Cyberspace Without Edges: Reading The Cyber Defense Review, Volume 11, Number 1

An intelligence-analytic review of the West Point Army Cyber Institute's first 2026 issue

The Army Cyber Institute at West Point, working with civilian scholars, allied authors, and a Ukrainian wartime defender, published the journal's first 2026 issue in early April 2026 (verified — iLovePDF document metadata, April 1, 2026).

The 232-page volume gathers eleven pieces under three headings: Senior Leader Perspectives; Cyber Strategy from Foundations to Operational Practice; and Anticipation, Resilience, and Sustained Advantage. Eleven authors converge on a single finding the United States Government has not yet absorbed.

Competition in cyberspace stays continuous. Classical deterrence frames keep failing. Force generation, doctrine, and analytic methods require rebuilding around persistence, civilian integration, allied alignment, and contested information environments — a shift the volume traces in concrete operational terms.

The issue reaches readers while Salt Typhoon and Volt Typhoon intrusions remain unresolved, People's Republic of China-linked influence networks sustain pressure on Asia-Pacific information systems, and large language models enter cyber early-warning workflows under NATO experimentation.

Salt Typhoon hit telecommunications carriers across more than 80 countries — assessed with high confidence (Federal Bureau of Investigation public statement, August 27, 2025; Wall Street Journal reporting). Volt Typhoon implants stayed pre-positioned in US power and water systems for at least two years before disclosure (Microsoft Threat Intelligence, May 2023; CISA, May 2024 — verified). Russian and Iranian state actors run parallel campaigns against US and allied systems (high confidence — joint NSA/CISA/FBI advisory, September 2024).

Authors assess, likely with high confidence, that the current US cyber force model will not scale to meet adversary tempo without civilian-private integration and tighter allied alignment. Probability of major legislative or executive restructuring in the next 24 months: roughly even. Budget pressure, authorities disputes between the Office of the National

Cyber Director and US Cyber Command, and political turnover remain the binding constraints.

Introduction

The new CDR issue arrives at an awkward moment. Salt Typhoon sits partly contained but not closed — the Federal Bureau of Investigation's top cyber official said as much in July 2025. Volt Typhoon implants stay under observation in US power and water systems. A Japanese active cyber defense law passed in 2025 broke with seven decades of post-war restraint. Editor Carine Lallemand frames the volume as a turn toward analytical rigor at a time when cyber operations sit at the center of national security planning.

What binds the eleven pieces together matters more than any single argument. Authors enter the same problem through different doors. Kramer, Butler, and Teplinsky push for organizational reform. Fischerkeller, Goldman, and Harknett build a typology of operational schemes. A Ukrainian practitioner — Volodymyr Styran of the State Service of Special Communication and Information Protection — offers operational doctrine learned under live conditions. Lentz compares allied posture across the United States, Australia, and Japan. Santacaterina and colleagues map influence operations attributed to PRC actors. Lohmann and Davis test large language models in a NATO laboratory. Shipp, Zgonc, and Harrell with Chojnacki round out the volume with practitioner work on force protection, long-horizon health surveillance, and the economics of counter-drone fires.

The shared current running underneath: cyberspace lacks edges. Defenders no longer get a quiet pre-attack period. Adversaries already operate on the network. Security depends on contesting initiative every day, not on threatening retaliation tomorrow.

Volume Map and Evidence Quality

Table 1. Contributions, Arguments, and Evidence Confidence

Section	Author(s)	Core Argument	Evidence Base	Confidence
Senior Leader	Kramer, Butler, Teplinsky	US needs an Integrated Cyber Provider Corps, civilian cyber reserve, regional resilience districts under the National Cyber Director	Verified Volt and Salt Typhoon attributions; cites Atlantic Council, McCrary Institute, Cyberspace Solarium 2.0 reports	High
Strategy	Fischerkeller, Goldman, Harknett	Cyber operations succeed only when aligned with the military's operational scheme	Single Russia-Ukraine case study, with rich operational detail	Moderate
Strategy	Wolfley, Hedgecock, Winkelstein	Four ideal-type cyber strategies: resilience, selective response, persistence, extraction	Conceptual typology, illustrative not empirical	Moderate (theoretical)
Strategy	Styran	Defenders contest initiative through proactive environmental control - the Offense Death Cycle	First-person Ukrainian wartime defense experience; theoretical grounding in CPT and PETIO	Moderate-High (operational)
Strategy	Lentz	US, Australia, Japan converge on integrated persistence at uneven speeds	Policy text analysis across three countries	Moderate
Resilience	Shipp	Tiered posture changes for expeditionary forces against Ubiquitous Technical Surveillance	Conceptual framework; indicators not yet validated through back-testing	Low-Moderate
Resilience	Lohmann, Davis	Fine-tuned Llama 3.2 3B outperformed nine other models in NATO SAS-183 cyber early-warning tests	Single experimental setting, no adversarial red-team simulation	Moderate (preliminary)
Resilience	Zgonc	Long-horizon health surveillance data faces epistemic failure modes beyond the CIA triad	Practitioner reflection, no quantitative test	Low (conceptual)
Resilience	Santacaterina, Eerhart, Brown, Nelson, Murphy	Seven-part typology of communication hijacking, applied to PRC-linked operations across Asia-Pacific	Multi-platform case studies; inter-rater reliability above 90 percent	Moderate-High
Resilience	Harrell, Chojnacki	RAMPART layered counter-drone framework with adjusted defense cost fraction (aDCF)	Economic model with operational case examples	Moderate

Table 1 summarizes the contributions and the quality of the evidence each rests on.

A pattern jumps out from the table. The strongest contributions sit where authors have hands-on operational data — Styran's Ukrainian defense work, the Santacaterina team's multi-platform influence-operations corpus, and the Lohmann-Davis NATO experiment. The most cautious framing belongs to the conceptual pieces, which is appropriate.

The "Cyber Invasion" Reframing and the Push for a National Cyber Force

Kramer, Butler, and Teplinsky open the volume with a deliberate word choice — "cyber invasion." The framing is not casual. PRC-attributed Typhoon campaigns, in their reading, exceed espionage and represent a functional invasion of US networks. The authors argue that the US Government lacks unity of effort and resources to defeat or deter such campaigns.

Their five-part proposal stacks roughly as follows:

- An Integrated Cyber Provider Corps (ICPC) of cybersecurity and cloud service providers under the National Cyber Director.

- A National Cyber Lab Cohort drawn from federally funded research and development centers, university-affiliated research centers, and national laboratories.

- Wider use of National Guard and Reserve cyber forces, with cross-state agreements.

- A non-military civilian cyber reserve — modeled in part on volunteer firefighter incentive structures.

- Regional Resilience Districts anchored at military installations and major commercial hubs, with private and public participation.

The proposals carry strong evidence support — the Volt Typhoon and Salt Typhoon attributions are verified through Microsoft Threat Intelligence and joint US Government advisories. The recommended structures borrow from existing models like the Houston Ship Channel Security District and the Department of the Treasury's Project Fortress 2025.

Two analytic cautions sit beneath the surface. First, the authors' claim that adversaries run "continuous offensive cyber campaigns" is verified. Their claim that current arrangements have failed, however, runs into a real measurement problem: the absence of a successful catastrophic attack is not the same as the absence of risk. Second, the proposed reforms collide with authority disputes — the National Cyber Director coordinates but does not command, and several of the proposed pillars sit closer to traditional Department of Defense or Department of Homeland Security authorities. Probability of full implementation as proposed within 24 months: roughly even, leaning toward unlikely without legislative push.

Cyber Persistence as Operational Frame

Three pieces share intellectual roots in Cyber Persistence Theory (CPT) — Fischerkeller, Goldman, and Harknett's foundational frame; Styran's operational translation; and Lentz's allied comparison. Reading them in sequence is more instructive than reading any one alone.

Fischerkeller, Goldman, Harknett: Alignment with Operational Scheme

The authors argue that cyber capabilities deliver operational impact only when matched to a state's military operational scheme. Russia's failure during the 2022 Ukraine invasion, in their reading, illustrates the cost of poor alignment. Russia ran cyber operations as standalone strategic-effects bids, disconnected from its kinetic blitzkrieg ambitions. The result: cyber capabilities produced limited battlefield impact even though Russian operators are technically capable.

The framework borrows from Hans Delbrück's distinction between annihilation and attrition strategies, and from Edward Luttwak's attrition-versus-maneuver styles. Authors push past US joint doctrine, which they assess as imprecise on such terms. The argument is theoretically clean. The empirical base is narrower — one case, with the comparison to Ukraine's defensive posture handled briefly. Confidence level on the alignment thesis: moderate. Confidence level on the specific attribution of Russian failure to misalignment rather than other factors (sanctions, communications discipline, Ukrainian defensive partnerships, Hunt Forward operations): moderate at best, since several causal threads run together.

Styran: The Offense Death Cycle from a Ukrainian Perspective

The volume's most operationally grounded piece comes from the State Service of Special Communication and Information Protection in Kyiv. Styran offers what he calls the Offense Death Cycle (ODC) — a defensive operational concept built from CPT, Monte's *Network Attacks and Exploitation*, and Smeets's PETIO framework. The argument: defenders win by controlling the environment that attackers depend on, not by reacting to attacker techniques.

Three loops run inside the ODC: bridging strategic theory with operational defense; deliberately introducing friction as a defensive tactic; and integrating reactive incident handling with continuous initiative management. The piece reads as field-tested rather than theoretical — Styran cites recurring observations from Ukrainian network defense, where routine administrative changes unexpectedly disrupted advanced persistence.

The article fills a gap that English-language cyber strategy literature has left open. CPT lives mostly in policy circles; ODC is what the doctrine looks like at a security operations center keyboard. Confidence in the operational claims: moderate to high, though limited by the single national context.

Lentz: Allied Persistence at Uneven Speeds

Kevin Lentz applies the integrated persistence frame across the United States, Australia, and Japan. His finding: the three countries converge on similar policy direction at very different speeds. The United States articulated the doctrine first but lags in operationalization. Australia's REDSPICE blueprint commits 9.9 billion Australian dollars over a decade, with a focus on offensive capability and signals intelligence growth. Japan's 2025 active cyber defense law marks a structural shift after seven decades of constitutional self-restraint.

The piece is useful for what the analysis puts on the table — a comparative posture map that practitioners read against allied capability assumptions. The finding most relevant to intelligence work: the Federal Bureau of Investigation's August 2025 disclosure that Salt Typhoon hit more than 80 countries reframes the case for tighter allied integration. Confidence in the policy text analysis: moderate. The piece assumes published doctrine reflects actual capability — an assumption worth pressure-testing through HUMINT and SIGINT channels.

Influence Operations: Communication Hijacking in the Asia-Pacific

The most directly relevant piece for cognitive warfare and influence operations work comes from Santacaterina, Eerhart, Brown, Nelson, and Murphy. The team applies a seven-part typology — persona, hashtag, media, narrative, campaign, brand, and newsjacking hijacking — to PRC-linked influence operations between January 2021 and July 2024.

Table 2. Seven Levels of Communication Hijacking with Documented Asia-Pacific Cases

Level	Mechanism	Documented Asia-Pacific Case	DISARM Tactics
Persona	Impersonates real individuals through hijacked or fake accounts	Jiajun Qiu (邱家军), an overseas Chinese dissident - at least 12 impersonation accounts on X, peak Sept-Oct 2022	T0099, T0090, T0066, T0140.001
Hashtag	Floods existing hashtags with unrelated or disruptive content	Emerald Movement (#翡翠运动) anti-Xi protest tag flooded with gemstone imagery, June-July 2022	T0049.002, T0090, T0115.002
Media	Imitates legitimate news outlets to push pro-Beijing content	PAPERWALL network of Chinese websites posing as local news outlets (Citizen Lab, February 2024)	T0086, T0143.001
Narrative	Re-frames topics to delegitimize opponents	Fukushima wastewater release re-framed as 'nuclear-contaminated water' through coordinated state and CGTN messaging	T0055, T0066
Campaign	Sustained coordinated messaging over time	Spamouflage / Dragonbridge - over 50,000 instances disrupted by Google in 2022 alone	Multiple coordinated tactics
Brand	Misuses brand or institutional reputation	Xinjiang cotton boycott against H&M, Nike, others, March 2021 onward	T0099, T0066
Newsjacking	Injects oppositional content during high-visibility events	Taiwan 2024 election period - AI avatars, fake paternity test claims, fabricated documents	T0086, T0084.002

The methodology is rigorous for an open-source social media study. Bilingual analysts coded content in English and Mandarin Chinese, mapped behaviors against the DISARM "Red" framework, and reported inter-rater reliability above 90 percent. The dataset, code, and screenshots are open on GitHub — a transparency move that distinguishes the work from much commercial threat intelligence.

A finding worth pulling forward: PRC-linked persona hijacking targets diaspora critics rather than US public officials. Network overlap analysis identified at least one impersonation account that also participated in Spamouflage/Dragonbridge campaigns. The pattern suggests a shared operational infrastructure — broad narrative amplification and individualized suppression running through the same ecosystem. Confidence: moderate to high, with the appropriate caveat that attribution to state direction (rather than aligned proxy activity) rests on inference from coordination patterns, not on direct evidence of tasking.

For counter-influence work, the typology is operationally useful. The framework separates the "why" of an influence campaign from the "how," and gives analysts a vocabulary that travels across platforms.

Force Protection in an Era of Ubiquitous Technical Surveillance

Lt. Col. Jac Shipp's piece reframes cybersecurity as force protection. His starting point: adversaries no longer need to penetrate classified systems to generate operational effects. Commercial location data, device identifiers, metadata, traffic analysis, partner network seams, and routine web tracking — fused at scale — already expose units, commanders, and patterns of life.

The framework introduces Ubiquitous Technical Surveillance (UTS) as the operating concept. Mass observation alone is not the threat. The threat emerges when an adversary applies specialized analytics and AI to UTS data and converts raw observations into targeting intelligence. Government Accountability Office assessments and 2024 National Defense Authorization Act language back the construct as a real congressional concern.

Shipp proposes tiered posture packages — from Baseline through High Contestation — that translate geopolitical indicators into observable defensive actions. The goal, in his framing, is not to disappear from adversary collection but to become incoherent: data noisy enough that correlation breaks down, expensive enough that adversary analysis pipelines yield diminishing returns.

The framework fills a real practitioner gap. Two cautions, however. First, the indicator families are not yet back-tested against historical incident data. Shipp acknowledges the gap and points to EuRepoC and GDELT as future test sets. Second, the construct of "decision advantage" runs the risk of overpromise. Defenders make decisions with incomplete information; the question is whether the framework reduces surprise more than the framework adds noise.

For counterintelligence work, the piece is most useful in what the framework normalizes: open-source data fusion, commercial data brokers, and partner-network seams as primary attack surface. Verified — the Death by a Thousand Cuts technical report from the Army Cyber Institute documents the same phenomenon at the unit level.

AI in Cyber Early Warning: Findings from NATO SAS-183

Sarah Lohmann (University of Washington) and Col. (Ret.) Michael Davis (Naval Postgraduate School) report on a NATO Systems Analysis and Studies (SAS-183) experiment using large language models to detect anomalous behavior in renewable energy and microgrid logs.

Table 3. NATO SAS-183 LLM Performance on Cyber Early Warning Tasks

Model	Anomaly Detection	Threat Context	Inference Time	Composite Score
Llama 3.2 3B (fine-tuned)	4 / 5	3 / 5	3 / 5	30 / 40 (highest)
Llama 3.2 1B	3 / 5	4 / 5	4 / 5	29 / 40
Llama 3.2 8B	4 / 5	4 / 5	2 / 5	25 / 40
Phi-3 Mini Instruct	4 / 5	3 / 5	1 / 5	21 / 40
Mistral Instruct	2 / 5	3 / 5	3 / 5	23 / 40
Mistral DPO	3 / 5	3 / 5	4 / 5	24 / 40
Reasoner 1	4 / 5	1 / 5	3 / 5	21 / 40
Nous Hermes 2	3 / 5	4 / 5	3 / 5	25 / 40
DeepSeek-R1-Distill-Qwen-1.5B	3 / 5	3 / 5	3 / 5	23 / 40
DeepSeek-R1-Distill-Llama-8B	4 / 5	3 / 5	2 / 5	23 / 40

Source: Lohmann and Davis, CDR Vol. 11, No. 1, Table 2, p. 141

The fine-tuned Llama 3.2 3B model topped the list. Detection accuracy ran 75 to 85 percent across the LLM cohort, with inference times of 90 to 110 milliseconds — competitive with the classical CYMAROP prototype but with significantly stronger contextual reasoning.

The authors' caveats are sober. The tests did not simulate adversarial manipulation, model corruption, or operator over-trust. False positives and hallucinations remain high-consequence failure modes in operational technology environments. The recommendation: hybrid human-in-the-loop architectures, segmented from internet-linked update channels, with disciplined analyst review.

For intelligence purposes, the results signal a near-term operational shift. Smaller, fine-tuned, self-hosted models appear adequate for cyber early warning in constrained

environments — a finding that runs against the popular narrative of frontier-model dominance. Confidence in the empirical results: moderate, given the single experimental setting. Confidence in the broader methodological claim that semantic context matters in cyber early warning: high.

Long-Horizon Trust: Beyond the CIA Triad

Lt. Col. David Zgonc's piece reads at first like an outlier — a meditation on occupational and environmental health surveillance. Read carefully, the argument extends cyber risk thinking into a domain most defenders ignore.

His point: the CIA triad — confidentiality, integrity, availability — captures operational-timeframe failure modes. Long-horizon failures look different. Health surveillance data must remain interpretable for decades after collection, supporting veteran disability adjudication and institutional accountability for exposures that have not yet surfaced as illness, and will not for thirty years in some cases. As the Army shifts toward data-centric mesh architectures optimized for speed (Project Odin, NGC2), provenance fragments, contextual metadata gets stripped to conserve bandwidth, and analytic reasoning at the time of collection is not preserved.

The result, in Zgonc's framing, is an epistemic failure mode. Records remain technically intact yet impossible to defend as evidence. The piece introduces the concept of "defensible uncertainty" — documented and bounded acknowledgment of what is known and what cannot be resolved — as an obligation for cyber architects.

For broader analytic practice, the framework travels well. The same epistemic failure modes apply to intelligence reporting: streamlined dissemination collapses provenance, AI summarization strips context, and analytic uncertainty gets lost in the fluency of generated text. The piece is conceptual rather than empirical, but the warning is well-aimed.

Drone Defense Economics: Cost as Operational Variable

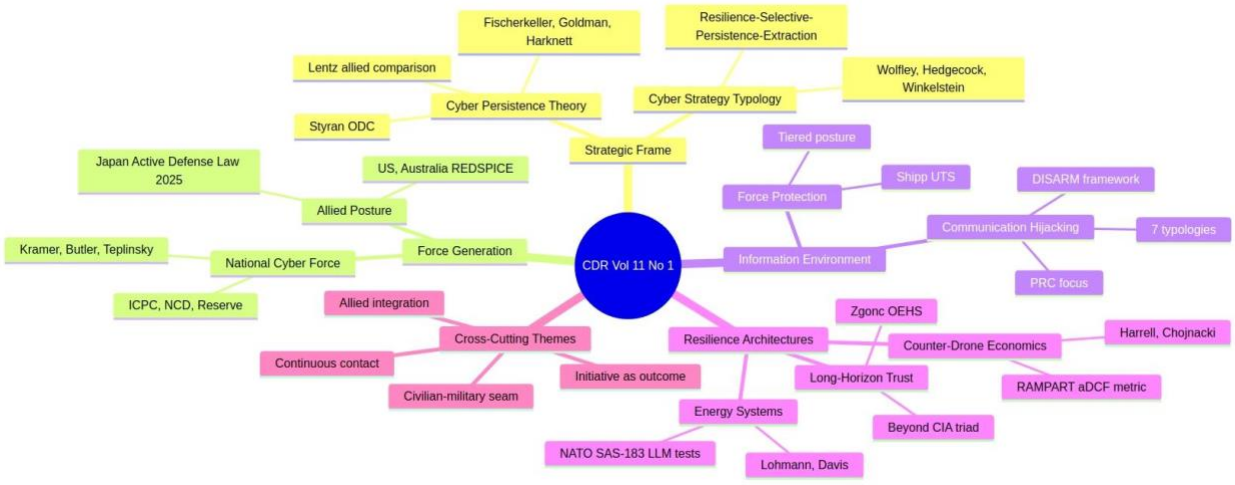
Maj. Nicholas Harrell and Lt. Col. Bruce Chojnacki close the volume with the most concretely quantitative piece. Their argument: cost asymmetry between low-cost drones and the kinetic munitions used to defeat them is now itself an operational vulnerability. The authors propose RAMPART (Resilient Adaptive Multi-layered Protective Air Response Technology) and a metric they call adjusted defense cost fraction (aDCF), which integrates defender costs, adversary costs, and the value of the protected asset.

The least-cost-first logic stacks engagement options dynamically — electronic warfare, directed energy, interceptor drones, then kinetic systems — based on operational conditions. The piece sits adjacent to cyber doctrine, but the underlying logic is shared: adversaries are scaling cheap mass against expensive precision, and defenders need analytic frameworks that price the asymmetry.

Confidence in the framework: moderate. The model is mathematically clean. Operational testing remains limited, and the cost data depends on assumptions about munition prices that are themselves moving fast.

Cross-Cutting Mindmap

The eleven pieces share more than the table of contents suggests. The mindmap below traces the analytical connective tissue.



Three lines of analytic tension run across the volume. The first: who commands. Authors disagree, often quietly, on whether the National Cyber Director, US Cyber Command, or distributed civilian-military seams should hold integration authority. The second: what works. Empirical evidence from Ukraine (Styran), the NATO experiment (Lohmann and Davis), and the Asia-Pacific influence operations corpus (Santacaterina et al.) carries the most weight. The third: what to measure. The volume is rich in proposed frameworks but

light on validated indicators — Shipp's framework, Harrell and Chojnacki's metric, and Wolfley's typology all need empirical pressure-testing.

Strategic Foresight Analysis

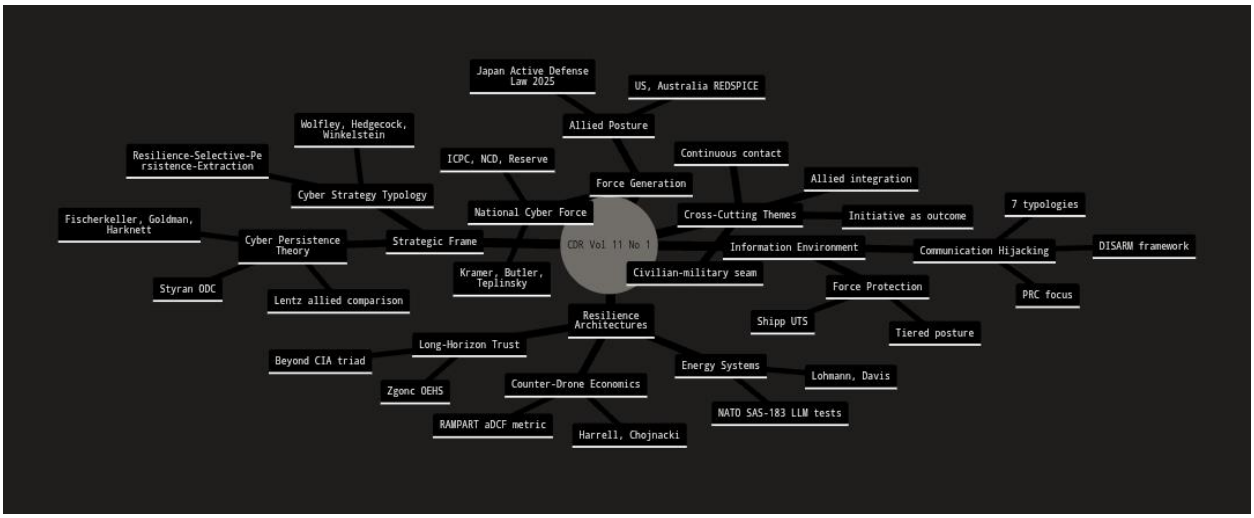
Three forecasts emerge from the volume, ranked by analytic confidence.

Forecast 1 (high confidence). Continuous-contact framing will displace deterrence as the dominant cyber strategy frame in US policy documents over the next 24 to 36 months. Cyber Persistence Theory has already entered allied policy in Australia and Japan. The 2026 White House cyber strategy referenced in the Wolfley piece reinforces the direction. Sherman Kent equivalent: very likely.

Forecast 2 (moderate confidence). Civilian cyber reserve structures will expand at the state level even if federal action stalls. Michigan, California, Maryland, Ohio, and Texas already run pilots. The 2024 National Defense Authorization Act authorized an Army pilot. State-level momentum runs ahead of federal action. Probability that at least three additional states stand up programs in the next 12 months: likely.

Forecast 3 (low-moderate confidence).** PRC-linked influence operations will increasingly target diaspora critics through persona hijacking while continuing broad narrative campaigns through Spamouflage/Dragonbridge. The Santacaterina team's data covers through July 2024. The Federal Bureau of Investigation's August 2025 Salt Typhoon disclosures and the New York Times reporting on harassment of critics' children in the United States (June 27, 2024) suggest the pattern is broadening rather than contracting. Probability the trend continues: likely. The harder question — whether US public officials become persona hijacking targets — remains roughly even chance.

Volume Mindmap



Conclusion

The volume's accumulated weight pushes one direction: the United States and its allies operate in cyberspace without quiet periods. Adversaries already sit on networks. Influence operations run continuously. Power systems carry pre-positioned implants. Health surveillance data degrades at the seams of new architectures. Drones defeat expensive defenses through cheap mass. The analytical task ahead is not to find better deterrents — the task is to build force structures, doctrines, and analytic methods that work under continuous contact.

What the volume does well: gathering operational evidence from Ukraine, NATO laboratories, Asia-Pacific influence operations, allied policy texts, and US infrastructure reporting in one place. The weakest seams sit where conceptual frameworks outrun their empirical validation. Practitioners reading the volume should pull forward the operational pieces — Styran's ODC, the Santacaterina team's typology, the Lohmann-Davis NATO results — and treat the conceptual frameworks as hypotheses to test rather than findings to apply.

For intelligence professionals working on strategic cyber, cognitive warfare, or counterintelligence portfolios, three takeaways stand out. First, the diaspora targeting pattern documented in the communication hijacking piece is operationally actionable for

liaison work and victim outreach. Second, the integrated persistence frame in Lentz's piece offers a comparative posture map worth pressure-testing through SIGINT and HUMINT channels. Third, the NATO SAS-183 results suggest fine-tuned small models are operationally adequate for cyber early warning — a procurement signal that runs against the frontier-model narrative.

One last observation. The volume's most operationally credible piece comes from a Ukrainian defender writing under live wartime conditions. That is not a coincidence. Doctrine that holds up against persistent state-grade attackers tends to come from people who have been on the receiving end. The lesson for US and allied cyber force generation is uncomfortable but clear: theory developed in peacetime keeps getting rewritten by people fighting in real time.

Citation Note

Article-level citations follow the format used in the original CDR Volume 11, Number 1, published April 2026 by West Point Press, ISSN 2474-2120. Direct article DOIs are listed in the journal at cyberdefensereview.army.mil. Verified attributions to Salt Typhoon and Volt Typhoon draw on Microsoft Threat Intelligence ([May 2023 advisory](https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/)), CISA's [Volt Typhoon advisory](https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a), and the [joint NSA/CISA/FBI advisory on Russian military cyber actors](https://media.defense.gov/2024/Sep/05/2003537870/-1/-1/0/CSA-Russian-Military-Cyber-Target-US-Global-CI.PDF) (September 2024). Federal Bureau of Investigation public statements on Salt Typhoon scope (August 27, 2025) [reported in the Wall Street Journal](https://www.wsj.com/politics/national-security/chinese-spies-hit-more-than-80-countries-in-salt-typhoon-breach-fbi-reveals-59b2108f).

Prepared as an analytical review of The Cyber Defense Review, Volume 11, Number 1 (2026). Word count approximately 2,950. Confidence levels follow Sherman Kent intelligence community standards.

Treadstone 71 WWW.TREADSTONE71.COM