurity Standards,” Upguard.com, May 03, 2024. https://www.upguard.com/blog/eu-cyber-diplomacy-toolbox (accessed Oct. 22, 2025).
[30] S. Seymour and B. Wales, “Partners or Provocateurs? Private-Sector Involvement in Offensive Cyber Operations,” Lawfare, Aug. 16, 2025. https://www.lawfaremedia.org/article/partners-or-provocateurs--private-sector-involvement-in-offensive-cyber-operations (accessed Oct. 22, 2025).

[31] Council of the European Union, “Revised Implementing Guidelines: EU Cyber Diplomacy Toolbox,” Cyber-diplomacy-toolbox.com, Jun. 08, 2023. https://www.cyber-diplomacy-toolbox.com/Revised_Implementing_Guidelines_Cyber_Diplomacy_Toolbox.html

[15] A. Ribeiro, “CISA identifies OT configuration flaws during cyber threat hunt at critical infrastructure organization, lists cyber hygiene - Industrial Cyber,” Industrial Cyber, Aug. 01, 2025. https://industrialcyber.co/cisa/cisa-identifies-ot-configuration-flaws-during-cyber-threat-hunt-at-critical-infrastructure-organization-lists-cyber-hygiene/

[32] European Union Lex, “EU secure connectivity programme (2023–2027) | EUR-Lex,” Europa.eu, Apr. 24, 2023. https://eur-lex.europa.eu/EN/legal-content/summary/eu-secure-connectivity-programme-2023-2027.html

[33] “IRIS2 | Secure Connectivity - European Commission,” defence-industry-space.ec.europa.eu. https://defence-industry-space.ec.europa.eu/eu-space/iris2-secure-connectivity_en

[34] Council of the European Union, “Regulation (EU) 2023/588 establishing the Union Secure Connectivity Programme for the period 2023-2027 – European Sources Online,” Europeansources.info, Mar. 17, 2023. https://www.europeansources.info/record/proposal-for-a-regulation-establishing-the-union-secure-connectivity-programme-for-the-period-2023-2027/ (accessed Oct. 22, 2025).

[35] THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, “L_2023079EN.01000101.xml,” Europa.eu, Mar. 15, 2023. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32023R0588 (accessed Oct. 22, 2025).

[36] The European Parliament and of the Council of the European Union, “Inhaltsverzeichnis Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 March 2023 establishing the Union Secure Connectivity Programme for the period 2023-2027 (Regulation (EU) 2023/588 of the European Parliament and of the Council of 15 Marc... (32023R0588)) |
Lexaris - Digital Laws,” Lexaris.de, Mar. 16, 2023. https://www.lexaris.de/library/tableofcontents/2055920 (accessed Oct. 22, 2025).

Additional Sources Consulted

[37] European Union Lex, “Regulation - 2023/588 - EN - EUR-Lex,” Europa.eu, Mar. 17, 2023. https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX%3A32023R0588 (accessed Oct. 22, 2025).
[38] Agentschap Innoveren & Ondernemen, “EU Funding Overview,” Eufundingoverview.be, 2023. https://eufundingoverview.be/funding/iris2-the-unions-secure-connectivity-programme (accessed Oct. 22, 2025).

[39] “ Strategic Compass and EU space-based defence capabilities European Parliament resolution of 23 November 2023 Strategic compass and EU space-based defence capabilities (2022/2078(INI)) ,” Europa.eu, Jul. 24, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52023IP0435 (accessed Oct. 22, 2025).

[40] The Commission to the European Parliament, “Report From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the Implementation of the EU Space Programme and on the Performance of the European Union Agency for the Space Programme,” https://european-union.europa.eu/, Oct. 07, 2024. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A52024DC0289

[41] G. Tricco, “The Upcoming Of IRIS2: Bridging The Digital Divide And Strengthening The Role Of The EU In International Space Law,” JLMI, Feb. 2023. https://ojs.unito.it/index.php/JLMI/article/view/7952

[42] M. Sintorn and I. Verduci, “IRIS2: The Dawn of EU Leadership in Space,” FINABEL, Dec. 2023. Accessed: Oct. 22, 2025. [Online]. Available: https://finabel.org/iris%C2%B2-the-dawn-of-eu-leadership-in-space/