VOLUME 10 ✧ NUMBER 2 2025

The Cyber Defense Review

Special Issue on Cyber Resilience and Power Projection

ARMY CYBER INSTITUTE ✧ WEST POINT PRESS

The Cyber Defense Review

✧ VOLUME 10, NUMBER 2 ✧

Aims and Scope

The Cyber Defense Review is an open-access, peer-reviewed, scholarly journal that serves as a forum for current and emerging research on cyber operations. Its focus is on strategy, operations, tactics, history, ethics, law, and policy in the cyber domain. The Cyber Defense Review positions itself as a leading venue for interdisciplinary work at the intersection of cyber and defense, welcoming contributions from the military, industry, professional, and academic communities.

The journal is committed to publishing original, previously unpublished, and intellectually rigorous research that advances the body of knowledge in this rapidly evolving field. We invite timely and relevant submissions that reflect both theoretical insight and practical application, with the goal of informing cyber-related decision-making, operations, and scholarship. As cyberspace is global, The Cyber Defense Review welcomes and encourages international participation. All submissions must contain unclassified material suitable for unrestricted distribution.

The Cyber Defense Review (ISSN 2474-2120) is published quarterly by West Point Press (westpointpress.com) and hosted by the Army Cyber Institute at West Point (cyber.army.mil).

Submitting to The Cyber Defense Review
For more information about the journal and guidance on how to submit, please see **cyberdefensereview.army.mil**

CONTACT
West Point Press
Taylor Hall, Building 600
West Point, NY 10996
TheCyberDefenseReview@westpoint.edu

This publication of The Cyber Defense Review was designed by Carine Lallemand and Joshua J. Dawson. The Cyber Defense Review is printed by McDonald & Eudy Printers, Inc. Printed on Acid Free paper.

INTRODUCTION

SENIOR LEADER PERSPECTIVES

SECTOR-SPECIFIC RESILIENCE

OPERATIONAL AND STRATEGIC FRAMING

EXERCISING RESILIENCE

EDUCATING AND EMPOWERING THE WORKFORCE

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 1-4
https://doi.org/10.55682/cdr/v76j-pd74

EDITORIAL

Widening the Aperture: A Global Perspective on Cyber Resilience of Critical Infrastructure

Patrick J. Davis*

Army Cyber Institute, West Point, NY, USA

The cyber defense of critical infrastructure is a national security imperative. The articles in this special issue of *The Cyber Defense Review* focus on cyber resilience and examine its role in enabling global power projection. Adversaries actively target, and have successfully infiltrated, the information technology (IT) and operational technology (OT) systems that underpin all sectors of critical infrastructure. In the United States, Presidential Policy Directive 21, issued in 2013, emphasized the importance of resilience—the ability of critical systems to recover quickly from threats ranging from cyberattacks to natural disasters. It identified sixteen sectors whose assets are considered so vital that their incapacitation would have "a debilitating effect on security, national economic security, national public health or safety." The directive's core tenets still underscore modern approaches to building resilience: unity of effort across levels of government and between sectors, risk-based management of vulnerabilities, and effective cross-border information sharing.

Critical infrastructure is a fundamental necessity for sustaining human health and safety; defending it against adversaries who play by different rules requires "whole of society" strategies and carefully engineered defenses that draw from multiple disciplines. Knowing that we heavily depend on the services provided by our complex, interconnected, and digitally vulnerable infrastructure, we must plan to fight through disruption when key systems are inevitably compromised or degraded. If necessary, we must also know how to operate and survive in analog mode. Additionally, due to the pervasive nature of the global threat and the spread of advanced technology, we must transition from a narrow focus on domestic

* Corresponding author: patrick.davis@westpoint.edu

coordination to one that embraces international collaboration. While the focus of this issue is rather U.S.-centric, we posit that the challenges and implications are applicable in global contexts. Major international alliances already acknowledge the defense of critical infrastructure as a technical imperative. The North Atlantic Treaty Organization (NATO), the European Union (EU), the Quad (India, Japan, Australia, and U.S.), and AUKUS (Australia, United Kingdom, and U.S.) are seeking to establish technical interoperability standards to protect the digital ecosystem underpinning energy grids, transport, and military logistics—a landscape characterized by the convergence of IT and OT, where defense is often hampered by incomplete visibility and authority gaps at jurisdictional boundaries and civil-military seams.

NATO has long recognized that cyberattacks on the critical infrastructure of a member nation could trigger Article 5. The alliance is operationalizing this concept by treating civilian energy and transport networks as dual-use military assets requiring active defense. They launched the NATO Integrated Cyber Defence Centre (NICC) and updated their Cyber Defence Pledge to focus on resilience by design. Rather than merely patching vulnerabilities, the alliance is driving member states to adopt federated data-sharing mechanisms that allow for the real-time exchange of threat intelligence without exposing the proprietary commercial data of private operators, who own the vast majority of this infrastructure. The *EU-NATO Task Force on Resilience of Critical Infrastructure* conducted technical assessments on the vulnerabilities of cross-border and cross-sector dependencies, acknowledging, for instance, that a cyberattack on a port management system in one country can create a logistical bottleneck that grounds NATO reinforcements in another. The Task Force also seeks to harmonize cyber resilience standards across the EU's NIS2 Directive and NATO's defense requirements to eliminate security gaps, such as those affecting transnational pipelines and undersea fiber optic cables. In the Indo-Pacific, the Quad is working on establishing common software security standards, improving threat information sharing, and addressing vulnerabilities in global supply chains for critical technologies like semiconductors. The Quad's Senior Cyber Group is focused on reducing reliance on high-risk suppliers for components like 5G hardware and Supervisory Control and Data Acquisition (SCADA) systems. Simultaneously, the AUKUS Pillar II initiative is developing and fielding advanced capabilities to protect critical communications networks and infrastructure.

Artificial intelligence (AI) can enhance the detection of dormant intrusions within OT networks, where pre-positioned adversaries live off of the land, sometimes for years, prepared to cause disruption when activated. Defending against this threat requires complete visibility of OT assets. In September 2025, the U.S. Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the UK's National Cyber Security Center (NCSC), alongside international partners, issued joint guidance prioritizing the creation of a "Definitive Record" for OT assets. It encourages operators to transition to dynamic automated

asset inventories, which enable full-scope environment monitoring for operational discrepancies, unauthorized changes, or insecure configurations. Crucially, this Definitive Record is also a prerequisite for enforcing technical standards and adapting Zero Trust principles to the OT environment. This is a complex undertaking; security solutions cannot add latency or overhead to sensitive cyber-physical processes and legacy industrial controllers cannot support computationally heavy authentication protocols or security enhancements. Instead, the focus must be on native device security, strict network micro-segmentation, and rigorous identity governance to contain lateral movement and prevent cascading failures.

As geopolitical tensions increase, cyber defenses are stress-tested daily in theaters like Ukraine, where kinetic warfare has converged with cyberattacks on civilian critical infrastructure. The current security environment is distinguished by the unprecedented pace at which emerging technologies are being weaponized. Autonomous systems, AI, quantum computing, and distributed ledger technologies are poised to change entire industries and are already altering the calculus of defense. Paradoxically, these technologies are force multipliers for both attacker and defender; threat actors can use AI to enhance and automatically execute phases of the cyber kill chain, while defenders can sift through large heterogeneous datasets in real-time and better detect and respond to anomalies. While the frontier of how these emerging technologies are used in civilian and military contexts is constantly expanding, the strategic importance of data is unchanged. Data serves as the foundational digital substrate upon which these systems operate and are secured. The integrity of AI training data, operational data, and the encryption standards that secure them are paramount. Here, there is work to do to protect against new attack vectors, and to prepare technology environments for a post-quantum future.

This special issue explores different techniques and practical applications of cyber resilience across high-stakes sectors. Our contributors examine vulnerabilities in healthcare, energy, water and wastewater, and transportation system sectors. While this issue does not include a deep-dive technical analysis into every sector—only addressing Energy in part and omitting especially critical sectors including Financial Services and Food & Agriculture—this does not diminish their importance. Indeed, sectors like Finance have long established mature resilience models through Information Sharing and Analysis Centers (ISACs) and public-private partnerships that other sectors would do well to emulate. The necessity of a systemic "whole of society" approach is central to the March 2023 recommendations from CISA's *Resilient Investment Planning and Development Working Group*. The report urges the government to take an integrated approach to federally-funded research, development, and innovation to move beyond siloed defenses to address the cascading dependencies of modern infrastructure. Today's threat landscape suggests that smart, coordinated investment in cyber defense research and development is now a shared global imperative.

Many of the insights presented in this issue are transferable across sectors and borders. Scholars and practitioners working in the cyber and critical infrastructure domains may find value in engaging with known gaps, assessing the efficacy of established operational frameworks and strategies, and considering how these might continue to evolve in theory and practice. The sophistication of our technical architectures cannot outpace the capability and capacity of the cyber workforce that is charged with defending them. Moreover, even the most advanced systems will fail without a foundation of trust—the essential cohesive that enables public-private partnerships and international alliances to function at speed. Consequently, the defense of critical infrastructure remains, at its core, a human endeavor. When AI agents can autonomously conduct cyberattacks and generate cascading effects, they easily exceed the protection afforded by traditional human-scale cyber defenses. We are now forced to grapple with an uncertain future caused by the proliferation of agentic AI, making it necessary to consider how the capabilities of human teams and global alliances can be enhanced by AI teammates. Securing this future requires a dual evolution: the rapid integration of innovative security technologies into our defensive architectures, and the deepening of the human trust that remains our most asymmetric advantage.

ABOUT THE EDITOR

Patrick J. Davis is the Editor-in-Chief of The Cyber Defense Review journal. He is also an Assistant Professor in the Department of Systems Engineering at the United States Military Academy (USMA). As an Army civilian data scientist and technologist, Patrick was previously a research scientist in the Data & Decision Sciences division at ACI and served as a data systems engineer in the USMA Office of Data & Analytics. His private sector experience includes management consulting, design, data science, and product leadership positions at PwC, AlixPartners, and EY, where he advised clients in the financial services industry on topics including data architecture, governance, advanced analytics, and digital strategy. Patrick served on active duty as an armor officer from 2004 until 2009, including two operational deployments to Iraq, for which he earned two Bronze Star Medals. His academic credentials include a BS in Electrical Engineering from USMA, a Master's in Civil Engineering from Norwich University, a Master's in Strategic Design from Parsons School of Design, and an MBA from The Wharton School.

ACKNOWLEDGMENTS

This special issue would not be possible without the dedicated efforts of our authors, the invaluable insights of our volunteer peer reviewers, and the support of our editorial board. We are also deeply grateful for the senior leader perspectives provided by Lt. Gen. Maria Barrett and Michaela Lee. Special thank you to the guest editor Dr. Karen Guttieri, Deborah Karagosian, and the Army Cyber Institute for hosting the workshop that brought this community together and sparked these critical conversations. Finally, a personal note of thanks to our Executive Editor, Dr. Carine Lallemand, for her expert orchestration of our internal editorial and publication processes.

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 5-13
https://doi.org/10.55682/cdr/eeng-3968

EDITORIAL

Cyber Resilience and Power Projection

Introduction to Volume 10 Issue 2

Karen Guttieri*

Janos LLC, Palo Alto, CA, USA

The assumption that the United States homeland is a sanctuary from attack no longer holds. Americans now depend so deeply on cyber-enabled IT and OT systems that rivals—whether strong or weak—can reach directly into the infrastructures that support U.S. military power and social stability. What once appeared to be distant "away-game" contests now routinely materialize at home: within the systems of military installations, logistics networks that sustain readiness, and civilian systems on which mobilization depends. These intrusions do not resemble declared hostilities. Instead, they unfold as hybrid campaigns marked by ambiguity: state-directed actors working through criminal proxies, covert exploitation disguised as routine network activity, and operations deliberately crafted to obscure attribution and intent.

The Jack Voltaic research program, launched by the Army Cyber Institute in 2016 (ACI, n.d.), anticipated these dangers by exposing civil–military interdependencies and highlighting how disruptions to local utilities, ports, and emergency services can cascade into operational effects. Jack Voltaic exercises demonstrated that resilience is a socio-technical practice: it must be rehearsed, shared, and built across critical infrastructure and government sectors. This special issue extends that lineage as interdependencies grow more consequential and adversaries exploit them with increasing sophistication.

* Corresponding author: kguttieri@icloud.com

WHY THIS SPECIAL ISSUE, WHY NOW?

Recent incidents show that competitors are already shaping the domestic battlespace by pre-positioning inside the critical infrastructure that supports force projection.

Chinese-sponsored Volt Typhoon access persisted for years inside networks around U.S. military installations (Lewis 2023). In August 2025, the FBI warned that Russia's Federal Security Service Center 16 had been detected collecting data from networking devices in multiple U.S. critical infrastructure sectors (FBI 2025). Such activities are troubling because the Army relies heavily on off-post utilities, logistics networks, and communications systems it does not control. As Lt. Gen. Maria Barrett observes in her Senior Leader contribution to this issue *"Resilient Dependencies: Preparing to Fight Through Cyber Disruption"*, Army resilience involves dependencies "in ways few understand well enough to sufficiently advise commanders on risk to mission."

From the state-level perspective, Michaela Lee shows that the civil domain is contested not only because adversaries pre-position there, but because the U.S. lacks any functioning coordination architecture to defend the civil–military seam. Installations depend on state-regulated utilities, locally managed water systems, and privately operated transportation networks, yet there is no mechanism to align authorities or information sharing across these boundaries. Adversaries target this civil-military seam not only for espionage or profit, but for strategic leverage—for latent power they can activate during crisis.

Together, these military and civilian perspectives capture a strategic inflection. The logic of nuclear deterrence encouraged great powers to avoid direct contact for fear of catastrophic escalation. Cyberspace, by contrast, creates incentives for continuous contact—probing, exploitation, and positional maneuver below the threshold of armed conflict (Fischerkeller, Goldman, and Harknett 2022). As a Russian diplomat observed in 2021: "The war [in cyberspace] is underway and unfolding very intensively" (Tass News Agency 2021). If this is true—and the evidence suggests it is—then deterrence in the traditional sense has already failed. The U.S. cannot rely on being untouchable; it must be prepared to operate in an environment where intrusion, not abstention, is the norm.

Much of the vulnerability stems from the same technological sophistication that has given the United States its military advantage. Today, the ability to project power is inseparable from cyber-reliant IT and OT systems. Mobility, logistics, command and control, energy distribution, transportation networks, telecommunications, and even municipal water depend on digital infrastructure that adversaries can—and demonstrably do—touch in peacetime. U.S. doctrine captures these interdependencies through Mission-Relevant Terrain in Cyberspace (MRT-C), which recognizes that systems essential to mission success often lie outside military control (Joint Chiefs of Staff 2018). Because the infrastructures that enable action are already contested, whole-of-nation resilience has become a decisive factor for credible power projection.

REFRAMING CYBER RESILIENCE

Cyber resilience is widely invoked but unevenly understood, in part because it fuses two concepts—cyber and resilience—that each carry different meanings across communities (Dupont et al. 2023). NIST's (2021) widely cited definition emphasizes preparation, absorption, recovery, and adaptation. This framework is influential, but in practice it is often interpreted through a static, technocentric enterprise-risk lens. By contrast, the UK Government (2022) Resilience Framework emphasizes anticipation, prevention, and whole-of-society responsibility. These different emphases reveal deeper cultural and strategic assumptions about what resilience is and how it should be practiced.

In my framing article for this project (Guttieri 2025), I argued for a dynamic conception of resilience as a practice—an operational logic rather than a steady state. Civilian and corporate actors typically understand resilience as maintaining operations or managing risk through measures such as shifting workflows, pausing services, or relying on backups. Military forces operate under different constraints: whether they can pause depends on the threat environment and mission requirements. In contested or degraded conditions, any pause risks losing tempo or initiative, so their resilience logic centers on sustaining action through disruption. This logic is already visible in routine practice. Units may shift logistics convoys to manual procedures when automated systems degrade or fail. Communications teams may improvise alternative pathways when automated routing collapses. Cyber defenders can exploit adversary errors, as occurred during the disruption of the TrickBot botnet in 2020. Together, such adaptations illustrate a military conception of resilience rooted in fighting through disruption, adapting in contact, and preserving initiative. The U.S. must signal to adversaries and allies alike that power projection remains credible even under sustained cyber pressure.

Reframing resilience for cyber competition requires moving beyond traditional notions of resilience as robustness (hardening) and rebound (restoring normal operations). Scholars such as David Woods and Chris Demchak illuminate why. Woods (2015) emphasizes *graceful extensibility*—the capacity to stretch performance at system boundaries—and *sustained adaptability*, the ability to reorganize across cycles of stress. When a cyberattack disrupts automated scheduling at a rail yard, the ability of logistics teams to shift rapidly to manual dispatch—improvised yet sufficient to preserve deployment tempo—is an example of graceful extensibility. When civil–military exercises such as Jack Voltaic or Cyber Yankee reveal weak points and prompt procedural changes in subsequent cycles, the organizations involved demonstrate sustained adaptability. Demchak (2021) complements this perspective by underscoring the importance of *slack in time*, collective proactive arrangements, and opportunities for action—the temporal and organizational maneuver space essential for preventing cascading failure. These insights resonate with the experience of Ukraine, which has had to mobilize and fight from an already degraded baseline (President's Council of Advisors on Science

and Technology 2024). Ukraine's distributed adaptation under relentless cyber, kinetic, and disinformation attacks demonstrates that resilience often emerges not as the preservation of normalcy but as the capacity to act, reorganize, and maintain initiative despite systemic disruption. As Gen. Barrett argues, "time is ammunition," and commanders must assume disruption as the baseline rather than a deviation.

CURATING A VIEW OF CYBER RESILIENCE AND POWER PROJECTION

The contributors to this special issue collectively push toward a more meaningful construct of cyber resilience while acknowledging the dilemmas that emerge in practice. This special issue begins with the domains where cyber defense is enacted—the sectors, technologies, and missions that must be protected—and gradually transitions toward the human and institutional systems that enable preparedness, coordination, and learning. By following this progression from practice to capacity, the issue traces a continuum of readiness, showing how the defense of critical infrastructures depends not only on technological innovation but also on education, governance, and collaboration across boundaries.

Sector-Specific Resilience

The opening section, *Sector-Specific Resilience*, grounds the reader in the operational realities of cyber defense. These contributions illuminate how vulnerabilities manifest in different infrastructures and how innovation can both strengthen and complicate resilience efforts. Pavlova and Albert's "*Defending Health Security: Securing Healthcare Infrastructure against Ransomware*" advances a novel "cyber health security" framework, positioning healthcare protection as an essential component of national defense and examining how ransomware attacks threaten both societal stability and public trust. Artusy's paper "*Autonomous Vehicles in Critical Infrastructure: Technologies, Vulnerabilities, and Implications*" explores how advances in artificial intelligence and sensor fusion transform transportation systems while introducing new ethical and cybersecurity dilemmas for both civilian and military applications.

Operational and Strategic Framing

The second section, *Operational and Strategic Framing*, zooms out from specific sectors to the systemic level of coordination, command, and policy. McNatt, Yoo, Welte and Sinclair's "*Pulling the Thread: A Campaign Approach to Mission Thread Defense of Force Projection*" examines how ARCYBER is redefining defensive cyberspace operations through a mission-driven campaign model, highlighting the interdependence between logistics, force mobility, and cyber readiness. Janosek's "*Toward a Global Framework for Cyber Threat Intelligence Sharing*" complements this view from a governance perspective, underscoring how international legal frameworks and data privacy regimes must evolve to support secure, ethical, and interoperable information sharing among allies and partners. Finally, Dempsey and Grotto's "*Ensuring*

the Cyber Resilience of Critical Infrastructure Serving Domestic Installations: Questions for Senior Leadership" examines the defense sector's dependencies on contractor-operated systems, calling for clearer standards and procurement clauses to secure operational technologies vital to Department of War installations. Together, these contributions articulate the strategic dimension of resilience—one grounded in trust, policy alignment, and mission continuity.

Exercising Resilience

Building on these operational insights, the third section, *Exercising Resilience*, turns to the rehearsal of preparedness—the practices through which defense capabilities are tested, learned, and strengthened before crises occur. Lohmann and Brown's "*Voices from Cyber Yankee: Lessons for Strengthening Critical Infrastructure Cyber Protection*" offers a practical reflection on interagency coordination during regional military–civilian exercises. Schwartz and colleagues' "*Access Denied and Sector Down: Introducing Resilience Games for Critical Infrastructure Preparedness*" introduces resilience games—serious games with wargaming elements—to explore systemic vulnerabilities through participatory simulation. Finally, "*Preparedness Wargaming for Critical Infrastructure Resilience: Taiwan Digital Blockade Wargame*" by Vogt, Kollars, and Poznansky extends the discussion to a geopolitical theater, illustrating how scenario-based exercises can inform national and allied resilience strategies in times of conflict. These contributions demonstrate that readiness is cultivated not only through technology, but through iterative learning, collective rehearsal, and trust-building across institutions.

Educating and Empowering the Workforce

Last but not least, *Educating and Empowering the Workforce* closes the issue with a forward-looking focus on human development—the continuous investment in skills, partnerships, and education that sustains national resilience. Chance, Franke, and Zwarg's "*Strengthening Cyber Resilience by Building Critical Infrastructure Communities: the C-CIC Pilot Study*" brings a sociotechnical perspective, exploring how intentional online networks can foster trust and mutual support among infrastructure operators. Hauptman's "*A Human-AI Teaming Approach to Closing the Talent Gap in Critical Infrastructure*" proposes practical questions to assess the viability of integrating AI teammates into infrastructure teams, offering a human-centered design perspective on automation and workforce augmentation. Nti Asare, Shackelford, Chun, and Powazek's "*Protecting Communities while Training Future Cybersecurity Professionals: Lessons from the Consortium of Cybersecurity Clinics*" examines how the rapid expansion of cybersecurity clinics is transforming education into a direct instrument of resilience, connecting students, professionals, and communities through hands-on engagement with real-world cyber challenges. These papers affirm that technological advancement must be matched by educational innovation and sustained human capacity-building.

RESILIENCE TRADEOFFS

Taken together, the contributions in this issue surface a pattern that may not be immediately apparent when reading each article in isolation: resilience practices carry costs and expose structural tensions. As systems become increasingly interconnected, automated, and civil–military in nature, strengthening resilience requires navigating cross-cutting pressures that recur across the special issue.

Efficiency vs. Slack

Optimization and automation improve steady-state performance but compress the temporal and organizational margin needed to maneuver through disruption. Artusy shows how AI-enabled transportation systems accelerate decision-making and tightly couple infrastructure, increasing brittleness when anomalies cascade. Schwartz and colleagues reveal through virtual exercise environments that rapid disruptions can quickly outpace organizational absorption capacity, while Lohmann's analysis of the Cyber Yankee exercise exposes how high-tempo conditions reveal coordination gaps across agencies. Optimized civilian lifelines—transport schedules, utilities, emergency-response processes—operate efficiently in steady state but often lack the buffer required for mobilization under cyber duress. These findings highlight that resilience requires restoring that maneuver space, whether through redundancy, practiced improvisation, or deliberate slack.

Interdependence vs. Exposure

Civil–military and cross-sector dependencies create operational leverage while simultaneously expanding the pathways adversaries can exploit. Resilience demands governance architectures capable of managing dependency risk across the civil–military ecosystem. McNatt and colleagues show how mission-thread analysis maps dependencies that create friction in mobilization and identifies where anticipatory slack is required. Dempsey and Grotto identify governance gaps in the OT systems that support domestic installations; because most MRT-C is civilian-owned, the Department of War (DoW) often lacks visibility into vendor practices or the authority to enforce resilience standards. Vogt's Taiwan blockade scenario highlights how partners differ in authorities, thresholds, and tempo, creating seams adversaries can exploit. Janosek demonstrates that cyber threat intelligence sharing creates structural interdependencies that are essential for early warning but widen organizational attack surfaces.

Our Senior Leader Perspectives echo these vulnerabilities: Gen. Barrett notes the Army's reliance on civilian utilities, logistics networks, and communications systems outside DoW control, while Lee highlights how fragmented authorities complicate coherent whole-of-government response.

Information Sharing vs. Sovereignty and Control

Timely information sharing enhances situational awareness but is constrained by legal authorities, jurisdictional boundaries, and sovereignty concerns. These constraints are not simply bureaucratic obstacles; they shape what organizations can see, share, and act upon during fast-moving crises. Janosek shows how cross-border CTI sharing faces privacy rules, liability concerns, and jurisdictional limits. The Taiwan Digital Blockade Wargame and the Cyber Yankee experience illustrate how classification regimes, authorities, and policy barriers can impede rapid sharing among agencies and partners. Domestic seams—municipal, state, federal, and DoW—create similar friction as organizations operate under different legal regimes. Jack Voltaic repeatedly revealed these challenges: agencies often held fragments of the operational picture but lacked mechanisms to exchange them quickly under stress. These patterns demonstrate that resilience requires controlled permeability across institutional boundaries—trust, authorities, and governance arrangements that enable lawful, rapid, interoperable flows of information.

Human Capability vs. Investment

Human judgment, trust, improvisation, and shared mental models provide the deepest reservoir of adaptive capacity, but developing and maintaining these qualities requires sustained institutional investment. Chance, Franke and Zwarg show how trust networks create "cognitive slack" that enables rapid coordination. Nti Asare and colleagues highlight cybersecurity clinics as a model for distributed human capacity, but these depend on sustained institutional support. Hauptman argues that the cyber talent gap has itself become a national-security risk and explores how human–AI teams may expand cognitive bandwidth while introducing new risks of bias, opacity, and reliance on proprietary systems. Schwartz and colleagues emphasize the importance of iterative rehearsal and safe-to-fail experimentation for sustained adaptability. The Jack Voltaic series reinforced that such capacities cannot be improvised during crisis and instead must be developed through sustained, repeated engagement. The planning of the exercise is as important as the exercise itself, yet many busy managers fear they cannot spare the time required for thorough preparation.

THE JACK VOLTAIC LINEAGE

As noted, the Army Cyber Institute's Jack Voltaic series[1] (ACI, n.d.) opened dialogue on civil–military interdependencies and how cyber disruption to local utilities, ports, and emergency services could cascade into national-level effects on mobilization.

This special issue extends the Jack Voltaic lineage in several key ways:

1. https://cyber.army.mil/Our-Work/Jack-Voltaic/

(1) **Operationalizing resilience**. Mission-thread analysis, MRT-C, and governance reform translate resilience into doctrine, authorities, and planning.
(2) **Socializing resilience**. Cyber clinics, communities of practice, and cross-sector exercises demonstrate how resilience must be cultivated, not presumed.
(3) **Expanding resilience**. Sector-specific analyses push beyond technical continuity toward societal stability, human security, and coalition cohesion.

Across these contributions, a model emerges: resilience for power projection requires extensibility, adaptability, and shared responsibility across military, civilian, and private partners. Authors emphasize practical mechanisms that build these capacities, including:

- Installations as regional resilience hubs
- Mission-thread analysis for anticipating friction before crisis
- Social capital as a resilience multiplier
- Exercises and clinics for generating learned adaptability
- Governance and contracting reforms for securing MRT-C
- Controlled permeability mechanisms for lawful, rapid information sharing across jurisdictions and sectors
- Human–AI teams for expanding cognitive and operational capacity
- Whole-of-society engagement for distributing resilience across communities

Together, these elements form a strategy for contested mobilization—preserving operational freedom of action in an environment where adversaries seek positional advantage long before a crisis materializes.

CONCLUSION: RESILIENCE AS AN OPERATIONAL IMPERATIVE

Across the contributions in this issue, resilience emerges not as a checklist or static attribute but as a practice shaped by structural tensions. Robustness and efficiency harden systems against expected conditions yet risk brittleness when disruptions exceed design assumptions. Extensibility and adaptability enable maneuver under stress but require slack, redundancy, and organizational diversity. These dilemmas are evident throughout this issue: automation compresses slack; interdependence widens exposure; information sharing is constrained by law; and human capability depends on long-term investment. No single organization—military, municipal, state, federal, or private—can defend critical infrastructure alone. Resilience requires joint rehearsal, shared situational awareness, and governance appropriate to our condition of interdependence. The contributors in this issue apply these insights to doctrine, policy, and practice, demonstrating that resilience has become the operational logic of credible power projection. Resilience in the cyber era is a continuous operational imperative—one that strengthens the technical, organizational, and social capacities required to fight through degradation and project power under sustained cyber pressure.

ABOUT THE GUEST EDITOR

Dr. Karen Guttieri is a cyber policy and strategy professional whose work spans technology, national security, and education. She previously served as a research analyst and associate professor at the U.S. Military Academy at West Point, affiliated with the Army Cyber Institute and the Department of Social Sciences. Her academic and leadership roles include serving as dean of the Air Force Cyber College and holding faculty positions at the Naval Postgraduate School. From 2022 to 2025, she led the Army Cyber Institute's Jack Voltaic initiative to advance national cyber resilience through collaborative civil–military and multi-sector engagement. She holds a Ph.D. in political science from the University of British Columbia and is affiliated with Stanford University's Center for International Security and Cooperation. She is also an honorary member of the U.S. Army Civil Affairs Regiment and was inducted into the Military Cyber Professionals Association's Order of Thor.

ACKNOWLEDGMENTS

The author thanks participants in the Jack Voltaic research program, from its inception through this current effort, for their contributions to cyber resilience and to the author's work. Thanks also go to colleagues at the Army Cyber Institute, with special appreciation to Paul Maxwell, for their insights and support. The author is grateful as well to David L. Alderson, Anne Marie Flores, and Herb Lin for discussions that informed and broadened the author's perspective.

REFERENCES

ACI (Army Cyber Institute). n.d. *Jack Voltaic Research Reports.* https://cyber.army.mil/Research/Jack-Voltaic/Research-Reports/.

Demchak, Chris. 2021. "Achieving Systemic Resilience in a Great Systems Conflict Era." *Cyber Defense Review* 6 (2): 51–70. https://www.jstor.org/stable/27021376.

Dupont, Benoıt, Clifford Shearing, Marilyne Bernier, and Rutger Leukfeldt. 2023. "The Tensions of Cyber-Resilience: From Sensemaking to Practice." *Computers & Security* 132:103372. https://doi.org/10.1016/j.cose.2023.103372.

FBI (Federal Bureau of Investigation). 2025. "Russian Government Cyber Actors Targeting Networking Devices, Critical Infrastructure," August 20, 2025. https://www.ic3.gov/PSA/2025/PSA250820.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford University Press.

Guttieri, Karen. 2025. "Fighting Through Disruption: Reframing Cyber Resilience for Power Projection and Strategic Credibility." *The Cyber Defense Review* 10 (1): 93–114. https://doi.org/10.55682/cdr/egvf-mkys.

Joint Chiefs of Staff. 2018. *Cyberspace Operations: JP 3-12.* U.S. Department of Defense, February 5, 2018. https://nsarchive.gwu.edu/document/16681-joint-chiefs-staff-joint-publication-3-12.

Lewis, James A. 2023. *Cyberattack on Civilian Critical Infrastructures in a Taiwan Scenario.* Center for Strategic and International Studies (CSIS), August 11, 2023. https://www.csis.org/analysis/cyberattack-civilian-critical-infrastructures-taiwan-scenario.

NIST (National Institute of Standards and Technology). 2021. *NIST SP 800-160 Volume 2: Developing Cyber Resilient Systems.* Technical report. December. https://doi.org/10.6028/NIST.SP.800-160v2r1.

President's Council of Advisors on Science and Technology. 2024. *Strategy for Cyber-Physical Resilience: Fortifying Our Critical Infrastructure for a Digital World.* Report to the President, February. https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf.

Tass News Agency. 2021. *Full-Blown Warfare in Cyberspace in Progress, Says Russian Diplomat,* December 16, 2021. https://tass.com/world/1376491.

UK Government. 2022. *UK Government Resilience Framework.* Cabinet Office, December. https://assets.publishing.service.gov.uk/media/63cff056e90e071ba7b41d54/UKG_Resilience_Framework_FINAL_v2.pdf.

Woods, David D. 2015. "Four Concepts for Resilience and the Implications for the Future of Resilience Engineering." *Reliability Engineering & System Safety* 141:5–9. https://doi.org/10.1016/j.ress.2015.03.018.

✧ Senior Leader Perspectives ✧

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 17-22
https://doi.org/10.55682/cdr/221s-3k44

SENIOR LEADER PERSPECTIVE

Resilient Dependencies: Preparing to Fight Through Cyber Disruption

Lt. Gen. Maria B. Barrett

U.S. Army Cyber Command, Fort Gordon, GA, USA

In a volatile threat environment, the Army's readiness and ability to execute missions at home and abroad increasingly hinge on digital dependencies spanning commercial software, IT/OT infrastructure, utilities, and the organic industrial base. This opener frames a cohesive approach to mission thread resilience across the Unified Network, emphasizing three imperatives: partner early and often with program managers, vendors, contractors, and local utilities to rehearse crisis response and establish shared understanding; procure secure by design capabilities with transparent vulnerability disclosure and rapid patching; and make data informed, commander owned risk decisions that enable formations to "fight through" disruption. Drawing lessons from the Army Cyber Institute's Jack Voltaic workshops and the inaugural Army Defensive Cyberspace Operations Optimization Conference, the article illustrates how civil military interdependencies can cascade and how rehearsals reveal hidden assumptions. A "fort to port" vignette, where a cyber compromise of national rail switching triggers operational delays, shows the value of synchronized public-private response, near real-time operational data, and flexible branches and sequels. The piece calls for acquisition leaders to weigh vendor track records on zero days and patch latency, signals the need to report and coordinate through ARCYBER's Information Warfare Operations Center and NETCOM's Global Cyber Center, and argues for a whole-of-nation model akin to the Civil Reserve Air Fleet to surge cyber resilience. Ultimately, it celebrates the tenacity of signal and cyber professionals and invites continued thought leadership that prevents strategic surprise in cyberspace while transforming how the Army teams, trains, and fights in and through a contested homeland.

Keywords: cyber resilience, DevSecOps, critical infrastructure, operational technology, mission risk

Lt. Gen. Maria B. Barrett assumed command of U.S. Army Cyber Command (ARCYBER) on May 3, 2022. A Massachusetts native, Barrett was commissioned as an Army second lieutenant via the Reserve Officers Training Corps program in 1988 after graduating from Tufts University with a B.A. in International Relations. Prior assignments include tours as Deputy Director of Current Operations, J-3, U.S. Cyber Command (USCYBERCOM); Deputy Commanding General, Joint Force Headquarters—Cyber, ARCYBER; and Deputy Commander (Operations), Cyber National Mission Force, USCYBERCOM. She has commanded units at the company, battalion, brigade, and command level, including service as Commander, 160th Signal Brigade, Third U.S. Army, and Commander, U.S. Army Network Enterprise Technology Command, her position prior to commanding ARCYBER. Barrett has also earned master's degrees in National Resource Strategy from the Industrial College of the Armed Forces (Eisenhower School) and in Telecommunications Management from Webster University.

OPENING

The volatility of today's world requires unceasing diligence in assessing risk to our Army organizations, units, and their missions. Threats in the cyber domain targeting our digital dependencies will always challenge the Army's combat readiness and ability to fulfill peace and wartime missions. Cyber events like the Colonial Pipeline disruption, and physical events like Hurricane Helene require shared trust and collaboration with commercial and municipal infrastructure partners that underpin the core functionality of our Army installations and nation. I strongly applaud the Army Cyber Institute at West Point (ACI) for its success in the Jack Voltaic® series of workshops, which have brought much-needed awareness and focus to the complexity of civil-military interdependencies. I also commend ACI's other invaluable contributions to the Army and operational force, as exhibited by products that make us think critically about how we team and train to tackle our Nation's cyber challenges. Continued thought leadership is a command imperative if we are to optimize support to the Army's operational force in areas like mission thread defense and national policy analysis. Here, ACI stands at the frontier, on mission to prevent strategic surprise in cyberspace.

OPERATIONALIZING SUPPORT FOR CAPABILITY DEPENDENCIES

This past January, the Army Cyber Command (ARCYBER) hosted the first Army Defensive Cyberspace Operations Optimization Conference (ADCyOC). The event spanned the gamut, leveraging robust academics to baseline Army command stakeholders' knowledge of mission thread analysis and information technology (IT) and operational technology (OT) dependencies on critical missions. Every intrusion the ARCYBER team analyzes, whether DoD or commercial domain, confirms a core tenet that the Army's cybersecurity and mission resilience is increasingly dependent on other entities and service providers in ways few understand well enough to sufficiently advise commanders on risk to mission. Our cyber

force must acknowledge this understanding gap and evaluate the risk of these dependencies in order to buttress Commanders' decision-making.

I offer three thoughts below on addressing our mission thread resiliency:

1) Partner for External IT/OT Dependency Support for Critical Operations

Program Managers, service providers, contractors, and infrastructure owners must understand the critical Army mission their technology (e.g., software) or infrastructure (e.g., municipal water, internet service circuit) is supporting. Start a healthy conversation between your Army organization and those organizations on which you depend. Ask how you can rehearse crisis response and continuously reinforce trust and shared understanding of impact "left of crisis". As ARCYBER operates and defends the Army's Unified Network, we engage with contractors and industry liaisons who provide network and data capabilities. Events like CrowdStrike in 2024 highlight that even advanced, well-resourced global conglomerates are susceptible to commercial software and IT infrastructure providers. That event did not disrupt Army networks, but it focused us on where a company's "first-call" should go in the future. Vendors often report to Army program or contracting offices costing valuable time for synchronizing an effective response. Time is ammunition in cyber operations. They should report critical cybersecurity information directly to ARCYBER's Information Warfare Operations Center (IWOC)—the command responsible for assessing risk and developing remediation plans, or to NETCOM's Global Cyber Center, the nexus of the Army's Unified Network. Bottom line: this issue is operational, not contractual.

Today, we constantly remind software and hardware vendors that their support, transparency, and leadership are vital to our Army missions; they are an extension of our network security. While imperfect, collaboratively thinking through 'likely' and 'most dangerous' cyber scenarios in advance has paid off with our commercial partners who value candor in their teaming with us.

IT and its dependencies are not the only concern for network owners and mission commanders. OT and the physical infrastructure it supports (for example, water and energy utilities) also impact Army missions. As with technology vendors, garrison leaders and senior mission commanders should continuously connect and collaborate with local agencies and utility providers to build relationships that optimize a shared understanding of capabilities, initial response actions, and most likely and/or threatening scenarios that could adversely impact services. ACI's Jack Voltaic workshops demonstrate the value in communities that openly discuss concerns, coordination points, and mutual support capabilities so that we avoid cascading failures caused by unvalidated assumptions.

The Army's on-premises OT within the organic industrial base (OIB) is a similar cause of concern. The Army manages critical missions that support global force projection and logistics

for the Joint Force. We should better understand our OIB dependencies on vendors, utility providers, and other critical infrastructure and key resources (CIKR) such as transportation and chemical ecosystems. Commanders overseeing these OIB missions should understand the dependencies fully within their control, and those that require special partnership, coordination and/or rehearsal to optimally mitigate service disruption.

2) Secure By Design | Expedient and Transparent Vulnerability Disclosure

We must start making purchasing and contracting decisions based on risk. A key first step is for our industry partners to better understand our risk profile and methodology. When deployed, I would never send a Soldier outside the berm with faulty body armor. Nor would I accept this risk on our network perimeter, within our mission command or business systems, or in other critical functions. We must stop acquiring technology and capabilities from vendors that are not developing products that are secure by design. Vendors' DevSecOps processes must include responsive and transparent vulnerability disclosure, matched by expedient patch delivery or effective risk mitigation. Software development in unsecured environments invites unseen long-term risk that is unacceptable in our critical warfighting systems. Accepting the risk of such software must be a decision of last resort.

While some acquisition programs are mandated to procure technology that meets high security standards, we are at an inflection point where everything we connect to the Unified Network is a potential avenue of approach for adversaries, exposing our critical missions and giving them the opportunity to hold our data at risk. Leaders with acquisition authority must be armed with the right questions, intelligence, and framework to analyze product risk. We should seldom, if ever, acquire a product from a vendor with a history of zero-day vulnerabilities that took months to patch. Our technology requirements will continuously grow as the Army increasingly employs artificial intelligence (AI) capabilities. Those advances must be informed by both our real-time understanding of the threat and the vendor's track record and reputation.

3) Data-Informed Decisions and Fighting Through Disruption

Army and Joint leaders understand that we likely will never have enough cyber defense capacity to fully defend all mission and terrain against a dedicated adversary. They also know we may need to "fight through" a disruption. Consider the following "fort to port" scenario:

> INDOPACOM tensions cause an Army division to mobilize to its Seaport of Debarkation (SPOD). Troops load their equipment onto trains at their installation railhead and depart on the several hundred-mile trip to the SPOD. Halfway to the SPOD, the Cybersecurity & Infrastructure Security Agency (CISA) alerts the Army that U.S. rail infrastructure has been compromised by a malicious cyber actor, and as a precautionary measure, rail operations have been halted nation-wide pending further assessment.

> What does the Division Commander do next?
>
> The Division Commander could request available cyber forces to expedite restoring rail operations. USCYBERCOM and DHS are likely already working to assess and resolve the situation. However, with elevated global tensions, Army cyber forces may already be committed against other existing cyber mission priorities.
>
> Assume the rail operators determine they must physically inspect the functionality of hundreds of automated switching devices along the track and projects requiring at least fourteen days to restore rail operations. The division G4 projects that a ground movement to the SPOD will take at least nine days.

There are several ways to tackle this hypothetical scenario. A cyber response team may either be unavailable or otherwise not aligned with the commander's optimal scheme of maneuver. However, our cyber forces in overwatch can be just as effective without 'boots on the ground.' Advances in technology now allow commanders and staffs to access more data in near real-time, with which to see options and make more timely decisions. Less complexity allows them to focus on the fight to their front. S6/G6 teams provide vital assessments to the commander on risks to data, platforms, and networks. This is key given our interdependence on commercial capabilities. Commanders still own the risk to their mission as well as the options they have to mitigate that risk. Fostering optimal operational transparency with commercial partners on which the commander's mission depends is crucial.

CYBER OPERATIONS MAY NOT BE SILVER-BULLET REMEDIES TO DISRUPTION

Having routinely participated in U.S. Forces Command's (FORSCOM) Rehearsal of Concept (ROC) Drill for a mass deployment and mobilization of U.S. Forces in support of a combatant command, "fight through" was the crux of my pitch describing to commanders the cyber realities of operating in, through, and from a contested homeland. Leaders who anticipate likely branches and sequels, triggered by technological disruption that are designed to disrupt movements and operations, are more likely to decide on successful alternative paths and are more resilient than those who don't.

A COHESIVE APPROACH TO CYBER DEFENSE

Every day, I'm encouraged by the tenacity of our Army signal and cyber professionals who operate and defend the Army's Unified Network. This is the backbone of Army data-centric operations. Still, I harbor a healthy respect for the malice and capabilities of our most formidable adversaries. Dominating cyberspace will require continuous investment and vigilance. While ARCYBER continues to adapt to meet the challenges of a domain evolving at warp-speed, we must align with national programs that partner industry and the DoD to confront them head on. I eagerly welcome collaboration among public and private sectors to establish trustworthy mechanisms that more effectively allow us to engage experts in troubleshooting

and responding to cyber emergencies. Programs like the Civil Reserve Air Fleet demonstrate the power and willingness of American industry to support national security endeavors and achieve a "whole-of-nation" approach to national defense.

This year marks the Army's 250th anniversary—our cyber forces continue to demonstrate the tenacity, innovation, and perseverance that have been our hallmarks since 1775. I'm honored and proud to be a part of our continued transformation. Please enjoy this volume of The Cyber Defense Review. I thank each of you for serving as a catalyst in making our cyber force the best it can be.

Respectfully,
mbb

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 23-37
https://doi.org/10.55682/cdr/s1yk-adc9

SENIOR LEADER PERSPECTIVE

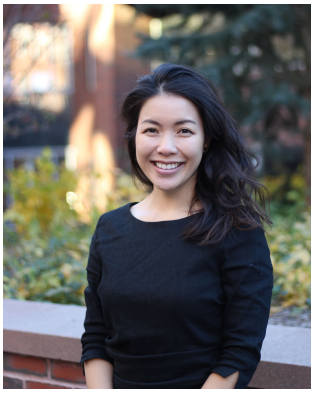
Beyond the Fence Line: Operationalizing Civil-Military Cyber Coordination at U.S. Military Installations

Michaela Lee

Deputy Chief Cyber Officer, State of New York, New York, NY, USA

U.S. military power projection increasingly depends on civilian critical infrastructure outside Department of War (DoW) control. Recent cyber campaigns—including China's Volt Typhoon pre-positioning in energy grids, water systems, and transportation networks—have systematically targeted the "civil-military seam" where DoW authority ends but operational dependencies continue. Federal-state-local coordination architecture is inadequate to defend this seam. Military installations often depend on state-regulated utilities, locally-managed water systems, and privately-operated transportation networks, yet lack formalized coordination mechanisms with these entities. Resource constraints at state and local levels, jurisdictional fragmentation, and classification barriers preventing information sharing leave installations vulnerable to disruption of surrounding civilian infrastructure. DoW's December 2024 directive requiring installations to coordinate "beyond the fence line" with state and local governments acknowledges this challenge but lacks an implementation framework. This article proposes operationalizing military installations as regional cyber resilience coordination nodes, or "seeds," from which federal-state-local partnerships develop.

Keywords: cyber resilience, critical infrastructure, power projection, military readiness, civil-military seam



Michaela Lee serves as the Deputy Chief Cyber Officer for Operations for New York State. In this role, she oversees cybersecurity operations across New York and works closely with other members of the Governor's Office, state agencies, local governments, and federal partners to ensure the security and resilience of the state's critical infrastructure. Before joining New York, Michaela was the Director for Strategy and Research at the White House Office of the National Cyber Director, helping develop and implement the National Cybersecurity Strategy and leading special projects on technology and democracy. Previously, she served as a Tech and Human Rights Manager at BSR, where she covered responsible AI, privacy, and end-to-end encryption. Michaela is a Non-Resident Fellow with the Carnegie Mellon Institute for Strategy & Technology and a term member at the Council on Foreign Relations. She received a bachelor's degree from UC Davis and a Master of Public Policy from the Harvard Kennedy School.

INTRODUCTION

In September 2024, reports emerged that U.S. telecommunications firms had been compromised by Chinese hackers (Krouse, McMillan, and Volz 2024). Subsequent reports revealed that Salt Typhoon, a Chinese state-sponsored cyber espionage group, had compromised at least 600 companies across more than 80 countries (Viswanatha and Krouse 2025). The campaign was primarily an intelligence operation, but it also demonstrated persistent access to networks critical to civilian and military everyday communications. When combined with Volt Typhoon pre-positioning in energy grids, transportation networks, and water and wastewater systems, a clear strategic picture emerges: adversaries are systematically mapping and infiltrating civilian critical infrastructure. Protecting critical infrastructure from sophisticated cyber threats is not merely a homeland security task; it is a fundamental prerequisite for maintaining military readiness, ensuring the lethality of the force, and projecting power in a contested world.

Cyber threat actors often disregard jurisdictional boundaries and distinctions between federal, state, and local authorities. They exploit the very interdependencies that make our society efficient and connected: information and communications technology, cloud-native services, shared utilities, and global supply chains. Karen Guttieri (2025) persuasively argues that these threats are most critical at the "civil-military seam," where there are gaps between military systems and assets controlled by the Department of War (DoW) and civilian-owned and -operated installation support infrastructure essential to military operations.

This article proposes operationalizing military installations as coordination nodes, or "seeds," for regional cyber resilience, providing the federal-state-local coordination framework required by DoW's December 2024 policy directive to establish resilience "beyond the fence line."

The stakes are clear. As a recent Cyberspace Solarium 2.0 report documents, U.S. military power projection depends on 18 commercial seaports, 69 civilian airports, 40,000 miles of commercial rail, and countless municipal utilities—all outside DoW direct control (Fixler, Montgomery, and Lane 2025). The 2025 *Annual Threat Assessment of the U.S. Intelligence Community* identified the threat even more clearly:

> If Beijing believed that a major conflict with Washington was imminent, it could consider aggressive cyber operations against U.S. critical infrastructure and military assets. Such strikes would be designed to deter U.S. military action by impeding U.S. decision-making, inducing societal panic, and interfering with the deployment of U.S. forces (ODNI 2025).

By identifying China's cyber campaigns against defense critical infrastructure as a top-tier threat, the Office of the Director of National Intelligence (ODNI) openly flags this challenge; the current federal-state-local coordination architecture is insufficient to defend the civil-military seam. What does operational cyber resilience look like from the perspective of a county office responsible for managing municipal water systems that serve nearby military installations? Do federal strategies adequately translate into actionable guidance for local utilities, transportation authorities, and emergency managers? And most critically: how can the U.S. bridge the persistent gap between federal recognition of cyber threats and the state/local capacity necessary to address them?

THE THREAT LANDSCAPE: CIVILIAN INFRASTRUCTURE AS CONTESTED TERRAIN

For many adversaries of the U.S., civilian infrastructure is an attractive target in geopolitical cyber conflict. Electrical grids, telecommunications, transportation networks, and health systems increasingly have become fair game, marking a stark evolution from past decades, when military operations largely avoided civilian targets under international norms.

The inconsistent application of deterrence strategy by the U.S. and others has helped adversaries undermine such norms. Today, adversaries see civilian infrastructure not just as collateral, but as a pressure point. It can be exploited for strategic leverage, political disruption, financial gain, and psychological effect, often as part of hybrid or pre-kinetic strategies.

Russia's cyber operations against Ukraine since 2022 are real-world demonstrations of adversary strategies targeting civilian infrastructure to degrade military response. Russia systematically attacked Ukrainian power grids, water systems, and telecommunications in an attempt to disrupt military logistics and undermine civilian morale simultaneously. Blackouts, disrupted logistics, and widespread distributed denial-of-service (DDoS) attacks caused societal and military disruption in tandem. Ukraine's resilience offers instructive lessons. Through rapid repair capabilities, distributed generation, international partnerships (including Starlink satellite communications and the Cyber Defense Assistance Collaborative),

and prior experience with Russian cyber tactics, Ukraine maintained critical capabilities despite sustained attacks (Smith 2022; Simonite 2022).

In 2020, Iranian actors attempted to manipulate Israeli water treatment systems to increase chemical dosing levels—potentially endangering the health of civilians (Jeffries et al. 2022). In 2023, Iranian actors compromised programmable logic controllers used by water and wastewater organizations. Such examples show how civilian infrastructure is no longer collateral; it is strategic.

The People's Republic of China's campaigns further illustrate the trend toward pre-positioning, that is, infiltrating critical infrastructure well before any overt conflict. Unlike traditional espionage operations, Volt Typhoon demonstrated deliberate pre-positioning in operational technology (OT) systems controlling physical infrastructure. The campaign targeted telecommunications networks, energy grids, water systems, and transportation infrastructure, which are precisely the sectors essential to military power projection. Technical analysis revealed sophisticated tradecraft, where adversaries utilized living off the land (LOTL) techniques that leverage native system utilities to avoid detection while maintaining persistent access for years (CISA 2024).

These tactics indicate a fundamental shift in how adversaries approach conflict, blending traditional military strategies with asymmetric cyber operations that target civilian infrastructure. This shift demands that the security of critical infrastructure is elevated to the same level of care and political importance as is the case for traditional national security assets.

The Dissolution of the Perimeter

For years, cybersecurity doctrine was anchored in the notion of the perimeter—a virtual boundary defending internal systems from external threats. However, the emergence of cloud-native architectures, remote workforces, Internet of Things ecosystems, and software supply chains has dissolved this boundary. Today, organizations rely on software-as-a-service (SaaS) providers for key business processes and depend on code libraries developed by unknown third parties. Meanwhile, many critical infrastructure providers still rely on legacy systems that were never designed to withstand cyberattacks. Attack surfaces have expanded exponentially, as has the number and sophistication of adversaries.

While DoW has adapted to this evolving challenge through Zero Trust principles, the civilian critical infrastructure upon which installations depend operates under different constraints. Implementing Zero Trust architectures is challenging in environments with legacy OT that don't easily integrate with modern authentication mechanisms. Resource constraints further complicate critical infrastructure entities' ability to adopt Zero Trust security architectures or maintain continuous monitoring capabilities.

In the new threat landscape, cyber resilience cannot be confined to firewalls or access control lists. A vulnerability in a widely used open-source component can place everything from hospital record systems to water utilities at risk. Resilience, therefore, must be systemic: it must anticipate unknown risks, account for interdependencies, and incorporate recovery into its very design.

The Convergence of Threat Actors and Insignificance of Attribution

The line between nation-state and criminal cyber actors is increasingly blurred, and this poses challenges for how the United States responds to cyberattacks. Sophisticated criminal groups now possess capabilities once reserved for intelligence agencies, and they frequently operate under tacit approval, or even direct guidance, of adversary governments. The Conti ransomware group, for example, operated with impunity out of Russia and, in some cases, appears to have shared resources and targets with state-sponsored actors. North Korea's Lazarus Group has conducted both state espionage and high-profile cryptocurrency theft to fund the regime.

For the U.S. federal government, the distinction between state and non-state actors matters significantly. Intelligence agencies have different authorities and restrictions based on the nature of the adversary, and any diplomatic or military responses hinge on clear attribution to a foreign government. However, for state and local governments or operators of critical infrastructure who are often on the front lines of these intrusions, the identity of the attacker is much less relevant. Whether a hospital system is taken down by a ransomware gang or a nation-state adversary, the operational consequences are the same: catastrophic.

This convergence benefits adversaries by creating plausible deniability and complicating coordinated response strategies. Intelligence agencies have limited authority to act domestically, while civilian critical infrastructure providers often lack insight into the sophistication or intent of attackers. The result is paralysis in moments of crisis and fragmentation in long-term strategy. The challenge is paradoxical; the United States must simultaneously prepare for strategic cyber conflict (such as one involving China and Taiwan) while also attempting to counter highly distributed, persistent ransomware attacks across sectors. Although counter-strategies, operational considerations, and effects of these threats are unique, both can cause comparable damage and disruption, particularly at the civil-military seam.

The Information Domain as Target and Enabler

Cyber-capable adversaries do not need to physically destroy infrastructure because non-kinetic cyber disruption can achieve similar effects without triggering escalatory action. In the information domain, data flows between military and civilian systems are targets for exploitation. Consider mobilization as an information-intensive process. When personnel receive deployment orders, they access information through commercial internet connections.

Logistics systems track equipment movement through civilian transportation networks, generating data about timing, routes, and cargo. Each of these information flows potentially reveals operational patterns, timing, and intentions to adversaries with access to civilian infrastructure.

Russia has used these tactics to great effect in its war with Ukraine. In addition to disruptive attacks, Russia has targeted Western logistics entities and technology companies involved in the coordination, transport, and delivery of foreign assistance to Ukraine (CISA 2025). Adversaries targeting civilian infrastructure can exfiltrate data revealing military dependencies and timing, manipulate data to cause operational confusion (e.g., incorrect fuel delivery schedules, altered cargo manifests), or deny access to data systems, forcing manual operations that slow mobilization.

The Civil-Military Seam as Battlespace

The "civil-military seam" describes where DoW authority ends but operational dependencies continue. This boundary manifests across four dimensions. Physically, it is the installation fence line separating military-controlled assets from civilian-owned infrastructure. Jurisdictionally, it divides federal military authority from state and local regulatory control over, for example, utilities, transportation, and telecommunications. Operationally, it separates DoW's cybersecurity standards and resources from civilian operators' often-limited capabilities. Informationally, it creates barriers between classified threat intelligence held by military and federal agencies and uncleared civilian infrastructure operators who need that intelligence to defend critical systems.

Adversaries exploit these seams through several mechanisms. They target civilian infrastructure knowing that DoW cannot unilaterally defend it. They leverage jurisdictional complexity, understanding that unclear roles and responsibilities create gaps in coverage. They exploit resource disparities, recognizing that small municipal utilities lack sophistication to detect nation-state intrusions.

The strategic implication is that resilience cannot be achieved through military hardening alone. If surrounding infrastructure degrades, military installations degrade with it. Conversely, securing civilian infrastructure serves both civilian essential services and military readiness, making resilience a shared civil-military imperative.

THE INTERDEPENDENCY FRAMEWORK: IDENTIFYING MILITARY DEPENDENCIES ON CIVILIAN INFRASTRUCTURE

Consider Joint Base Lewis-McChord (JBLM) in Washington State, home to I Corps and the only Army power projection platform west of the Rocky Mountains. The base depends entirely on Tacoma Power for electrical service to operate climate control systems that protect sensitive

equipment, power logistics systems that coordinate deployment and sustainment, maintain communications networks, and sustain force health protection for personnel and families. In the case of an extended outage, the base is required to be able to independently sustain operation of mission-critical facilities for at least fourteen days (Secretary of the Army 2020).

To address risks to military energy resilience, the Department of War has focused extensively on "inside the fence" backup power systems and microgrids. JBLM recently put forward plans to construct a microgrid to sustain critical facilities, noting that only 35% of their airfield's critical facilities have backup generators in place, and none have alternative sources capable of providing continuous long-term power (Under Secretary of War Comptroller 2024).

On-site resilience strategies such as microgrids are necessary but insufficient, given the heavy reliance of bases on civilian infrastructure. For example, JBLM supports approximately 30,000 active duty service members, as well as nearly 295,000 civilians, family members, and local retirees who are also connected to the base. Many of them live in the surrounding region and are also dependent on civilian critical infrastructure for basic services (Military OneSource 2025).

In recognition of this challenge, DoW issued a new policy in December 2024 that requires components to include considerations "beyond the fence line" in their infrastructure resilience strategies. This policy includes a requirement to:

> Undertake planning and assistance with State and local governments to ensure efficient preparedness and resilience of essential transportation, logistical, or other necessary resources *outside of a military installation* that are necessary in order to maintain, improve, or rapidly reestablish military installation mission assurance and mission-essential functions (Under Secretary of Defense for Acquisition and Sustainment 2024).

This new policy reflects a growing recognition that defense communities are crucial for delivering mission capabilities and projecting power. However, the policy intention currently lacks the enforcement mechanism necessary to ensure resilience against a Volt Typhoon-level threat. A notable challenge is that dependencies between installations and civilian networks are inherently multi-dimensional:

- Physical – electricity, water, fuel, and transportation.
- Digital – telecommunications, industrial-control systems, and logistics data.
- Human – workforce, contractors, and emergency-response capacity.

Because these dependencies span multiple jurisdictions, accountability is fragmented, and it is challenging to identify and map all potential vulnerabilities and their cascading effects. While the following survey is not exhaustive, it aims to provide an overview and examples of sector-specific implications that impact resilience at the civil-military seam for U.S. military installations.

Sectoral Implications

Energy. Grids and fuel logistics are primary operational enablers. OT vulnerabilities in electrical grids and pipelines, combined with distributed ownership and regulatory fragmentation, make the energy sector a high-leverage target for adversaries seeking to delay or complicate force projection. The May 2021 Colonial Pipeline ransomware attack exposed vulnerabilities in the U.S. fuel logistics system; although non-OT billing systems were compromised, uncertainty about system integrity led Colonial to preemptively shut down 5,500 miles of pipeline delivering 45% of the total fuel supply for the East Coast, which is home to multiple military installations (Mittal 2024).

Transportation and Ports. Strategic sealift and heavy equipment movement depend on commercial ports, railways, and intermodal connectors. Recent analysis by the Foundation for Defense of Democracies states that 90% of military equipment deploys through commercial seaports, such as the Port of Jacksonville, which handles military cargo for U.S. Central Command and U.S. Southern Command operations (Fixler, Montgomery, and Lane 2025). Rail infrastructure moves heavy equipment that cannot be transported by road or air. Strategic rail corridors from Fort Riley, Kansas to ports on both coasts carry tanks, artillery, and armored vehicles for overseas deployment. These rail networks are owned and operated by private companies—BNSF Railway, Union Pacific, and CSX Transportation—whose dispatch systems, signaling networks, and logistics software are potential cyber targets. Because many of these strategic assets are privately operated under federal safety regulation, a cohesive nation-level response depends on extensive public-private coordination.

Water and Wastewater. Military installations require water for human consumption, equipment cooling systems, firefighting, medical facilities, and food service operations. Most installations receive water from municipal systems managed by local governments or regional authorities. While some systems have mature cybersecurity programs, many small and mid-sized municipal systems operate with minimal cyber staff and outdated OT. The Oldsmar incident and other intrusions highlight the potential for public health consequences and operational degradation if water treatment or distribution systems are manipulated (Jeffries et al. 2022). The risk is particularly acute for hospitals. The CDC notes that emergency water storage capacity at hospitals typically lasts under two hours, whereas backup power may last for multiple days (Centers for Disease Control and Prevention and American Water Works Association 2019). This asymmetry makes water infrastructure disruption potentially more operationally significant than power outages.

Telecommunications and Data Networks. Military installations rely on commercial internet service providers for daily administrative functions, coordinating unclassified logistics, communicating with personnel, and storing non-classified data on cloud-based platforms. Persistent

adversarial access to carrier networks enables them to analyze traffic, conduct man-in-the-middle operations, and establish routes for denying or manipulating connectivity. The Salt Typhoon incident highlights the strategic value of pre-positioning within telecommunications infrastructure. The broader ecosystem's components— including Domain Name System (DNS), routing, backbone fiber, and mobile networks— are vulnerable to both observation and disruption.

JBLM alone depends on at least 15 distinct civilian critical infrastructure entities. Other military installations have similar profiles and must also navigate numerous operational relationships with municipal entities, critical infrastructure operators, and state and local officials. The remaining sections of this article will lay out the challenges and opportunities for stronger coordination and resilience across the civil-military seam.

STATE AND LOCAL PERSPECTIVES: BRIDGING FEDERAL STRATEGY AND OPERATIONAL REALITY

Federal cyber strategies often assume state and local entities will implement federal guidance and priorities. The reality is much more complex. States face competing demands for limited resources: education funding, healthcare costs, infrastructure repair, and numerous other priorities. Cybersecurity competes with these pressing needs, often without dedicated funding.

Resource Constraints and Competing Priorities

Federal strategies and guidance establish national priorities but often have limited funding or operational support for state and local implementation. This creates a strategic disconnect: federal plans assume state capacity that doesn't exist, while states may struggle to operationalize federal guidance without corresponding funding or technical assistance.

This resource disparity manifests in several ways. State budgets often operate under balanced budget requirements and tax revenue constraints that limit discretionary spending, leaving little fiscal flexibility for cybersecurity investments that lack dedicated funding streams. States also struggle with significant personnel constraints, often unable to compete with the federal government and the private sector for cyber talent. Technology gaps exacerbate this issue, as many state and local systems operate on outdated legacy technology with deferred upgrades and a history of poor vulnerability management. Furthermore, training deficiencies mean cybersecurity awareness remains inconsistent, and the issue as a whole struggles to compete for executive attention against more immediate, visible challenges.

Jurisdictional Complexity and Authority Gaps

Critical infrastructure protection involves overlapping federal, state, local, and private sector authorities. Utilities are regulated at the state level, but interstate transmission is regulated at the federal level. Water systems are locally managed but federally regulated for quality without federal cybersecurity standards. Telecommunications are federally regulated, but state commissions maintain some limited oversight over them. This fragmentation means no single entity has comprehensive authority or visibility.

Private sector complications add complexity. Most critical infrastructure is privately owned. States can regulate entities within their jurisdiction, but enforcement mechanisms are limited. The Colonial Pipeline decision to shut down, for instance, while rational from a corporate risk perspective, created cascading effects that state and federal authorities had limited ability to prevent or mitigate.

Information Sharing: The Persistent Barrier

Many of the most frustrating gaps in federal-state coordination involve information sharing. Classification systems designed for the federal government create barriers preventing effective cooperation with state and local partners. Federal threat intelligence is often classified, which prevents it from being shared with state officials who lack clearances. While some state officials maintain clearances, most stakeholders at the operational level—including utility operators, emergency managers, and local officials—typically do not. This means actionable threat intelligence never reaches the people who must respond to it.

Even when state officials hold clearances, "need to know" determinations may prevent sharing. Amid uncertainty, private sector infrastructure operators may fear that reporting cyber incidents will trigger regulatory consequences, lawsuits, or public disclosure that can damage their reputation. Years of inconsistent federal engagement with states on these matters have created trust deficits. These structural barriers impede information sharing even when it is in the best interest of all parties to cooperate.

Coordination Gaps at the Civil-Military Interface

Given the gaps stated above, it is no surprise that military installations and surrounding civilian infrastructure often operate as separate worlds, despite deep operational interdependencies. Many installations lack regular engagement with local utility operators, emergency managers, or municipal officials. Communication occurs only during crises, which can result in mistrust and unfamiliarity with each others' procedures. Military installations may not understand civilian infrastructure vulnerabilities or operational constraints, while civilian operators may not understand military mobilization requirements, critical timing windows, or priority needs during crises.

A realistic scenario illustrates these gaps: A cyberattack disrupts a power grid during hurricane response. The military installation must mobilize for disaster relief while continuing to support its own mission. The civilian population needs power for life safety. State-level emergency management coordinates response but lacks visibility into military requirements. The military installation operates backup generators but needs fuel resupply through civilian logistics networks that were disrupted by hurricane damage and cyberattack. Who makes prioritization decisions? Through what mechanism? Based on what pre-established framework? Currently, such scenarios are often resolved through ad hoc coordination and improvisation—approaches that usually fail under stress.

Recent incidents demonstrate that these gaps are not theoretical. Winter Storm Uri caused cascading failures across Texas's electrical grid in February 2021, affecting multiple military installations including Fort Hood, Fort Sill, Fort Polk, and Fort Riley (Gabram 2021). While these installations maintained backup generation capacity consistent with DoW requirements, the broader grid collapse created secondary effects the military could not address unilaterally.

The Electric Reliability Council of Texas (ERCOT), which operates the state's independent grid, had no formal coordination mechanism with military installations. As the crisis unfolded, installations were treated as large commercial customers rather than entities with national security missions. No pre-established protocol existed for installations to communicate operational criticality to ERCOT operators, who needed to make load-shedding decisions. Consequently, some installation facilities experienced rolling blackouts alongside civilian neighborhoods, despite housing mission-critical operations.

Fuel resupply for backup generators became critical as the storm persisted beyond the typical 72-96 hour backup durations assumed by DoW planning. However, civilian fuel distribution networks were themselves compromised by power outages at pumping stations, refineries, and other pipeline infrastructure. Natural gas production facilities also lost power and were unable to pump gas to power plants, creating a cascading feedback loop that extended the crisis. The incident revealed fundamental coordination gaps. While installations understood their dependency on civilian infrastructure, no mechanism existed for real-time coordination with ERCOT, the Texas Division of Emergency Management, state energy offices, or fuel distributors. Information sharing was informal and episodic (Busby et al. 2021). The Texas winter storm illustrated what the DoW's December 2024 directive seeks to address: installations cannot achieve resilience inside the fence line when surrounding civilian infrastructure fails.

Having identified the gaps in the current structures, the following section proposes an operational framework for addressing them.

REGIONAL RESILIENCE AS STRATEGIC READINESS: MOVING FROM AWARENESS TO INTEGRATION

Military bases are among the most resource-intensive and infrastructure-dependent institutions in the nation. Their operational readiness depends on local utilities that are often managed by civilian and private sector entities with limited cybersecurity capabilities and resources. Because of this, resilience must be reciprocal. It is not enough for bases to harden their own networks and build internal redundancies. They must also actively assist their host communities in building resilience and institutionalizing coordination across federal, state, and local domains. The central requirement is not new technology or statutory authority, but an operational framework that aligns defense readiness with civilian continuity.

The "Seeds" Concept: Installations as Coordination Nodes

The core recommendation is to utilize military bases as coordination nodes—or "seeds"—for unifying federal, state, and local cyber defenses at the civil-military seam. Military installations offer unique advantages: their geographic distribution across the country (approximately 800 DoW installations across 50 states) covers a significant portion of critical infrastructure; active, reserve, and guard personnel have organic cyber capabilities based on private and public sector experience; installations have a strong, institutionally-stable presence in their communities; existing command structures and security clearances facilitate federal coordination; and they have a clear and direct operational interest in the security of surrounding infrastructure (Under Secretary of Defense for Acquisition and Sustainment 2024).

The "seeds" metaphor is deliberate. Installations don't control surrounding ecosystems but provide growth opportunities from which broader resilience capabilities develop. This is not militarization of domestic infrastructure. Rather, it leverages existing military presence to bridge persistent federal-state-local gaps in cyber defense coordination—the same gaps adversaries actively exploit.

Consequently, installation commanders should treat engagement with state and local infrastructure partners as a normal function of readiness rather than a discretionary activity. Regular exchanges of information on critical dependencies, joint participation in regional planning forums, and inclusion in state or regional-level resilience exercises will create a shared understanding of operational risk. Such practices would also clarify the thresholds at which local disruptions become national security concerns.

Institutionalizing Routine Coordination

Experience from both cyber incidents and natural disasters demonstrates that the nature of the relationships established before a crisis determines the effectiveness of the response. Formal structures—such as standing working groups that link installations, National Guard cyber

units, emergency managers, and utilities—can convert episodic cooperation into habitual coordination. Over time, these relationships form a regional network capable of identifying interdependencies, rehearsing response procedures, and coordinating restoration priorities. The value lies not in creating new organizations but in normalizing contact across the existing ones.

Routine coordination also enables the development of clear protocols for rapid coordination during actual cyber incidents. This reduces the risk of improvised responses. Participants know whom to call, what information to share, and how decisions get made.

Integrating Resilience into Readiness Frameworks

Resilience must be treated as a measurable dimension of military readiness. Operational plans that assume assured access to power, water, and digital connectivity should incorporate the risk of local infrastructure disruption and the time required to restore essential services.

Joint vulnerability assessments could help map critical dependencies and single points of failure that could affect multiple customers, including installations. This coordinated mapping would enable military and civilian partners to identify mutually reinforcing investments that could be fulfilled through programs such as the Defense Community Infrastructure Program.

Aligning Incentives and Information Flows

Persistent information asymmetries continue to be a significant impediment to joint resilience. Classified threat reporting seldom reaches those who operate the systems upon which installations depend, while local operational data rarely informs federal planning. The DoW, the ODNI, and the Cybersecurity and Infrastructure Security Agency should continue refining methods to share actionable intelligence at appropriate classification levels.

Parallel adjustments to grant programs and infrastructure funding mechanisms could incentivize civilian operators to adopt security measures that also enhance military continuity, ensuring that national defense and economic resilience advance together rather than in parallel.

Embedding Resilience in Strategic Culture

Ultimately, resilience should be recognized as a strategic attribute of power, rather than a support function. Adversaries seek to exploit friction within the national enterprise, assuming that the fragmentation of responsibilities will slow response and recovery. Countering that assumption requires a culture of planning that anticipates degradation. Integrating civilian infrastructure resilience into national defense planning would demonstrate that the United States can sustain operations under prolonged pressure—an assurance that contributes directly to deterrence credibility.

CONCLUSION: RESILIENCE AS A SHARED IMPERATIVE

Military readiness and civilian critical infrastructure cybersecurity have become inextricably linked by technology, logistics, and shared vulnerabilities. As cyber threats grow more sophisticated and indiscriminate, resilience will depend on hardened systems and on trust, coordination, and sustained partnership across jurisdictions.

Adversaries systematically exploit the gap between federal cybersecurity strategy and under-resourced state and local implementation. Closing this gap requires recognizing that military installations and civilian communities share vital interests in resilient infrastructure. A more resilient power grid, for example, serves residential customers, businesses, hospitals, and military installations simultaneously. This is not a zero-sum competition; it is an alignment of interests.

The December 2024 DoW directive provides the policy mandate. But policy without implementation mechanisms falls short. The future of the nation's cybersecurity will not be determined by technological advancements alone, but by our ability to foster seamless, collaborative resilience across jurisdictional, sectoral, and organizational boundaries. This requires new governance models spanning public and private sectors, intelligence sharing mechanisms balancing security with accessibility, and funding that prioritizes infrastructure resilience.

Military installations and their host communities represent natural starting points for collaboration. This article has proposed leveraging military installations as regional coordination nodes—"seeds" from which federal-state-local partnerships can grow through formalized structures: standing working groups, joint vulnerability assessments, shared threat intelligence, and rehearsed crisis response protocols. By building regional cyber resilience ecosystems around these critical locations, the nation can develop scalable models demonstrating that collaborative cyber defense is operationally feasible.

The path forward requires political will, sustained commitment, and modest resource investment, but the alternative is continuing a fragmented approach that allows adversaries to methodically map and infiltrate the civilian infrastructure foundation of American military power. Whether the United States can defend this foundation depends not on recognizing the threat—which is clear—but on implementing the collaborative partnerships that will drive national resilience.

REFERENCES

Busby, Joshua W., Kyri Baker, Morgan D. Bazilian, Alex Q. Gilbert, Emily Grubert, Varun Rai, Joshua D. Rhodes, Sarang Shidore, Caitlin A. Smith, and Michael E. Webber. 2021. "Cascading risks: Understanding the 2021 winter blackout in Texas." *Energy Research & Social Science* 77 (July). https://doi.org/10.1016/j.erss.2021.102106.

Centers for Disease Control and Prevention and American Water Works Association. 2019. *Emergency Water Supply Planning Guide for Hospitals and Healthcare Facilities.* Technical report. U.S. Department of Health

and Human Services. https://www.cdc.gov/water-emergency/media/pdfs/2024/07/emergency-water-supply-planning-guide-2019-508.pdf.

CISA (Cybersecurity and Infrastructure Security Agency). 2024. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure,* February 7, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

CISA (Cybersecurity and Infrastructure Security Agency). 2025. *Russian GRU Targeting Western Logistics Entities and Technology Companies,* May 21, 2025. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a.

Fixler, Annie, Mark Montgomery, and Rory Lane. 2025. *Military Mobility Depends on Secure Critical Infrastructure.* Foundation for Defense of Democracies (FDD), March 2025. https://www.fdd.org/analysis/2025/03/27/military-mobility-depends-on-secure-critical-infrastructure/.

Gabram, Douglas M. 2021. *Statement on Installation Resiliency: Lessons Learned from Winter Storm Uri and Beyond.* Testimony before the Subcommittee on Readiness of the Committee on Armed Services, House of Representatives, March 26, 2021. https://www.govinfo.gov/content/pkg/CHRG-117hhrg48485/html/CHRG-117hhrg48485.htm.

Guttieri, Karen. 2025. "Fighting Through Disruption: Reframing Cyber Resilience for Power Projection and Strategic Credibility." *Cyber Defense Review* 10 (1): 93–114. https://doi.org/10.55682/cdr/egvf-mkys.

Jeffries, Blaine, Stephanie Saravia, Cedric Carter, and Zachary Ankuda. 2022. *Cyber Risk to Mission Case Study.* Technical report. MITRE, October 14, 2022. https://apps.dtic.mil/sti/trecms/pdf/AD1183009.pdf.

Krouse, Sarah, Robert McMillan, and Dustin Volz. 2024. "China-Linked Hackers Breach U.S. Internet Providers in New 'Salt Typhoon' Cyberattack." *Wall Street Journal* (September 26, 2024). https://www.wsj.com/politics/national-security/china-cyberattack-internet-providers-260bd835.

Military OneSource. 2025. *Military Installations: Joint Base Lewis-McChord,* October 26, 2025. https://installations.militaryonesource.mil/in-depth-overview/joint-base-lewis-mcchord.

Mittal, Manav. 2024. "Colonial Pipeline Cyberattack Drives Urgent Reforms in Cybersecurity and Critical Infrastructure Resilience." *International Journal of Oil, Gas and Coal Engineering* 12 (5): 106–119. https://doi.org/10.11648/j.ogce.20241205.11.

ODNI (Office of the Director of National Intelligence). 2025. *Annual Threat Assessment of the U.S. Intelligence Community.* Technical report. https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf.

Secretary of the Army. 2020. *Army Directive 2020-03 (Installation Energy and Water Resilience Policy).* Technical report. Department of the Army, March 31, 2020. https://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN21689_AD2020_03_FINAL_Revised.pdf.

Simonite, Tom. 2022. "How Starlink Scrambled to Keep Ukraine Online." *WIRED* (May 11, 2022). https://www.wired.com/story/starlink-ukraine-internet/.

Smith, Brad. 2022. "Defending Ukraine: Early Lessons from the Cyber War," June 22, 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/.

Under Secretary of Defense for Acquisition and Sustainment. 2024. *DoD Instruction 4715.28 (Military Installation Resilience).* Department of Defense, December 17, 2024. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/471528p.PDF?ver=ar5bin4QPM3DMnDxJLv0Mw%3D%3D.

Under Secretary of War Comptroller. 2024. *Energy Resilience and Conservation Investment Program (ERCIP) FY 2025 Military Construction, Defense-Wide Project List by State/Country.* Department of War. https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/07_Military_Construction/14-Energy_Resilience_and_Conservation_Investment_Program.pdf.

Viswanatha, Aruna, and Sarah Krouse. 2025. "Chinese Spies Hit More than 80 Countries in 'Salt Typhoon' Breach, FBI Reveals." *Wall Street Journal* (August 27, 2025). https://www.wsj.com/politics/national-security/chinese-spies-hit-more-than-80-countries-in-salt-typhoon-breach-fbi-reveals-59b2108f.

Received 3 July 2025; Revised 27 October 2025; Accepted 5 November 2025

✧ Sector-Specific Resilience ✧

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 41-68
https://doi.org/10.55682/cdr/8esp-2b06

RESEARCH ARTICLE

Defending Health Security: Securing Healthcare Infrastructure against Ransomware

Pavlina Pavlova[1], Craig D. Albert*[2]

[1]Association of NGOs on Crime Prevention and Criminal Justice, Vienna, Austria
[2]Augusta University, Augusta, GA, USA

Ransomware attacks pose a significant threat to the United States, particularly when they target the healthcare sector. State-affiliated and cybercriminal groups exploit vulnerabilities across healthcare networks, supply chains, and software systems, causing financial and operational disruptions and undermining national security. These incidents are increasing in frequency, sophistication, and impact, signaling a deepening cybersecurity crisis. Healthcare remains a prime target due to its reliance on interconnected legacy systems, weak cybersecurity baselines, sensitive patient data, and the need to maintain continuity of care. Large-scale breaches, such as the Change Healthcare incident, underscore ransomware's devastating implications for public health and safety. This paper introduces cyber health security theory, extending the notion of human security into the cyber domain. It posits that the integrity of health systems, data, and care is foundational to national security. Attacks on healthcare infrastructure are direct assaults on sector resilience and individual well-being, with cascading effects on economic and societal stability, and strategic power. Drawing on three case studies and related mitigation strategies, this analysis highlights the urgent need for stronger cybersecurity measures, public-private collaboration, and targeted policy reforms. Strengthening cyber resilience in healthcare is a national security imperative for protecting citizens and preserving societal stability.

Keywords: cybersecurity; health security; ransomware attacks; critical infrastructure; cyber resilience; national security

* Corresponding author: calbert@augusta.edu

INTRODUCTION

Cyberspace is a key operational domain where threat actors project power and exert influence (Fischerkeller, Goldman, and Harknett 2022). States and their proxies have long exploited vulnerabilities to penetrate networks, exfiltrated sensitive data in cyberespionage, manipulated information ecosystems through coordinated influence campaigns, and leveraged plausible deniability to maintain strategic advantage with minimal risk. Exerting pressure on states by attacking critical infrastructure is part of this toolbox to project power. The interconnectivity of critical infrastructure—its systems, services, and supply chains—raises the potential for cyber-attacks to cause large-scale disruptions and affect civilian populations. In this way, ransomware attacks—cyber intrusions that encrypt a victim's data or systems and demand payment for decryption or restored access—constitute a significant strategic threat to the United States (U.S.), with far-reaching implications for national security, economic and societal stability, and public health and safety.

Data breaches can serve as a tool in geopolitics, and recent attacks on U.S. healthcare infrastructure have been linked to cybercriminal groups operating from Russia, Iran, China, and North Korea. Russian ransomware-as-a-service (RaaS) groups such as Black Basta, LockBit, and BlackCat are the main source of ransomware attacks against U.S. healthcare organizations, alongside Qilin, associated with the North Korean state actor Moonstone Sleet (Health-ISAC 2025). While attribution to Chinese groups in recent healthcare-specific ransomware incidents are less documented, state-backed actors have persistently targeted U.S. critical infrastructure, including healthcare, for espionage and disruption (CISA, FBI and HHS 2020). Iranian-affiliated actors, notably the Cyber Av3ngers, compromised healthcare ICS by exploiting vulnerabilities and defacing systems with political messages. These attacks highlight the urgent need for enhanced cyber resilience and coordinated national response strategies in healthcare.

This paper examines the growing threat of ransomware attacks against U.S. critical healthcare infrastructure by addressing the question: Through what mechanisms do ransomware attacks on healthcare infrastructure translate from technical disruptions into threats to national security? To illustrate how harm to the population resulting from these attacks delegitimizes U.S. resiliency, this paper adopts a health security framework and adds to the theoretical space by presenting a case for cyber health security theory. The first section of the paper analyzes how ransomware attacks on critical healthcare infrastructure pose a challenge to national security. The second section details the actors, tactics, and impacts of such attacks to demonstrate resulting harm, and broader implications for national security through a health security lens. The third section illustrates individual and national harm posed by these attacks through three case study briefs including attacks against UnitedHealth, Ascension Health, and Conceptions Reproductive Associates. The paper concludes with a discussion and a set of policy recommendations.

REFRAMING CYBER-ATTACKS ON HEALTHCARE AS A NATIONAL SECURITY CHALLENGE

If a critical infrastructure sector lacks resilience, it poses severe risks to the communities that depend on the essential services it provides. Thus, a lack of resilience represents a threat at the local, state, and federal levels. To assess how attacks on health infrastructure jeopardize national security, it is important to conceptualize resilience in relation to health security. The paper advances two complementary understandings of resilience: (1) cyber and critical infrastructure resiliency, and (2) human or community resiliency.

Cyber resilience is commonly defined by the National Institute of Standards and Technology (NIST 2019), as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources". Concerning critical infrastructure resilience, NIST specifies it as: "the ability to reduce the magnitude and/or duration of disruptive events to critical infrastructure. The effectiveness of a resilient infrastructure or enterprise depends upon its ability to anticipate, absorb, adapt to, and/or rapidly recover from a potentially disruptive event".

Expanding on these definitions, Guttieri (2025, 111) emphasizes the need to "fight through" disruption rather than merely recover from it, arguing that:

> "Resilience is not just the capacity to withstand. It is the ability to fight through, to adapt in contact, and to preserve freedom of action when it matters most. In an era of persistent cyber conflict, it is lethality's indispensable partner. Without it, military power is built on an unstable foundation. With it, national defense becomes adaptable, enduring, and credible."

Building on this perspective, the present paper adopts a whole-of-society approach, including social, organizational, and human behavior factors. It follows an integrated definition of cyber and infrastructure resilience as: the ability to anticipate, prevent, withstand, recover from, adapt to, and fight through adverse conditions, stresses, attacks, or compromises on critical infrastructure and cyber systems.

The second dimension, human or community resilience, draws on the framework proposed by Wulff, Donato, and Lurie (2015), which envisions resilience as fostering healthy individuals and thriving communities. A resilience-centered approach offers concrete strategies to promote sustainable, long-term well-being in communities facing adversity or disaster. While resilience captures the adaptive capacities of systems and communities, it can be more effectively situated within the broader theoretical framework of health security, which is recognized in both international relations and public health scholarship.

The Healthcare and Public Health (HPH) Sector is one of the 16 critical infrastructure sectors identified by the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). In this paper, "critical healthcare infrastructure"

encompasses the full scope of the HPH sector defined by CISA—not only hospitals but also medical device manufacturers, clinics, supply chains, and logistical operations. CISA defines the HPH sector as, "protecting all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters." "Because the vast majority of the sector's assets are privately owned and operated, collaboration and information sharing between public and private sectors is essential to increasing resilience of the nation's Healthcare and Public Health Critical Infrastructure" (CISA, n.d.[b]).

EXTENDING HEALTH SECURITY THEORY INTO THE CYBER DOMAIN

The designation of healthcare as critical infrastructure implies that (cyber-induced) disruptions can have cascading, nationwide consequences. Attacks on hospitals, clinics, and care facilities, therefore, hold the potential to undermine U.S. national security. This threat is particularly salient when viewed through the lens of health security theory.

Health security is a subfield of human security theory, which integrates harms to individuals and perceptions of insecurity into the broader national security paradigm (Peterson 2002). Malik, Barlow, and Johnson (2021) define health security as all aspects of public health that protect the vital core of human lives. Similarly, the U.S. Centers for Disease Control (CDC) defines it as the protection against threats that make people and nations insecure, emphasizing that global health security exists when strong and resilient public health systems can prevent, detect, and respond to infectious disease threats (Centers for Disease Control and Prevention 2024).

Although traditionally focused on communicable and infectious diseases or other natural risks to individual security, health security also concerns protection against acute health vulnerabilities, risks, and threats (Šehović 2020). Traditional frameworks have emphasized protection against naturally occurring hazards such as infectious disease outbreaks, pandemics, and bioterrorism (McInnes and Lee 2006; Davies 2008; Aldis 2008; Fidler 2003). Much of this literature has traced the rise of health security to the 1990s, when crisis such as HIV/AIDS, SARS, and avian influenza reframed disease as both a national and international security concern (Rushton 2011; Caballero-Anthony 2006). Scholars have since cautioned against the securitization of health: Elbe (2010) and Wenham (2019) warn that framing health as security can distort priorities and justify exceptional measures, while Hanrieder and Kreuder-Sonnen (2014) analyze how emergencies reshape governance at the World Health Organization (WHO).

Cyber Health Security Theory

Building on this foundation, while remaining mindful of the risks to improperly securitize healthcare infrastructure resiliency, this paper extends health security theory into the cyber domain. Specifically, we argue that ransomware and other technologically mediated attacks

constitute health-security threats because they undermine both the individual—the foundational unit of security in human-security thinking—and the systems that enable care delivery. Our framework therefore:

(1) centers the individual as the irreducible referent object of security;
(2) expands health security beyond biological threats to include cyber-attacks on healthcare infrastructure;
(3) links systemic resilience with human and community resilience, recognizing that cyber disruptions harm patients, communities, and the state's ability to provide essential services;
(4) treats cyber-attacks on health infrastructure as national security threats due to their cascading harms that extend from the personal to the societal to the geopolitical level.

Cyber health security theory thus asserts that attacks on critical infrastructure are threats to national security because of the catastrophic effects present to individuals. Thus, the theory bridges the gap between traditional notions of the individual in human security approaches, with the broader notions of health security that keep national security as the referent object. In this understanding, health security is national security; or put another way, an attack on a state's citizenry via health infrastructure or health systems is a threat to all national security.

In this expanded view, health security should also encompass human-engineered threats in cyberspace. Ransomware attacks on hospitals or healthcare networks are not merely disruptions of IT systems but assaults on the health and safety of populations. By targeting medical data, devices, and care delivery systems, ransomware produces the full spectrum of harms recognized in health security theory: physical harms (e.g., delayed surgeries, increased morbidity, and mortality), psychological harms (including trauma, stigma, loss of dignity, fear of seeking treatment), and systemic harms (such as the erosion of institutional trust, and cascading failures across interdependent sectors).

Just as pandemics or biothreats have been treated as health-security issues (Albert, Baez, and Rutland 2021), so too should cyber-attacks on healthcare infrastructure, which compromise individual well-being, community resilience, and national security. Within this framework, resilience becomes central: the stronger the individual, community, and infrastructure resilience, the more secure the nation-state.

This paper examines disruptive ransomware attacks on healthcare infrastructure, arguing that their growing volume and intensity inflict not only technical and operational harm but also societal harm, manifested in severe and lasting effects on staff, patients, and communities. Despite the growing scale of such attacks, their direct and cascading effects and impacts on individuals, communities, and society remain under-investigated. While several reports have examined ransomware and its impacts (MacColl et al. 2024), few have addressed how such harms should inform national security and resilience strategies (Oz et al. 2022). The Royal

United Services Institute (RUSI) recently noted significant knowledge gaps in understanding the national-level impact of ransomware, making it challenging to assess the true severity of such harm (MacColl et al. 2024). The remaining gap creates the risk that governments will not prioritize and properly resource responses to ransomware.

Our analysis aims to fill that gap by critically examining the impacts of ransomware attacks on providers and individuals, situating them within broader national security concerns. In doing so, the paper positions effective prevention, response, and recovery from ransomware attacks as a national security priority. The framing offers a novel contribution to the field of cyber defense by demonstrating how these impacts matter for power positioning—and should be factored in—national security strategies. The following section examines the nature and extent of the harms resulting from ransomware attacks targeting U.S. healthcare infrastructure.

RANSOMWARE ATTACKS ON U.S. HEALTHCARE INFRASTRUCTURE: ACTORS, TACTICS, AND IMPACTS

Overview and key actors

Ransomware attacks – malware-based cyber-attacks characterized by blocking access to a device or/and encrypting valuable data for ransom – have intensified in frequency. According to NCC Group (2025), ransomware attacks in 2024 reached record levels, with 5,414 published incidents worldwide, an 11% increase compared to 2023. The Joint Cybersecurity Advisory identified ransomware as one of the most acute cyber threats to the U.S. (CISA, FBI and HHS 2020), the most targeted country globally, accounting for over 50% of recorded cases (Bleih 2025).

Ransomware attacks have evolved in sophistication over the years. Malicious actors operate in organized groups, prominently under RaaS. This model involves collaboration between criminals who develop and maintain the infrastructure and tools behind the operations, and affiliates who conduct operations for a share of profits (Microsoft 2022), effectively lowering the technical and financial threshold for conducting cyber-attacks.

Healthcare and emergency services are among the most targeted sectors. The U.S. Federal Bureau of Investigation (FBI) reported 444 ransomware-related incidents in healthcare in 2024 (238 ransomware threats and 206 data breach events), making healthcare the most targeted critical infrastructure sector (American Hospital Association 2025). Well-documented cases include McLaren Health Care (Alder 2025a), Boston University's Framingham Heart Center for Vein Restoration (Alder 2024c), and telehealth platform ConnectOnCall (Alder 2024d). Threat actors view healthcare as a high-reward, low-resistance target. Medical facilities and services operate in data-rich environments and rely heavily on digital and interconnected systems (Abbou et al. 2024). Rapid digitization and widespread use of networked medical devices have

greatly expanded the attack surface, while cybersecurity, data privacy, and response measures have been treated as secondary concerns. The sector's dependence on legacy systems and outdated software introduces additional vulnerabilities. Third-party contractors and vendors in the healthcare supply chain further increase vulnerability points. The attackers employ phishing as a leading vector to deploy ransomware, and social engineering tactics is leveraged in most data breaches (Fox 2023).

Although ransomware campaigns are financially motivated, these attacks increasingly combine political and ideological motives. For instance, the Conti RaaS group publicly pledged support for Russia's invasion of Ukraine in 2022 (Dudley 2022). According to the FBI and the Department of Homeland Security intelligence, Conti planned simultaneous ransomware attacks on numerous U.S. healthcare facilities (Krebs 2022). U.S. officials also observed close ties between Evil Corp, a Russian cybercrime syndicate responsible for several healthcare attacks in the U.S. (Office of Information Security 2022), and Russia's Federal Security Service (FSB) (U.S. Department of the Treasury 2019). These operations weaken U.S. economic and societal resilience and serve adversarial interests. Research indicates that Russian intelligence agencies maintain a range of symbiotic relationships with cybercriminals, providing sanctuary jurisdiction, plausible deniability, and at times co-opting their operations for strategic purposes (Nershi and Grossman 2023).

North Korean criminals have targeted a wide range of sectors for financial purposes, including healthcare facilities. Most of these attacks have been directed at the U.S. and South Korea, both in volume and impact, with an increasing degree of scale, sophistication, and strategic value. In 2022, the U.S. Department of Justice indicted North Korean national Rim Jong Hyok for conspiracy to commit computer hacking and money laundering. Believed to be a member of the Andariel hacker group, controlled by the Reconnaissance General Bureau, Rim allegedly orchestrated ransomware attacks against 17 healthcare entities across 11 U.S. states (Landi 2024). The Qilin RaaS, associated with North Korea and believed to cooperate with the Moonstone Sleet threat group, has become a leading ransomware actor targeting healthcare (Moody 2025). Illicit proceeds from these operations are often traced to the North Korean regime's weapons programs developing nuclear and submarine capabilities (Bae 2025).

Evolving tactics and patterns of harm

Ransomware coercive tactics have evolved as organizations improve defenses, secure backups, and resist ransom payments. Originally focused on encrypting victims' data and demanding payment for decryption, attackers increasingly shift to double and triple extortion, exfiltrating data and threatening public disclosure to maximize leverage with reputational damage. A larger radius of victim organizations and even patients can be extorted as secondary targets. Multiple ransomware operators have published stolen medical data following breaches —

prominent cases include stigmatized diagnoses alongside personally identifiable information in Australia's Medicare health insurance breach (SBS News 2024), mental health records in the Vastaamo clinic attack in Finland (Ghanbari and Koskinen 2024), medical records of minors in a ransomware attack against the Scottish National Health Service (Martin) and blood test data in a hack of the National Health Service blood testing company in England (BBC News 2024). In some cases, perpetrators explicitly publicize leak sites to amplify harm; for example, detailing that stolen data included nude images of patients, information related to sexual and reproductive health, or other sensitive diagnoses, alongside protected health information (PHI), potentially linked to personally identifiable information (PII) (Pavlova 2024). The resulting coercive distress over data misuse and stigma increases pressure on the organizations to pay ransom. Such attacks clearly meet the conditions to constitute a threat to health security and thus, to national security. By disrupting medical care, leading to poorer health outcomes, and exposing patients' medical and private data for further victimization (Pavlova 2025), these incidents threaten both individual lives and societal resilience.

Ransomware also causes reputational damages, especially when media scrutiny reveals failure to comply with security standards (Pattnaik et al. 2023). Given the highly regulated nature of U.S. healthcare data, any unauthorized disclosure carries regulatory and legal risk to the organization. The sensitivity of health information increases the value of stolen data for extortion, pressuring organizations to pay to prevent exposure. When public trust erodes, communities lose confidence in the provided care and institutions, undermining social stability and national security, and harming both medical staff and patients. These cumulative impacts highlight the need to prioritize preparedness and recovery, and the impacts should guide risk assessments, resource allocation, and policy innovation (Agrafiotis et al. 2018). As argued earlier, and demonstrated in the following section, attacks on healthcare infrastructure are attacks on health security, violating the core of public health security by imposing physical, emotional, and psychological harm.

To structure the assessment of these effects, Agrafiotis et al. (2018) introduced a taxonomy of five harm types—physical/digital, economic, psychological, reputational, and social and societal. This can inform countries on cost-effective measures for the prevention and mitigation of demonstrable cyber-enabled harms, including indirect or secondary effects. Similarly, the CyberPeace Institute's Harms Methodology (CyberPeace Institute 2024) identifies overlapping categories such as physical, psychological, deprivation, societal, environmental, and harm to international peace and security. Assessing the full extent and sequence of harms remains challenging due to limited quantitative and qualitative data about the incidents and multi-tiered causality. Therefore, case studies present an important contribution in documenting the impacts of ransomware attacks against healthcare. Such analysis enables mapping the level and extent of experienced harms, as opposed to speculating about potential harms (Horne, Mott, and MacColl 2024).

RESEARCH OBJECTIVES

The following comparative case study illustrates how ransomware attacks pose a significant threat to national security, particularly in the context of health security theory.

Our main research question is: *Through what mechanisms do ransomware attacks on healthcare infrastructure translate from technical disruptions into threats to national security?*

The analysis also addresses several sub-questions: first, which structural and organizational factors amplify or mitigate the national-level impacts of ransomware attacks in the healthcare sector? Second, how do different forms of harm (technical, operational, and societal) interact to undermine resilience and public trust? Third, what governance gaps (detection, coordination, communication) emerge across cases, and how do they shape the capacity to contain cascading harm? And finally, how can the novel concept of cyber health security advance understanding of the link between digital infrastructure failures and human security at scale?

CASE STUDY ANALYSIS

To address our research questions, we analyzed three major ransomware incidents that affected the U.S. healthcare sector and had implications for national security. The cases feature different foreign ransomware groups with varied tactics and have documented forensic, operational, and societal impacts. The selection observed a purposive sampling technique (Carr et al. 2018) to conduct a brief case study analysis.

The analysis applies a structured coding scheme and harm taxonomy. The coding scheme traces the attack lifecycle, from initial access and lateral movement to encryption and extortion. The harm taxonomy differentiates:

(1) technical harms (data breaches, system outages),
(2) organizational harms (operational disruption, financial loss, reputational damage),
(3) societal harms, including individual (compromised data, delayed or denied care, psychological distress), community (disruption of continuity of services, erosion of trust in institutions) and national-level harms (systemic fragility that adversarial states can exploit).

This framework maps how technical vulnerabilities cascade into societal consequences. Each case features a matrix demonstrating the specific parameters of the attack and response, followed by a comparative analysis that explains the cases in relation to the research objectives.

Case 1: UnitedHealth/Change Healthcare breach (February 2024)

Change Healthcare, a UnitedHealth Group-owned U.S. company providing revenue and payment cycle management services, connects healthcare providers, payers, and patients. On February 21, 2024, the company detected a ransomware attack and disconnected infected

networks, later attributing the incident to BlackCat/ALPHV. This Russian-speaking RaaS specializes in multi-stage intrusions that escalate through double and triple extortion tactics, including data theft, publication threats and DDoS attacks (Martin 2023). On March 3, 2024, UnitedHealth reportedly paid a $22 million ransom, but the payment did not secure the stolen data. On March 13, Change Healthcare obtained a copy of the stolen files to assess the breach, and between June 20, 2024, and January 14, 2025, affected individuals were notified (Change Healthcare 2024). The U.S. Department of State later offered rewards of up to $10 million for information leading to the identification or location of the perpetrators (Alder 2025b). The Office for Civil Rights opened an investigation to determine if the breach was the result of a failure to comply with the HIPAA Security Rule standards. The attack forced Change Healthcare to shut down its entire network, causing widespread outages across the healthcare sector. Disruptions affected billing systems, insurance claims, and prescription fulfillment, halting revenue cycles for providers and threatening the financial viability of healthcare organizations nationwide (Alder 2025b).

Because Change Healthcare's works as a vendor to both providers and insurers, the attack exposed a vast array of personal and medical data (Alder 2025b). In May 2024, UnitedHealth CEO Andrew Witty testified before Congress that a third of all American's health data may have been compromised (Abrams 2025). The company's data breach notification later confirmed that the ransomware attack exposed a "substantial quantity of data" belonging to a "substantial proportion of people in America", with early estimates ranging from 100 to 190 million affected individuals (Abrams 2025). Stolen data included health insurance information, medical record numbers, providers and diagnoses details, billing and claims data, payment information, and government identifiers. UnitedHealth stated that it had not identified evidence of active misuse of the stolen data (Change Healthcare 2024).

Since June 20, 2024, Change Healthcare has provided a notice to help individuals understand what happened, detailing which information might have been impacted, and providing guidance to protect privacy, including a complimentary credit monitoring and identity theft protection services (Change Healthcare 2024). A third-party firm was hired to monitor the dark web for leaked data (Alder 2025b). Nearly 50 lawsuits were filed, and UnitedHealth estimated the cost of the breach to $2.46 billion (Change Healthcare 2024). The cyber-attack has been described as "the most significant and consequential incident of its kind against the U.S. healthcare system in history," highlighting the vulnerability of critical healthcare infrastructure to cyber threats (CMIT Solutions, n.d.). This incident was not only an attack on systems but also an assault on people, exposing vast amount of personal and medical data and producing long-term insecurity in ways that health security scholars describe as threats to the "vital core of human lives" (McInnes and Lee 2006; Aldis 2008).

At the individual level, the compromise of diagnoses, insurance identifiers, and financial information undermined privacy, financial stability, and mental health—echoing Stoeva's

(2020) argument that health security must include both psychosocial and systemic dimensions of vulnerability. At the community level, widespread delays in billing, claims processing, and prescription fulfillment disrupted continuity of care, eroded trust in providers, and disproportionately burdened vulnerable populations, aligning with Davies's (2008) and Rushton's (2011) observations that health insecurity often exacerbates inequality and uneven access to essential services.

At the national level, the incident demonstrated how the concentration of key functions in a single clearinghouse can create systemic fragility, where compromise of one node cascades across the entire healthcare ecosystem. From a health-security perspective, this exemplifies how resilience failures in critical health infrastructure become matters of national security. The securitization literature warns that such crises justify extraordinary state intervention (Elbe 2010; Wenham 2019). This case illustrates how ransomware attacks against healthcare simultaneously undermine patient security, community resilience, and the nation's ability to protect its citizens.

Table 1. Change Healthcare Attack Matrix

Exploited vulnerabilities		Citrix access with compromised credentials; missing multi-factor authentication (MFA) enabled lateral movement and data exfiltration before ransomware deployment; prolonged breach detection.
Attack tactics		Multi-stage intrusion; double extortion (encryption + exfiltration + threats to publish stolen data); exit scam after ransom payment without data suppression.
Causal chain		Missing MFA on Citrix + stolen credentials → multi-stage intrusion → exfiltration + encryption + extortion → clearinghouse shutdown → Rx/claims/billing paralysis → provider cash-flow crisis + delayed care → population-scale exposure and national-level response.
Mitigation	*Success*	Rapid network isolation to contain spread; large-scale notification and monitoring; cross-sector coordination.
	Failure	Attack detection ~9 days after initial infiltration (delayed containment); ransom payment failed to secure/suppress stolen data and RaaS executed an exit scam; vendor concentration produced cascading impacts.
Harms	*Technical*	Theft of vast PHI/PII/financial data; confidentiality compromise of ~190 million Americans; risk to data integrity (claims/billing accuracy); multi-week outages impacting availability (2 weeks to 3 months for some providers to normalize); disruptions across U.S. hospitals and providers.
	Operational	Nationwide outages in prescription fulfillment, claims processing, and billing; revenue cycles interrupted for weeks; $2.46B reported cost; ~50 lawsuits; OCR investigation on HIPAA Security Rule compliance; dark-web monitoring initiated.
	Societal	Widespread exposure of medical/identity data; delayed/denied care and pharmacy disruptions; erosion of trust in healthcare infrastructure; national-level attention (including $10M reward for perpetrators); threat to national health security.

Case 2: Ascension Health (February 2024)

Ascension Health, a nationwide healthcare organization operating 118 hospitals and multiple care facilities, including services for low-income populations and senior living facilities (Ahmed 2024; Greig 2024), suffered a major cyber-attack in 2024. The intrusion began on

February 29, but the data breach remained undetected until May 8, disrupting clinical operations across six states upon detection. The Black Basta RaaS group was identified as the perpetrator. The cybercriminal gang uses aggressive double extortion tactics, selecting victims to maximize impact, rather than having a broad, indiscriminate approach. Its tactics leverage phishing, software vulnerabilities, and social engineering, supported by obfuscation methods to evade detection (CISA 2024a; Flashpoint 2024). A joint U.S. cybersecurity advisory warned the healthcare sector about the Black Basta's activities (Alder 2024b).

The attack was launched when an employee downloaded a malicious file disguised as legitimate content, locking providers out of electronic health records, communication systems, and systems utilized to order tests, procedures, and medications (Pradhan and Wells 2024). Multiple facilities lost access to electronic records for weeks. A nurse in Michigan reported that the outage was "put[ting] patients' lives in danger," while other affected staff described delayed or lost lab results, medication errors, and an absence of routine safety checks via technology to prevent potentially fatal mistakes. At Ascension St. John Hospital in Detroit, clinicians waited up to four hours for computed tomography (CT) scans of patients with strokes or brain bleeds (Shamus 2024). Another nurse in Kansas nearly administered the wrong narcotic dose, relying on paperwork when electronic patient data became unavailable. Across several states, medical staff reported that patient care was severely compromised (Pradhan and Wells 2024).

It took the hospital network weeks to restore every facility's access to the internet and records systems, and patient wait times tripled during the recovery process (Greig 2024). Ascension reported an 8-12% drop in patient volume between May and June compared to 2023, attributing the decline to the disruptions caused by the incident (Ahmed 2024). This event clearly demonstrates how ransomware attacks produce health insecurity that cascades from the individual to the national level, undermining both care delivery, patient safety, and resilience.

The data potentially accessed in the breach included personal information, medical data (e.g., record number, dates of service, lab test types, procedure codes), payment details (credit card and bank account numbers), insurance information, and government identifiers. On December 20, 2024, Ascension notified the Maine Attorney General that 5.6 million individuals were affected in the breach (Alder 2024a). Impacted patients were offered 24 months of credit monitoring, a $1 million insurance reimbursement policy, and identity theft recovery services (Freedman 2025). There was no evidence that patient electronic health records were directly compromised following the attack (Ahmed 2024).

The financial consequences for the provider were substantial. The attack caused delays in revenue cycles, claims submission, and payment processing. For the fiscal year ending June 30, 2024, Ascension reported $1.4 billion in recurring operational losses, equivalent to a -4.9% margin (Arghire 2024; Vogel 2024). Class-action lawsuits were filed by patients in Texas,

Illinois, and Tennessee over exposure of sensitive health data (Greig 2024). The attack also compounded the downstream effects of the Change Healthcare breach, intensifying systemic stress on national healthcare operations (Ahmed 2024).

The Ascension's ransomware attack exemplifies how cyber incidents manifest as health insecurity across multiple levels. At the individual level, patients endured delayed diagnostics, postponed surgeries, and lapses in medication safety—directly endangering life and health. These harms echo McInnes and Lee (2006) and Aldis (2008), who argue that health security must prioritize the protection of individuals as the foundational unit of security. At the community level, prolonged electronic health record outages and system lockouts forced hospitals to revert to paper-based processes, leading to longer wait times, ambulance diversions, and reduced patient capacity. This aligns with Davies (2008) and Rushton (2011), who note that health insecurity deepens inequities in access to care.

At the national level, the compromise of a system spanning 118 hospitals revealed the structural fragility of a large U.S. healthcare network, confirming Stoeva's (2020) multidimensional framework that ties hazards and exposure to resilience and governance.

From the perspective of securitization theory, such widespread disruptions necessitate extraordinary state responses to protect population health (Elbe 2010; Wenham 2019). The Ascension case illustrates that ransomware is not merely a technical or financial incident, but a profound health-security breach, cascading from individual harm to systemic vulnerability, ultimately threatening national resilience and security.

Case 3: Conceptions Reproductive Associates (April 2024)

Conceptions Reproductive Associates of Colorado is a women's healthcare and fertility organization, providing a range of fertility testing and treatment services (Strauss Borrelli PLLC 2024). In early 2024, the clinic suffered a ransomware attack detected in mid-April 2024. The threat actor infiltrated legacy systems and extracted data files of approximately 80,000 patients and their associates (Peintener 2024; Culhane 2025). The attack was attributed to the INC_RANSOM group (BreachSense, n.d.), a cybercriminal gang with indicators of Russian affiliation. INC_RANSOM employs a multi-staged attack strategy, combining spear-phishing, vulnerability exploitation, and double extortion tactics to maximize damage and enforce ransom payments. The group has been linked to the exploitation of a critical Citrix NetScaler vulnerability, which allows attackers to bypass multi-factor authentication and hijack legitimate user sessions (Vectra AI, n.d.).

The breach exposed personal identifiers, medical information (including test results, diagnostic imaging, and vital signs), government identification and financial details such as account and credit card numbers (Business Insider 2025; Ortega 2024). Public notification began on November 25—six months after detection— a delay that allegedly violated HIPAA

Table 2. Ascension Health Attack Matrix

Exploited vulnerabilities		Employee downloading a malicious file; phishing; RaaS leveraged software vulnerabilities and social engineering; prolonged undetected breach causing delayed response; gaps in electronic data systems containment and least-privilege allowed rapid propagation.
Attack tactics		Double extortion targeting high-impact systems, using phishing, software vulnerabilities, social engineering, and obfuscation techniques to evade detection.
Causal chain		Malicious file downloaded by employee → RaaS intrusion → systems locked (EHR, phones, test/procedure ordering) → weeks-long outage → delayed care, postponed surgeries, ambulance diversions → increased wait times and medical errors → drop in patient volume + operational losses → lawsuits and regulatory filings → national-level healthcare disruption and security concerns.
Mitigation	*Success*	Paper and manual fallbacks sustained minimal continuity; eventual restoration of internet and systems access across facilities; notification to affected individuals; provision of 24-month credit monitoring, insurance reimbursement, and identity-theft recovery services.
	Failure	Delayed detection (attack began Feb 29, detected May 8), indicating insufficient monitoring, privilege controls, and electronic data system containment; prolonged operational paralysis; EHR data not confirmed compromised, but system unavailability persisted; endpoint hygiene and attachment isolation likely inadequate.
Harms	*Technical*	Potential exposure of personal, medical, payment, insurance, and government ID data for 5.6 million individuals; system lockouts caused multi-week unavailability of EHRs and communication systems.
	Operational	Clinical operations disrupted across six states; postponed surgeries and appointments; ambulance diversions; medication errors; nurses forced into ad-hoc manual workarounds; tripled wait times; 8–12% YoY drop in patient volume (May–Jun); $1.4B loss with –4.9% operating margin; multiple class-action lawsuits.
	Societal	Patient care compromised with life-threatening consequences; elevated clinical risk (e.g., delayed stroke/bleed CTs, medication safety lapses); reduced patient volume; community-wide delays and safety hazards; strain on providers; systemic vulnerability highlighting national health security risks and erosion of public trust in healthcare continuity.

requirements (Culhane 2025). Attacks against sexual and reproductive health data pose particularly serious risks. Exposure of such information can cause long-term harm to women, discourage access to healthcare, and lead to discriminatory access to services (Pavlova 2024). Recent ransomware incidents have increasingly involved sensitive and stigmatized data, including records of sexual orientation, gender, reproductive status, and biometric information (MacColl et al. 2024; Pavlova 2025). Wong (2024) observes that "Russian hackers 'train' for state-sponsored operations by conducting ransomware attacks against Western states, targeting victims based on how personally devastating their leaked data might be". These dynamics illustrate how ransomware attacks on reproductive health providers threaten patient privacy and safety, inflict psychological and social harm, underscoring their relevance to the national security agenda.

The Conceptions ransomware incident reveals how cyber-attacks intersect with deeply personal domains of health security. At the individual level, the exposure of reproductive and fertility data carried the risk of stigma, discrimination, psychological and even physical harm, threatening what McInnes and Lee (2006) describe as the "vital core" of personal well-being.

At the community level, breaches of reproductive health data risk deterring women and marginalized groups from seeking care, reinforcing Davies's (2008) concern that health insecurity amplifies social inequities (such as inability to pay for care or travel, rural residence, and limited autonomy) and barriers to essential services (Pavlova 2025).

At the societal and national levels, adversarial actors can weaponize such breaches to sow distrust, exploit cultural and political sensitivities, and undermine confidence in health institutions—an effect Stoeva (2020) emphasizes in her multidimensional account of health security, where governance and resilience are equally critical as hazard response. In this light, ransomware impacts extend beyond data compromise; these attacks reshape patterns of access, erode institutional legitimacy, and challenge state capacity to uphold secure, equitable health systems.

Table 3. Women's Health Clinic Attack Matrix

Exploited vulnerabilities		Legacy systems; Citrix NetScaler flaw allowing MFA bypass and session hijack; spear-phishing; limited security staffing and elevated exposure due to legacy infrastructure.
Attack tactics		Multi-stage intrusion; double extortion (exfiltration + leak threat) leveraging highly sensitive reproductive data
Causal chain		Legacy/Citrix exposure + spear-phishing → INC_RANSOM intrusion + data exfiltration → extortion leveraging sensitive reproductive data → erosion of trust + delayed notification → deterrence from care + heightened psychosocial harm.
Mitigation	*Success*	(Limited evidence) Eventual identification of breach scope and notification of affected individuals.
	Failure	Notification latency (six-month delay undermining risk mitigation); legacy systems and incomplete MFA/patching enabling intrusion.
Harms	*Technical*	Confidentiality breach affecting ~80,000 individuals (PHI, PII, financial data, test results, imaging). Operational impacts not quantified.
	Operational	Notification delay triggered HIPAA compliance scrutiny; reputational damage; costs for forensic investigation, response, and notification (amounts not publicly disclosed).
	Societal	Long-term gendered harms; psychological distress and stigma; chilling effect on care-seeking; potential exacerbation of inequities and disparities in healthcare access; erosion of trust in healthcare provision; national security risks from exposure and potential weaponization of sensitive health data, with implications for social cohesion and public health resilience.

Cross-Case Comparative Analysis: Pathways from Cyberattacks to National Security Threats

The comparative examination of the Change Healthcare, Ascension Health, and Conceptions Reproductive Associates incidents highlights distinct but interrelated mechanisms through which ransomware attacks against healthcare systems cascade into national security concerns. Five recurring patterns emerge across cases: vulnerability drivers, attack dynamics, response capacity, harm distribution, and governance and resilience factors. Vulnerability patterns show how specific weaknesses serve as entry points for widespread disruption. Attacks dynamics details how attacker behavior interacts with those vulnerabilities to produce cascading effects. The remaining factors track escalation from technical failures to operational

paralysis, social destabilization, and erosion of institutional trust. Together, these patterns outline the causal pathways by which local cyber incidents escalate into systemic threats.

Patterns of vulnerability. Each case exposes a unique configuration of vulnerabilities that magnified the consequences of attack. Change Healthcare demonstrated the dangers of systemic concentration: the absence of multi-factor authentication on Citrix systems allowed credential compromise, while the organization's national clearinghouse function created a single point of failure for claims and billing across the U.S. healthcare economy. Ascension Health revealed the risks inherent in human-technical interface failures: an employee's mistaken download, combined with inadequate endpoint isolation and monitoring, paralyzed six state-wide hospital networks. Conceptions Reproductive Associates, by contrast, exemplified under-resourced cybersecurity capacity: outdated legacy systems and minimal staff oversight enabled a relatively small breach to produce psychosocial harm. Across cases, interdependence without redundancy emerged as the key vulnerability vector—whether through centralized infrastructure, dispersed but poorly governed systems, or small clinics lacking defensive capacity—and compounded by excessive or poorly controlled access privileges that allowed attackers to move laterally and escalate their impact.

Attacks tactics and escalation. While all attackers employed multi-stage intrusions and extortion tactics, their objectives and escalation logics diverged. BlackCat/ALPHV sought maximum systemic leverage by targeting a national intermediary whose paralysis could coerce payment through sheer scale. Black Basta aimed for high operational disruption, focusing on direct interference with patient care to generate urgency. INC_RANSOM exploited data sensitivity, using reproductive health information to inflict reputational and psychological pressure. These differences illustrate how ransomware operations have evolved from opportunistic crime into adaptive strategies aligned with victims' societal salience. The targeting of healthcare, where human life and trust are at stake, maximizes coercive power and political symbolism. These cases clearly exemplify how ransomware attacks support the cyber health security theory framework as threats to national security.

Detection and response capacity. Response timelines varied but were decisive in determining harm severity. Change Healthcare detected the intrusion nine days after initial compromise, too late to prevent exfiltration, and its ransom payment failed to suppress data publication. Ascension required over two months to detect and isolate the breach, relying on paper-based fallbacks during disruptions that preserved minimal continuity but generated clinical risk. Conceptions identified the incident within weeks but delayed public notification for six months, compounding regulatory exposure and community mistrust. Across cases, temporal lag (between infiltration, detection, containment, and disclosure) proved central. Each delay amplified cascading consequences: data exposure in Change Healthcare, clinical paralysis in

Ascension, and psychosocial trauma in Conceptions. Thus, speed of detection and transparency of communication are as critical to national resilience as technical containment.

Distribution and cascading of harms. Although all incidents inflicted multi-layered damage, the dominant harm type differed. Change Healthcare produced economic and systemic harm: a $2.46 billion cost, nationwide billing paralysis, and exposure of 190 million citizens. Ascension Health caused operational and clinical harm: delayed diagnostics, medication errors, and direct threats to patient safety, accompanied by $1.4 billion in losses. Conceptions generated psychosocial and ethical harm: stigma, discrimination, and deterrence from reproductive care, magnified by the gendered nature of the data. These variations confirm that ransomware is a multidimensional security hazard. Technical breaches quickly cascade into organizational disruption, which in turn yields social destabilization, regulatory, and public pressure. The resulting erosion of trust in healthcare systems constitutes a strategic vulnerability at the national level.

Governance and resilience factors. Across cases, three governance failures explain escalation trajectories:

- Concentration without redundancy (Change Healthcare) magnified systemic risk.
- Distributed operations without adequate oversight (Ascension) extended recovery time.
- Limited compliance and communication capacity (Conceptions) deepened psychosocial impact.

Conversely, partial successes, such as network isolation (Change Healthcare) and manual continuity procedures (Ascension), show that resilience depends not only on technical defenses but on organizational adaptability and human coordination. Effective cyber health security, therefore, requires a whole-of-society approach integrating technological safeguards, human judgment, and transparent communication.

These findings shed light on the mechanisms linking cyber incidents to national security concerns. Technical vulnerabilities and governance gaps interact with operational dependencies, social trust, and data sensitivity to generate cascading harm. When healthcare systems fail, the result is not confined to service interruption; it is a crisis of human security that undermines confidence in institutions and challenges the state's capacity to protect populations. These insights reinforce the central argument of cyber health security theory: safeguarding digital health infrastructures is inseparable from safeguarding the vital core of human life, and thus an essential component of national security strategy.

FROM HEALTH INSECURITY TO NATIONAL SECURITY THREAT: DISCUSSION AND POLICY RECOMMENDATIONS

The comparative analysis above identified five recurring mechanisms through which ransomware incidents in healthcare escalate from local technical disruptions to national-level insecurity. Building on these empirical insights, this discussion interprets their broader theoretical significance through the lens of cyber health security and translates them into concrete governance and policy recommendations.

There are four main clusters of recommendations (Table 4), encompassing both novel contributions and refinements of well-established ideas that remain underdeveloped in this context. Together, they include the reinforcement of existing policies, proposed revisions to current practices, and the introduction of new measures.

Table 4. Summary of Cyber Health Security Clusters and Key Recommendations

	Established recommendations	Novel recommendations
Strategic and institutional integration	Recognize ransomware as a national security threat (McInnes and Lee 2006; Aldis 2008) Integrate health systems into national security planning (WHO 2018; Brown et al. 2022) Mandatory incident reporting (CIRCIA 2024; U.S. Congress 2015) International cooperation (Five Eyes, Counter Ransomware Initiative)	Designate key healthcare operations as Health Security Critical Functions Make cybersecurity a condition for Medicare/Medicaid participation Establish Health Security Activation Protocol (HSAP) Adopt Ukraine's "radical disclosure and sharing" model.
Operational and infrastructural backbone	Privacy-by-design and data protection strategies (Saltarella et al. 2024; Mitra et al. 2023) Regular risk and supply chain vulnerability assessments Redundant, segmented security systems CISA's Cybersecurity Performance Goals Security-by-design for supply chains (CISA 2024c)	Comprehensive data collection and standardized incident methodologies Health-Cyber Reserve Corps for surge capacity Early safeguards for emerging technologies (AR/VR, AI-assisted telehealth).
Societal and psychological resilience	Psychological harm recognition (Pavlova 2024) HIPAA Breach Notification Rule Credit monitoring and mental health support for breach victims	Greater transparency in reporting downstream harms Health-Security Harm Registry Clearer distinctions between system-targeted and individual-targeted attacks.
Economic continuity and accountability	Cyber insurance as soft regulator (Adriko and Nurse 2024b) Financial safeguards for cyber-related health crises Public-private partnerships for resilience investments CISA's Joint Cyber Defense Collaborative expanded to include healthcare-specific working groups	Accountability frameworks for private sector actors in health tech Regular review of cyber insurance policies and state support for uncovered infrastructure Incident classification to include dignity and economic security impacts Public-private bond programs.

Strategic and Institutional Integration: Embedding Cyber Health Security into National Security Doctrine

Ransomware attacks on healthcare are not merely technical disruptions or financial crimes; they represent national security threats when viewed through health security theory, which emphasizes the protection of the "vital core" of human life (McInnes and Lee 2006; Aldis 2008). Health security spans hazards, exposure, resilience, and governance (Stoeva 2020).

Ransomware produces cascading harms at the individual (compromised data, delayed care, psychological distress), community (service disruption, erosion of trust), and national levels (systemic fragility exploitable by adversaries). Thus, digital vulnerabilities become health insecurity and, ultimately, national insecurity.

To address this, the federal government should designate key healthcare operations—claims processors, e-prescribing systems, oxygen supply chains, trauma centers—as Health Security Critical Functions, similar to energy and financial sectors. This aligns with the WHO's framework on essential public health functions and calls for integrating health systems into national security planning (WHO 2018; Brown et al. 2022). Such designation mandates redundancy, resilience testing, and prioritized protection. Cybersecurity must be reframed as a condition of participation in the national healthcare system, not just an administrative requirement. Medicare and Medicaid reimbursements should be contingent on baseline safeguards (e.g., MFA, segmented networks, immutable backups), aligned with CISA's Cybersecurity Performance Goals. Prompt cyber incident reporting and information sharing must be mandatory, closing coordination gaps identified under the Cybersecurity Information Sharing Act (U.S. Congress 2015) and Cyber Incident Reporting for Critical Infrastructure Act (U.S. Congress 2022).

The Cybersecurity Information Sharing Act of 2015, which established CISA, should be reauthorized and expanded to address health security harms (Ribeiro 2024). Ukraine's model of "radical disclosure and sharing" during the invasion—rapid intelligence sharing and declassification—offers a compelling precedent. CISA's "Ukraine tensions plan", joint exercises with infrastructure owners, and pre-ransomware notification initiatives reflect this approach (Zegart 2022; Vasquez 2023; CISA 2022; CISA and FBI 2022). The U.S. should adopt similar strategies. Incident classification should account for physical, financial, psychological, and societal harms, including impacts on dignity and economic security, to better inform response and resilience planning.

A Health Security Activation Protocol (HSAP) should be established to define thresholds for national-level responses to large-scale cyber disruptions. When triggered, HSAP would mobilize federal and state agencies (HHS, FEMA) to coordinate containment and recovery, operationalizing resilience theory (Guttieri 2025). In this light, a Health-Cyber Reserve Corps of vetted cybersecurity engineers and clinical IT specialists should be established to support hospitals during prolonged outages, maintaining essential care amid cyber disruption. Measurement must also evolve. Existing reporting systems still focus narrowly on financial loss or the number of records breached, missing broader health security harms.

At the international level, the U.S. should reinforce global cooperation, cyber norms, and accountability mechanisms through continuous engagement with the International Counter Ransomware Initiative and the Five Eyes alliance. A compelling example was presented

in joint sanctions by the U.S., UK, and Australia against perpetrators of the Medibank ransomware attack (U.S. Department of the Treasury 2024). Clear redlines must be established to reaffirm that some critical infrastructure, like healthcare, are off-limit targets. Coordinated sanctions, payment tracing and seizing, and law-enforcement collaboration can help dismantle ransomware networks and deter future attacks.

Operational and Infrastructural Backbone for Resilience

Building resilience against cyber-attacks on critical healthcare infrastructure requires comprehensive data collection and standardized incident methodologies (HHS 2022). Quantitative and qualitative indicators reveal vulnerabilities, enabling preventative and restorative strategies. Data-driven and patient-centered approaches highlight harms beyond financial loss, improving resource allocation, risk assessments, and incident response planning. Standardized methodologies support regulatory and policy development by identifying sector-wide patterns (WHO 2024).

Healthcare providers must adopt privacy-by-design principles (Saltarella et al. 2024) and data protection strategies: they must understand what data is collected (privacy-by-design), how it is stored (data protection strategy; Mitra et al. (2023)), who has access to it (privileged access strategy; McConomy and Leber (2022) and Mandru (2024)), and where it will end up following any data-related transaction. Organizations should identify their 'crown jewels'—critical and sensitive data assets requiring the highest protection. The White House Executive Order 14117 (2024) on sensitive personal data underscores data as a national security imperative. The order puts a clear requirement on the private sector to closely know their data and the nature of its sensitivity. We recommend following these guidelines and tracking which organizations are abiding by them.

Cybersecurity readiness must include regular risk and supply chain vulnerability assessments, redundant and segmented security systems, clear delineation of responsibilities, and early safeguards for emerging technologies like AR/VR and AI-assisted telehealth. Cybersecurity must be a continuous enabler of healthcare—not a compliance checkbox. Leadership should invest in cyber hygiene programs, continuity testing, and regular crisis exercises (CyberPeace Institute 2022). CISA's Cross-Sector Cybersecurity Performance Goals provide baseline practices for mitigating risks across critical infrastructure (CISA, n.d.[a]). The National Security Memorandum (NSM) extends these principles by promoting minimum security standards and resilience across essential services (CISA 2024b; The White House Office of the Press Secretary 2013). Finally, healthcare providers must secure their medical supply chains using security-by-design principles (CISA 2024c) to limit systemic vulnerabilities. These measures should be mandatory, not voluntary.

Societal and Psychological Resilience: Translating Human Harms into Governance Insight

Harms caused by ransomware attacks unfold across temporal and social scales. Technical and operational harms are almost immediate, while economic and psychological harms may surface later, depending on the service affected. Victims of healthcare data breaches experience psychological insecurity, violation, and trauma, especially when medical and personal data are exposed together. Once breached, data may circulate indefinitely, making harm effectively permanent (Pavlova 2024). Incident reporting remains inconsistent and incomplete, impeding research into cascading effects. Organizations must determine how far downstream to assess harm and what is appropriate to include, especially for cyberattacks targeting healthcare, where both immediate and long-term reliance on the provided services is pronounced. Greater transparency on the multiple tiers of impacts would improve understanding and benefit organizational, community, and national resilience.

Timely communication and transparent reporting are crucial in reducing psychological harm during crises. Under HIPAA's Breach Notification Rule, providers must notify individuals of PHI breaches within 60 days (HHS 2023). Organizations should offer credit monitoring, identity theft recovery, insurance reimbursement, and mental health support to affected individuals. More proactive, empathetic, and timely engagement with victims and staff, and clearer distinctions between system-targeted and individual-targeted attacks are needed to increase resilience against aggressive ransomware tactics. Measurement must evolve beyond financial loss or records breached. A dedicated Health-Security Harm Registry should be established to capture the full spectrum of consequences that health security theory highlights: delayed surgeries, diverted ambulances, mortality incidents, and psychological harms to patients and staff. Such a registry aligns with the RUSI framework (MacColl et al. 2024) on cyber harms and would ensure that policy decisions reflect the true human and systemic costs of cyberattacks, not just economic metrics.

Economic Continuity and Accountability: Sustaining National Health Security Readiness

Protecting health sector supply chains from cyber disruptions is a critical part of national power positioning amid intensifying ransomware operations by foreign actors. Financial safeguards for cyber-related health crises should be established, and accountability frameworks for private sector actors in health tech must be created. Incentivizing resilience investments through public-private partnerships and monitoring economic impacts of cyber health events, combined with targeted regulatory pressure, can improve cybersecurity posture and recovery planning. A key element would require major medical suppliers to report cyber vulnerabilities to HHS's Health Sector Cybersecurity Coordination Center (HC3). Vendors should also provide a software bill of materials for connected medical devices regulated by the Food and

Drug Administration (FDA). The Federal Trade Commission (FTC) should oversee a minimum cybersecurity framework for healthcare technology providers, with penalties for negligence that leads to patient harm or service interruptions. Finally, to encourage proactive resilience, CISA's Joint Cyber Defense Collaborative (JCDC) should expand to include healthcare-specific working groups. A public-private bond program, funded by vendors and government agencies, could help finance cybersecurity modernization in smaller hospitals and critical medical logistics hubs.

Cyber insurance, intended as a soft regulator, has fallen short of strengthening cyber defenses. Policies often lack standardization, fail to incentivize security improvements, and discourage transparency due to fears of premium hikes or denial of coverage (Adriko and Nurse 2024a). Claims may be denied if attacks are deemed "warlike" or nation-state actions (Wolff 2024). Some cybercriminals specifically target insured entities to increase ransom payment success. Regular review of cyber insurance policies and state support for uncovered infrastructure is crucial as threats evolve. Incident classification should account for physical, financial, psychological, and societal harms, including impacts on dignity and economic security, to better inform response and resilience planning.

Taken together, these measures extend health security theory into the digital domain. They recognize that ransomware simultaneously undermines the individual, the community, and the nation. By embedding healthcare infrastructure within the national security apparatus—through designation, funding conditions, emergency protocols, and harm-based accountability—the U.S. can move from reactive containment to a coherent cyber health security strategy.

CONCLUSION

Cybersecurity is inseparable from national security. The U.S. faces challenges in defending against foreign actors deploying cyber capabilities for destruction, disruption, and malicious influence. Cyber threats intensify, posing risks to critical infrastructure, resilience, and individual and community well-being. Adversarial states and cybercriminals increasingly exploit healthcare vulnerabilities to gain strategic and psychological leverage. To project national power in cyberspace, the U.S. must adapt to changing circumstances, ensure public support for a strategy combining resilience and preparedness, and deterrence by denial and accountability measures. A collective defense of healthcare, spanning federal agencies, private vendors, and citizens, should be embedded within a coherent cyber health security strategy. This way, cybersecurity principles can be integrated with public health goals, ensuring comprehensive protection against cyber threats that disrupt critical healthcare services, endangering patient safety, data integrity, and national resilience.

ABOUT THE AUTHORS

Pavlina Pavlova is a policy expert specializing in international cybersecurity and transnational cybercrime. She has over a decade of experience in technology, governance, security, and human rights across civil society and national, regional, and international institutions, including the United Nations (UN), the Organization for Security and Cooperation in Europe (OSCE), and the European Parliament. Pavlova has been at the forefront of stakeholder engagement in UN negotiations on responsible state behavior in cyberspace and on the Convention against Cybercrime, and she coordinates the Cybercrime Working Group at the Alliance of NGOs on Crime Prevention and Criminal Justice, advancing stakeholder input into treaty implementation. She was a fellow at New America and the Internet Society, and a research awardee at the University of California, Berkeley. Pavlova founded Critical Cyber, an impact-driven initiative that transforms frontline experiences of cyber incidents into improved resilience and policy innovation.

Dr. Craig Douglas Albert is a Professor of Political Science and Graduate Director of the PhD in Intelligence, Defense, and Cybersecurity Policy and the MA in Intelligence and Security Studies at Augusta University. He earned his PhD from the University of Connecticut in 2009. His research focuses on international security, cybersecurity policy, information warfare, propaganda, ethnic conflict, and political philosophy. Dr. Albert is widely published in leading journals such as The Cyber Defense Review, Intelligence and National Security, and Journal of Cyber Policy, among others. He has testified before the U.S. Congress and contributed expert commentary to major national and international media, including Fox News, CTVNews, and Forbes. He has presented at the Council on Foreign Relations and serves as a Distinguished Higher Education Ambassador for the organization, promoting the teaching of international relations and cybersecurity policy.

ACKNOWLEDGMENTS

The authors want to thank the editors and reviewers at CDR. The editorial team was an incredible asset to this manuscript getting published. Dr. Albert would also like to thank Chris Forde, a Ph.D. student in his program, for his assistance. The authors also benefited from and would like to thank the participants and organizers of Jack Voltaic 2025, held at the Army Cyber Institute at West Point.

REFERENCES

Abbou, Benyamine, Boris Kessel, Merav Ben Natan, Rinat Gabbay-Benziv, Dikla Dahan Shriki, Anna Ophir, Nimrod Goldschmid, Adi Klein, Ariel Roguin, and Mickey Dudkiewicz. 2024. "When All Computers Shut Down: The Clinical Impact of a Major Cyber-Attack on a General Hospital." *Frontiers in Digital Health* 6:1321485. https://doi.org/10.3389/fdgth.2024.1321485.

Abrams, Lawrence. 2025. "UnitedHealth Now Says 190 Million Impacted by 2024 Data Breach," January 26, 2025. https://www.bleepingcomputer.com/news/security/unitedhealth-now-says-190-million-impacted-by-2024-data-breach/.

Adriko, Rodney, and Jason R. C. Nurse. 2024a. "Cybersecurity, Cyber Insurance, and Small-to-Medium-sized Enterprises: A Systematic Review." *Information and Computer Security,* ISSN: 2056-4961. https://doi.org/10.1108/ICS-01-2024-0025.

Adriko, Rodney, and Jason R. C. Nurse. 2024b. "Does Cyber Insurance Promote Cyber Security Best Practice? An Analysis Based on Insurance Application Forms." *Digital Threats* (New York, NY, USA) 5, no. 3 (October). https://doi.org/10.1145/3676283.

Agrafiotis, Ioannis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. "A Taxonomy of Cyber Harms: Defining the Impacts of Cyber-Attacks and Understanding How They Propagate." *Journal of Cybersecurity* 4 (1): tyy006. https://doi.org/10.1093/cybsec/tyy006.

Ahmed, Zo. 2024. "Human Error to Blame in Ascension Data Breach That Impacted 5.6 Million Patients," December 27, 2024. https://www.techspot.com/news/106119-employee-error-blameascension-data-breach-impacting-56.html.

Albert, Craig Douglas, Amado Baez, and Joshua Rutland. 2021. "Human Security as Biosecurity: Reconceptualizing National Security Threats in the Time of COVID-19." *Politics and the Life Sciences* 40 (1): 83–105. https://doi.org/10.1017/pls.2021.1.

Alder, Steve. 2024a. "Ascension Ransomware Attack Affects 5.6 Million Patients." *The HIPAA Journal* (December 20, 2024). https://www.hipaajournal.com/ascension-cyberattack-2024/.

Alder, Steve. 2024b. "Black Basta Ransomware Group Targeting Healthcare Organizations." *The HIPAA Journal* (May 13, 2024). https://www.hipaajournal.com/black-basta-ransomware-healthcare/.

Alder, Steve. 2024c. "Center for Vein Restoration Data Breach Affects Almost 450,000 Individuals." *The HIPAA Journal* (December 11, 2024). https://www.hipaajournal.com/center-for-vein-restoration-data-breach/.

Alder, Steve. 2024d. "ConnectOnCall Announces 914K-Record Data Breach." *The HIPAA Journal* (December 16, 2024). https://www.hipaajournal.com/connectoncall-data-breach/.

Alder, Steve. 2025a. "McLaren Health Care Restores IT Systems Following Ransomware Attack." *The HIPAA Journal* (June 23, 2025). https://www.hipaajournal.com/mclaren-health-care-investigating-potential-cyberattack/.

Alder, Steve. 2025b. "UHG Increases Change Healthcare Data Breach Victim Count to 190 Million." *The HIPAA Journal* (November 17, 2025). https://www.hipaajournal.com/change-healthcare-responding-to-cyberattack/.

Aldis, William. 2008. "Health Security as a Public Health Concept: A Critical Analysis." *Health Policy and Planning* 23 (6): 369–375. https://doi.org/10.1093/heapol/czn030.

American Hospital Association. 2025. "Report: Health care had most reported cyberthreats in 2024," May 12, 2025. https://www.aha.org/news/headline/2025-05-12-report-health-care-had-most-reported-cyberthreats-2024.

Arghire, Ionut. 2024. "5.6 Million Impacted by Ransomware Attack on Healthcare Giant Ascension," December 23, 2024. https://www.securityweek.com/5-6-million-impacted-by-ransomware-attack-on-healthcare-giant-ascension/.

Bae, Sunha. 2025. "Deterrence Under Pressure: Sustaining U.S.–ROK Cyber Cooperation Against North Korea," April 1, 2025. https://www.csis.org/analysis/deterrence-under-pressure-sustaining-us-rok-cyber-cooperation-against-north-korea.

BBC News. 2024. "NHS England Confirm Patient Data Stolen in Cyber Attack," June 24, 2024. https://www.bbc.com/news/articles/c9777v4m8zdo.

Bleih, Ady. 2025. *Ransomware Annual Report 2024.* Technical report. January 13, 2025. https://cyberint.com/blog/research/ransomware-annual-report-2024.

BreachSense. n.d. *INC Ransom. BreachSense*. Accessed February 9, 2025. https://www.breachsense.com/breaches/conceptions-repro-data-breach/.

Brown, Garrett Wallace, Gemma Bridge, Jessica Martini, Jimyong Um, Owain D. Williams, Luc Bertrand Tsachoua Choupe, Natalie Rhodes, Zheng Jie Marc Ho, Stella Chungong, and Nirmal Kandel. 2022. "The Role of Health Systems for Health Security: A Scoping Review Revealing the Need for Improved Conceptual and Practical Linkages." *Globalization and Health* 18 (51). https://doi.org/10.1186/s12992-022-00840-6.

Business Insider. 2025. "Conceptions Reproductive Associates of Colorado Data Breach under Investigation by Levi & Korsinsky," January 13, 2025. https://markets.businessinsider.com/news/stocks/conceptions-reproductive-associates-of-colorado-data-breach-under-investigation-by-levi-korsinsky-1034222342.

Caballero-Anthony, Mely. 2006. "Combating Infectious Diseases in East Asia: Securitization and Global Public Goods for Health and Human Security." *Journal of International Affairs* 59 (2): 105–127. https://www.jstor.org/stable/24358429.

Carr, Deborah, Elizabeth Heger Boyle, Benjamin Cornwell, Shelley Correll, Robert Crosnoe, Jeremy Freese, and Mary C. Waters, eds. 2018. *The Art and Science of Social Research.* New York: W. W. Norton & Company.

Centers for Disease Control and Prevention. 2024. *Global Health Security. CDC*. https://www.cdc.gov/global-health/topics-programs/global-health-security.html.

Change Healthcare. 2024. "Notice of Data Breach," June 20, 2024. https://www.pchne.org/wp-content/uploads/2024/09/Change-Healthcare-HIPAA-Website-Substitute-Notice.pdf.

CIRCIA (Federal Register). 2024. *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA): Proposed Rule.* https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.

CISA (Cybersecurity and Infrastructure Security Agency). 2022. *AA22-057A: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices.* Cybersecurity Advisory, August 9, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-057a.

CISA (Cybersecurity and Infrastructure Security Agency). 2024a. "#StopRansomware: Black Basta," November 8, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a.

CISA (Cybersecurity and Infrastructure Security Agency). 2024b. *National Security Memorandum on Critical Infrastructure Security and Resilience.* CISA. https://www.cisa.gov/national-security-memorandum-critical-infrastructure-security-and-resilience.

CISA (Cybersecurity and Infrastructure Security Agency). 2024c. "Secure-By-Design," October 27, 2024. https://www.cisa.gov/resources-tools/resources/secure-by-design.

CISA (Cybersecurity and Infrastructure Security Agency). n.d.(a). *Cross-Sector Cybersecurity Performance Goals.* CISA. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

CISA (Cybersecurity and Infrastructure Security Agency). n.d.(b). *Healthcare and Public Health Sector.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/healthcare-and-public-health-sector.

CISA and FBI (Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation). 2022. *CISA and FBI Publish Advisory to Protect Organizations from Destructive Malware Used in Ukraine.* Online news release, February. https://www.cisa.gov/news-events/news/cisa-and-fbi-publish-advisory-protect-organizations-destructive-malware-used-ukraine.

CISA, FBI and HHS (Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, and U.S. Department of Health and Human Services). 2020. *Ransomware Activity Targeting the Healthcare and Public Health Sector (AA20-302A). Joint Cybersecurity Advisory*, November 2, 2020. https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-302a.

CMIT Solutions. n.d. *Another Day, Another Data Breach.* CMIT Solutions Blog. Accessed February 9, 2025. https://cmitsolutions.com/blog/another-week-another-healthcare-breach/.

Culhane, Mallory. 2025. "Colorado Fertility Clinic Sued Over Data Breach Affecting 80,000," January 3, 2025. https://news.bloomberglaw.com/litigation/colorado-fertility-clinic-sued-over-data-breach-affecting-80-000.

CyberPeace Institute. 2022. *Compendium of Multistakeholder Perspectives. CyberPeace Institute*, July. https://cyberpeaceinstitute.org/publications/compendium-of-multistakeholder-perspectives/.

CyberPeace Institute. 2024. *Harm Methodology.* https://cyberpeaceinstitute.org/harm-methodology/.

Davies, Sara E. 2008. *Global Politics of Health.* Cambridge: Polity Press.

Dudley, Renee. 2022. "Why It's Hard to Sanction Ransomware Groups," May 23, 2022. https://www.propublica.org/article/ransomware-russia-ukraine-sanctions-ofac-conti.

Elbe, Stefan. 2010. *Security and Global Health.* Cambridge: Polity Press.

Executive Order 14117 (Executive Office of the President). 2024. *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern.* Federal Register 89:14615 (March 1, 2024). https://www.federalregister.gov/documents/2024/03/01/2024-04434/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related-data.

Fidler, David P. 2003. "Public Health and National Security in the Global Age: Infectious Diseases, Bioterrorism, and Realpolitik." *The George Washington International Law Review* 35 (4): 787–856. https://www.repository.law.indiana.edu/facpub/416.

Fischerkeller, Michael P., Emily O. Goldman, and Richard J. Harknett. 2022. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford: Oxford University Press.

Flashpoint. 2024. "From Origins to Operations: Understanding Black Basta Ransomware," May 28, 2024. https://flashpoint.io/blog/understanding-black-basta-ransomware/.

Fox, Andrea. 2023. "Warning: Cybercriminals Have More Weapons with AI," July 18, 2023. https://www.healthcareitnews.com/news/warning-cybercriminals-have-more-weapons-ai.

Freedman, Linn Foster. 2025. "Ascension Health Notifying 5.6 Million of Data Breach" (January 2, 2025). https://natlawreview.com/article/ascension-health-notifying-56-million-data-breach.

Ghanbari, Hadi, and Kari Koskinen. 2024. "When Data Breach Hits a Psychotherapy Clinic: The Vastaamo Case." *Journal of Information Technology Teaching Cases,* https://doi.org/10.1177/20438869241258235.

Greig, Jonathan. 2024. "Nearly 6 Million People Were Impacted by Ransomware Attack on Ascension Health," December 20, 2024. https://therecord.media/nearly-six-million-affected-ransomware.

Guttieri, Karen. 2025. "Fighting Through Disruption: Reframing Cyber Resilience for Power Projection and Strategic Credibility." *The Cyber Defense Review* 10 (1): 93–114. https://doi.org/10.55682/cdr/egvf-mkys.

Hanrieder, Tine, and Christian Kreuder-Sonnen. 2014. "WHO Decides on the Exception? Securitization and Emergency Governance in Global Health." *Security Dialogue* 45 (4): 331–348. https://doi.org/10.1177/0967010614535833%0A.

Health-ISAC. 2025. *2025 Health Sector Cyber Threat Landscape.* Technical report. February 2025. https://health-isac.org/wp-content/uploads/Health-ISAC_2025-Annual-Threat-Report.pdf.

HHS (U.S. Department of Health and Human Services). 2022. "Healthcare System Cybersecurity: Readiness and Response Considerations." https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf.

HHS (U.S. Department of Health and Human Services). 2023. *Breach Notification Rule – HIPAA for Professionals.* https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

Horne, Si, Gareth Mott, and Jamie MacColl. 2024. "Ransomware: A Life and Death Form of Cybercrime," June 25, 2024. https://rusi.org/explore-our-research/publications/commentary/ransomware-life-and-death-form-cybercrime.

Krebs, Brian R. 2022. "Conti's Ransomware Toll on the Healthcare Industry," April 18, 2022. https://krebsonsecurity.com/2022/04/contis-ransomware-toll-on-the-healthcare-industry/.

Landi, Heather. 2024. "US indicts North Korean hacker for leading ransomware attacks against hospitals," July 30, 2024. https://www.fiercehealthcare.com/health-tech/us-indicts-north-korean-hacker-leading-2022-ransomware-attacks-against-hospitals.

MacColl, Jamie, Pia Hüsch, Gareth Mott, James Sullivan, Jason R. C. Nurse, Sarah Turner, and Nandita Pattnaik. 2024. "Ransomware: Victim Insights on Harms to Individuals, Organisations and Society," January 16, 2024. https://static.rusi.org/ransomware-harms-op-january-2024.pdf.

Malik, Sadia Mariam, Amy Barlow, and Benjamin Johnson. 2021. "Reconceptualising Health Security in Post-COVID-19 World." *BMJ Global Health* 6 (7): e006520. https://doi.org/10.1136/bmjgh-2021-006520.

Mandru, S. 2024. "Privileged Access Management and Regulatory Compliance." *J Artif Intell Mach Learn & Data Sci* 2 (2): 728–732. https://doi.org/10.51219/JAIMLD/Srikanth-mandru/182.

Martin, Alexander. 2023. "Ransomware Gang Posts Breast Cancer Patients' Clinical Photographs," March 6, 2023. https://therecord.media/ransomware-lehigh-valley-alphv-black-cat.

Martin, Alexander. *Ransomware Gang Leaks Stolen Scottish Healthcare Patient Data in Extortion Bid.* Online news article on *The Record*, March 29, 2024. https://therecord.media/healthcare-ransomware-data-breach-nhs-scotland.

McConomy, Bryan C., and Dennis E. Leber. 2022. "Cybersecurity in Healthcare." In *Clinical Informatics Study Guide,* edited by John T. Finnell and Brian E. Dixon, 241–253. Springer International Publishing. https://doi.org/10.1007/978-3-030-86976-8_17.

McInnes, Colin, and Kelley Lee. 2006. "Health, Security and Foreign Policy." *Review of International Studies* 32 (1): 5–23. https://doi.org/10.1017/S0260210506006905.

Microsoft. 2022. *Microsoft Digital Defense Report 2022.* Microsoft Corporation. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/microsoft-digital-defense-report-2022.pdf?culture=en-us&country=us.

Mitra, Aritra, Saikat Gochhait, Ahmed J. Obaid, and Mohammed Ayad Alkhafaji. 2023. "A Strategic Data Protection Plan for the Healthcare Industry–A Review." In *2023 8th International Conference on Communication and Electronics Systems (ICCES),* 1784–1788. IEEE. https://doi.org/10.1109/ICCES56750.2023.10149916.

Moody, Rebecca. 2025. *Healthcare Ransomware Roundup: H1 2025 Stats on Attacks, Ransoms, and Data Breaches.* Comparitech, July 17, 2025. https://www.comparitech.com/news/healthcare-ransomware-roundup-h1-2025/.

NCC Group. 2025. *2024 Breaks Records with Highest-Ever Amount of Ransomware Attacks as Cybercriminals Target Critical Infrastructure. Annual Cyber Threat Monitor Report 2024*, January 31, 2025. https://www.nccgroup.com/newsroom/ncc-group-releases-annual-cyber-threat-monitor-report-2024/.

Nershi, Karen, and Shelby Grossman. 2023. *Assessing the Political Motivations behind Ransomware Attacks,* July 12, 2023. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4507111.

NIST (National Institute of Standards and Technology). 2019. *Cyber Resilience: Glossary and Framework.* NIST Computer Security Resource Center. https://csrc.nist.gov/glossary/term/cyber_resilience.

Office of Information Security. 2022. *HC3 Threat Profile: Evil Corp.* Report No. 202208291500, U.S. Department of Health and Human Services, August 29, 2022. https://www.hhs.gov/sites/default/files/evil-corp-threat-profile.pdf.

Ortega, Bruno. 2024. "Conceptions Reproductive Associates of Colorado, Inc. Data Breach Investigation." M&R LLP, December 19, 2024. https://classlawdc.com/2024/12/19/conceptions-reproductive-associates-of-colorado-inc-data-breach-investigation/.

Oz, Harun, Ahmet Aris, Albert Levi, and A. Selcuk Uluagac. 2022. "A Survey on Ransomware: Evolution, Taxonomy, and Defense Solutions." *ACM Computing Surveys* 54 (11s): 1–37. https://doi.org/10.1145/3514229.

Pattnaik, Nandita, Jason R. C. Nurse, Sarah Turner, Gareth Mott, Jamie MacColl, Pia Huesch, and James Sullivan. 2023. "It's More Than Just Money: The Real-World Harms from Ransomware Attacks." In *Proceedings of the International Symposium on Human Aspects of Information Security and Assurance,* 261–274.

Pavlova, Pavlina. 2024. "Gendered Harms of Data Weaponization: Historical Patterns, New Battlefields, and the Implications for Democracy and National Security," November 14, 2024. https://www.newamerica.org/future-security/reports/gendered-harms-of-data-weaponization/.

Pavlova, Pavlina. 2025. *Enhancing Cyber Resilience for Equitable Healthcare: Analysis of Cyberattacks Targeting Sexual and Reproductive Facilities and Services.* UC Berkeley Center for Long-Term Cybersecurity, October 2025. https://cltc.berkeley.edu/publication/enhancing-cyber-resilience-for-equitable-sexual-reproductive-healthcare/.

Peintener, Tiffany. 2024. "Federman & Sherwood Investigates Conceptions Reproductive Associates of Colorado for Data Breach," December 18, 2024. https://www.federmanlaw.com/blog/federman-sherwood-investigates-conceptions-reproductive-associates-of-colorado-for-data-breach/.

Peterson, Susan. 2002. "Epidemic Disease and National Security." *Security Studies* 12 (2): 43–81. https://doi.org/10.1080/09636410212120009.

Pradhan, Rachana, and Kate Wells. 2024. "Cyberattack Led to Harrowing Lapses at Ascension Hospitals, Clinicians Say," June 19, 2024. https://www.npr.org/2024/06/19/nx-s1-5010219/ascension-hospital-ransomware-attack-care-lapses.

Ribeiro, Anna. 2024. "DoJ Audit Finds CISA Faces Challenges in Cyber Threat Information Sharing, as Participation Hits Record Low," October 1, 2024. https://industrialcyber.co/reports/doj-audit-finds-cisa-faces-challenges-in-cyber-threat-information-sharing-as-participation-hits-record-low/.

Rushton, Simon. 2011. "Global Health Security: Security for Whom? Security from What?" *Political Studies* 59 (4): 779–796. https://doi.org/10.1111/j.1467-9248.2011.00919.x.

Saltarella, Marco, Giuseppe Desolda, Rosa Lanzilotti, and Vita Santa Barletta. 2024. "Translating Privacy Design Principles into Human-Centered Software Lifecycle: A Literature Review." *International Journal of Human–Computer Interaction* 40 (17): 4465–4483. https://doi.org/10.1080/10447318.2023.2219964.

SBS News. 2024. *Albanese Says MediSecure Hack "Very Significant" and Warns It Won't Be the Last.* Online news article, July 19, 2024. https://www.sbs.com.au/news/article/albanese-says-medisecure-hack-very-significant-and-warns-it-wont-be-the-last/apqpt2iqr.

Šehović, Annamarie B. 2020. "Towards a New Definition of Health Security: A Three-Part Rationale for the Twenty-First Century." *Global Public Health* 15 (1): 1–12. https://doi.org/10.1080/17441692.2019.1634119.

Shamus, Kristen. 2024. "Ascension Nurse: Ransomware Attack Makes Caring for Hospital Patients 'So, So Dangerous.'," May 21, 2024. https://www.freep.com/story/news/health/2024/05/21/ascensionhospital-hack-ransomware-cyber-attack/73776557007/.

Stoeva, Preslava. 2020. "Dimensions of Health Security: A Conceptual Analysis." *Global Challenges* 4 (10). https://doi.org/10.1002/gch2.201700003.

Strauss Borrelli PLLC. 2024. "Conceptions Reproductive Associates of Colorado Data Breach Investigation," December 18, 2024. https://straussborrelli.com/2024/12/18/conceptions-reproductive-associates-of-colorado-data-breach-investigation/.

The White House Office of the Press Secretary. 2013. *Presidential Policy Directive–Critical Infrastructure Security and Resilience.* The White House, February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

U.S. Congress. 2015. *Cybersecurity Information Sharing Act of 2015.* Public Law 114–113, Div. N, Title I.

U.S. Congress. 2022. *Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).* Public Law 117–103, Division Y.

U.S. Department of the Treasury. 2019. *Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware.* Press Release, December 5, 2019. https://home.treasury.gov/news/press-releases/sm845.

U.S. Department of the Treasury. 2024. "United States, Australia, and the United Kingdom Sanction Russian Cyber Actor Responsible for the Medibank Hack," January 23, 2024. https://home.treasury.gov/news/press-releases/jy2041.

Vasquez, Christian. 2023. "Ukraine Information Sharing a Model for Countering China, Top Cyber Official Says," June 12, 2023. https://cyberscoop.com/information-sharing-china-threat/.

Vectra AI. n.d. *INC Ransom.* Vectra AI Threat Actor Profile. https://www.vectra.ai/modern-attack/threat-actors/inc-ransom.

Vogel, Susanna. 2024. "Ascension Reduces Operating Loss as It Rebounds from Cyberattack," December 4, 2024. https://www.cybersecuritydive.com/news/ascension-reduces-operating-cyber-attack/734580/.

Wenham, Clare. 2019. "The Oversecuritization of Global Health: Changing the Terms of Debate." *International Affairs* 95 (5): 1093–1110. https://doi.org/10.1093/ia/iiz170.

WHO (World Health Organization). 2018. *Essential Public Health Functions, Health Systems, and Health Security: Developing Conceptual Clarity and a WHO Roadmap for Action.* World Health Organization. https://iris.who.int/server/api/core/bitstreams/398d7efa-cd89-4724-9784-f59743f38a8d/content.

WHO (World Health Organization). 2024. "WHO Releases First Ever Guidance on Health Practitioner Regulation," September 19, 2024. https://www.who.int/news/item/19-09-2024-20240920-health-practitioner-regulation.

Wolff, Josephine. 2024. *Insurers Will Help Define the Threshold for Cyberwar.* BindingHook, July 4, 2024. https://bindinghook.com/insurers-will-help-define-the-threshold-for-cyberwar/.

Wong, Owen. 2024. "Cyberwarfare: The 'Pink Tax' of Hacking," April 1, 2024. https://www.queensu.ca/cidp/publications/policy-briefs/cyberwarfare-pink-tax-hacking.

Wulff, Katharine, Darrin Donato, and Nicole Lurie. 2015. "What Is Health Resilience and How Can We Build It?" *Annual Review of Public Health* 36:361–374. https://doi.org/10.1146/annurev-publhealth-031914-122829.

Zegart, Amy. 2022. "The Weapon the West Used Against Putin," March 5, 2022. https://www.theatlantic.com/ideas/archive/2022/03/russia-ukraine-invasion-classified-intelligence/626557/.

Received 17 March 2025; Revised 30 October 2025; Accepted 5 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 69-78
https://doi.org/10.55682/cdr/m9d9-5ee5

PROFESSIONAL COMMENTARY

Autonomous Vehicles in Critical Infrastructure: Technologies, Vulnerabilities, and Implications

Donna Artusy

Autonomous vehicles (AVs) are quickly emerging as a critical component of the Transportation Systems Sector (TSS), one of the essential infrastructure sectors designated by the Department of Homeland Security (DHS). While autonomy is not a new concept, advancements in artificial intelligence (AI), real-time data processing, and sensor fusion have accelerated the deployment of AV technology in both military and commercial civilian sectors. These technologies enable AVs to operate with varying levels of autonomy but also introduce significant cybersecurity, legal, and ethical challenges. As AV integration into critical infrastructure scales and military reliance on interconnected autonomous systems grows, ensuring cyber and operational resilience becomes a national security imperative to guard against cyber-physical threats. This article explores the technological foundation of AVs, their military and commercial applications, and the cybersecurity risks impeding safe deployment. We examine specific frameworks, such as the commercial SAE autonomy levels (1-5) and military adaptations like the Robotic Combat Vehicle (RCV) program, alongside key cybersecurity threats, including remote hacking, GPS spoofing, and Denial-of-Service (DoS) attacks. This analysis highlights the immense potential and inherent vulnerabilities of AV technology as it becomes more deeply integrated into civilian and military systems. The paper concludes by addressing critical cybersecurity measures, including strong encryption and AI model training, to mitigate these risks and enhance AV security in commercial and defense applications.

Keywords: critical infrastructure, autonomous vehicles, autonomy level, transportation systems sector, cybersecurity

INTRODUCTION

Autonomous vehicles (AVs) are integral components of the Transportation Systems Sector (TSS)-one of the Department of Homeland Security's (DHS) sixteen critical infrastructure sectors (CISA 2022). TSS consists of various modes of transportation essential for the movement of both people and goods, and autonomous ground vehicles are now among them. Although the concept of autonomously operated vehicles is not novel per se, their commercial applications and implementation into military systems have introduced both clear efficiencies and significant vulnerabilities. AVs include a number of complex and robust integrations of artificial intelligence (AI), real-time data processing, and geospatial mapping. These foundational technologies, however, expand the attack surface and introduce new cybersecurity threats. Algorithmic limitations and a growing dependence on existing infrastructure become critical vulnerabilities. Furthermore, the deployment of AVs raises novel legal and ethical concerns.

As AVs become increasingly embedded within both civilian and military transportation networks, they function not only as vehicles but as cyber-physical platforms deeply dependent on the integrity and reliability of other critical infrastructure systems and data that support their operation. This reliance creates strategic vulnerabilities, exposed to the disruption of digital enablers such as Global Positioning System (GPS), mobile 5G communications, and cloud-based control architectures. Threats can directly impair mobility operations, logistical continuity, and broader defense readiness. Cybersecurity and operational resilience are therefore not ancillary concerns: they are foundational requirements for the secure deployment of AVs within national infrastructure.

Technological advances are double-edged swords. In this particular case, the advent of autonomous technology in both military and civilian settings presents many potential benefits along with new vectors of vulnerability ripe for exploitation by U.S. adversaries (Guttieri 2025, 95). AVs expand the national cyber-physical attack surface by linking AI-driven decision-making systems, sensors, and cloud-connected infrastructure, thereby intertwining transportation with other critical infrastructure sectors (National Counterintelligence and Security Center 2022). Because AVs rely on the continuous exchange of data and constant connectivity, a 'successful' cyberattack could cascade across logistics and emergency services, underscoring the need to integrate AV cybersecurity into broader national resilience and infrastructure protection frameworks (NHTSA, n.d.). Accordingly, it would make logical sense to conceptualize cyber resilience as integral to a sustained national strategic posture (Demchak 2021). This framework of considering cyber resilience will help position the U.S. in a more strategically favorable position on the world stage, where progressively sophisticated cyber threats are constantly emerging.

This article provides a high-level overview of the technologies underpinning AV systems and examines their use in commercial and military contexts. The article then analyzes the impact

of AVs on critical infrastructure and discusses key cybersecurity vulnerabilities, concluding with a high-level snapshot of the legal and policy landscapes for the technology.

Levels of Autonomy

The Society of Automotive Engineers (SAE) provides a helpful standardized taxonomy of levels of vehicle automation. According to this framework, Levels 1 and 2 necessitate driver assistance features and are not classified as fully autonomous systems. Levels 3-5 represent higher levels of automation that culminate with full autonomy. Vehicles classified at either Level 4 or 5 are capable of operating without human intervention when automated systems are engaged; however, Level 4 systems still allow for human oversight in specific conditions (SAE 2021). Commercially available technologies such as Google's Waymo cars are currently considered Level 4: they are fully autonomous in the sense that humans are not directly driving the vehicle, but can still provide guidance for the vehicle in new or unknown situations (Ackerman 2021). As of this writing, Level 5 autonomy—representing full automation without any human intervention in all driving conditions—has not yet been achieved.

Technologies Used in Autonomous Vehicles

AVs integrate a diverse range of technologies and computational systems to operate with varying levels of autonomy. These technologies typically include AI, high-definition real-time geospatial mapping, advanced perception systems such as LiDAR (Light Detection and Ranging), radar, and Vehicle-to-Everything (V2X) communication. Most AVs employ a combination of LiDAR, radar, GPS, cameras, high-definition maps (including Simultaneous Localization and Mapping (SLAM)), sensor fusion, and Inertial Navigation Systems (INS) to accurately perceive their surroundings, determine their position, and navigate within their environment. However, certain AV systems prioritize camera-based perception and AI-driven computer vision over LiDAR, relying on deep learning algorithms and real-time image processing to interpret the driving environment and make navigation decisions.

Each of these technologies contributes to the vehicle's capacity for operating with greater levels of autonomy and accuracy, as well as its ability to adapt to unexpected environmental changes. By integrating AI, advanced sensor systems, high-definition mapping, and real-time data processing, AVs can more effectively perceive, interpret, and react to dynamic road conditions. Consequently, this causes a reduction in reliance on human intervention and increases operational reliability. AI serves as the basis for the 'intelligence' of AVs, leveraging subfields of AI, including machine learning (ML), neural networks, and generative AI (genAI) to process sensory data and make real-time driving decisions. AI significantly improves the vehicle's ability to predict and react to dynamic road conditions (Bojarski et al. 2016). LiDAR enhances both object detection and depth perception, creating a high-resolution 3-dimensional model of the AV's surroundings. This is critical for obstacle avoidance and precise

navigation in complex, evolving environments (Shan and Englot 2018). Radar can add an additional layer of perception, particularly in adverse weather conditions where LiDAR and cameras are less effective.

GPS and INS work together to maintain accurate vehicle positioning: GPS provides more precise global location data, while INS compensates for GPS signal disruptions by tracking motion and orientation through accelerometers and gyroscopes (Groves 2013). SLAM algorithms allow AVs to build and refine maps of their environment in real-time, improving localization and adaptation to previously unknown geographies (Durrant-Whyte and Bailey 2006). Sensor fusion rapidly combines and processes incoming sensor data to improve the accuracy, reliability, and robustness of the autonomous system. This helps AVs detect obstacles, road conditions, pedestrians, and infrastructure signals more accurately than relying on a single sensor modality. Lastly, V2X communication enhances vehicle decision-making by enabling AVs to exchange real-time data with other vehicles and infrastructure. This improves efficiency and safety through cooperative maneuvering and collision avoidance (Papadimitratos et al. 2009). The collective use of all of these technologies reduces the need for human intervention, bringing AVs closer to achieving full autonomy.

MILITARY AND COMMERCIAL APPLICATIONS OF AUTONOMOUS VEHICLES

While the commercial development of AVs has garnered public attention for decades, the U.S. Army has simultaneously pursued its own applications through various initiatives. Autonomous combat vehicles offer the potential to reduce casualties on the battlefield, where over 50% of casualties historically occur during the transport and delivery of supplies in combat zones (Muller 2019). The Army's initial endeavor focused on the "leader-follower" robotic vehicle deployment program, which utilized AV technologies to enhance force protection and sustainment. In March 2023, the "leader-follower" program was replaced by the Autonomous Vehicle Transport System, which aims to expand these autonomously driven capabilities further (Luckenbaugh 2023).

A few months later, the Army shifted its focus to leveraging commercial autonomous driving technologies for implementation in convoy operations (Eversden 2023). The shift was driven by a desire to accelerate the adoption of emerging capabilities readily available in the commercial sector. This new direction included a prototyping competition managed by the Defense Innovation Unit (DIU)—the Ground Expeditionary Autonomy Retrofit Systems (GEARS). GEARS sought vendors to equip existing military vehicles with reliable unmanned operational capabilities (Harper 2023). The program's goal was to integrate both hardware and software to enable autonomous functions, including convoy operations and navigation, while maintaining an open architecture to facilitate future upgrades.

The Army is also developing a Robotic Combat Vehicle (RCV) program as part of its "Next Generation Combat Vehicle" series, designed to function directly in combat scenarios (Feickert 2025). This ongoing program aims to develop a family of unmanned, combat-ready vehicles that can operate collaboratively with manned vehicles. The RCV's mission set has been expanded to include reconnaissance, execution of complex tactical maneuvers, and direct self-defense when attacked. As of October 2024, the Army planned to select one vendor from a 2023 Army Request for Prototype Proposal (RPP) to proceed with the platform prototype design and build phase of the RCV program (John 2023). Although current RCVs incorporate advanced sensors, they remain dependent on soldiers for operation; testing in 2024 revealed that one control vehicle with a crew of five soldiers was necessary for the deployment of two RCVs. The progression toward greater autonomy will be heavily influenced by funding considerations and how well RCVs perform in battle-simulated environments. While the aforementioned SAE standards apply to commercial automotive applications, it is reasonable to infer from publicly available information that the RCVs currently operate at an equivalent of approximately Level 3 autonomy.

CRITICAL INFRASTRUCTURE IMPLICATIONS

AVs have become more embedded within critical infrastructure due to their reliance on and integration with interconnected cyber-physical systems that underpin modern transportation networks. The security of such networks extends well beyond individual vehicles, encompassing mobile communication protocols such as 5G, GPS navigation systems, cloud-based command and control systems, and the physical infrastructure that supports these technologies. Such dependencies magnify the potential negative impact of cyber and physical disruptions, which can cascade through many sectors, thereby threatening broader national resilience. The breadth of this exposure necessitates robust risk management and mitigation strategies, combined with cross-sector coordination to safeguard these interdependent systems from increasingly sophisticated threats. Effective risk management for AVs within critical infrastructure involves continuous threat identification, timely vulnerability assessments, and implementation of layered cybersecurity controls. Collaboration across interdependent critical infrastructure sectors will proactively mitigate emerging threats, ensure reliability, and lead to increased resilience.

In military operations, AVs play critical roles in autonomous logistics, reconnaissance, and force mobility. To simultaneously reduce personnel risk while also enhancing operational flexibility and responsiveness, the resilience of these platforms is vital. Disruptions may impair mission-critical capabilities and strategic mobility. Addressing these vulnerabilities requires adherence to established cybersecurity frameworks from the National Institute of Standards and Technology (NIST), such as NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations* (Joint Task Force 2018), and NIST SP 800-82 Revision

3, *Guide to Operational Technology (OT) Security* (Stouffer et al. 2023), alongside integrated policies that unify civilian and military cybersecurity efforts. This comprehensive approach helps to ensure that the deployment of AVs strengthens, rather than jeopardizes, national security objectives across both civilian and defense domains.

CYBERSECURITY VULNERABILITIES AND MITIGATION STRATEGIES

As has been an evident trend over the last decade, cybersecurity attacks are becoming increasingly prevalent, and malicious actors are becoming more sophisticated. AVs are not immune to such attacks. Although autonomous technologies are not yet widespread and remain limited to select commercial applications, their expansion to buses and other public transportation will increase the vulnerabilities of related critical infrastructure. Understanding potential threat vectors will significantly mitigate potential damages and threats to human life, while also raising awareness of legal liability issues. Some of the potential vulnerabilities for both commercial and subsequently military AVs include data breaches and privacy concerns, remote hacking and unauthorized access, GPS spoofing and sensor manipulation, and Denial of Service (DoS) attacks. Although each of these present significant potential harm to users and those around them, mitigating measures can be taken to reduce such risks considerably.

Data Breach and Privacy Considerations

There are clear legal concerns around AVs, including liability, data breaches, and potential exposure of user data. This particular topic is broad and has been extensively examined in academic analyses, articles, and books. To remain within the scope of this article, the analysis here will provide a high-level overview rather than engaging in an in-depth legal examination. In constantly evolving and multi-faceted environments with AVs, the information security considerations impact not only the integrity of data, but also the physical security of the passengers and those around them. Consequently, robust security practices are critical to both informational and physical safety by securing the information and data. A primary security objective is to maintain the confidentiality, integrity, and availability of data.

AVs may generate and collect substantial amounts of data during operation: while not an exhaustive list, this may include real-time and geolocation data, synced device data, and driving habits. AVs are also vulnerable to malware infections via over-the-air software updates. Mitigating strategies can be implemented at several levels, including multi-layer authentication, intrusion detection systems (IDS), robust encryption practices, multi-factor authentication, and AI model training to ensure the security of deep learning models. Typically, AVs utilize Advanced Encryption Standard (AES) 256 and secure communication protocols, including Transport Layer Security (TLS), to protect data transmitted between the vehicle, infrastructure, and cloud environments (Rossi, Tiffiny 2019). AVs increasingly incorporate generative AI (genAI) models to enhance decision-making, communication with operators, and further

advance autonomous capabilities. Such models rely on a vast amount of training data to 'learn' and subsequently make effective decisions during the deployment of the technology (Muller 2024). Ensuring that genAI models are trained on high-quality and integrity-verified data provides safeguards for reducing biases, improving real-world adaptability, and mitigating safety risks associated with unpredictable driving conditions. Curated datasets further help AVs respond accurately to edge cases, diverse environmental conditions, and complex scenarios, ultimately enhancing reliability and trust in autonomous systems.

Remote Hacking, Unauthorized Access, GPS Spoofing, and Denial of Service

Remote hacking involves exploiting security vulnerabilities in an AV's communication networks, such as the Controller Area Network (CAN), to gain unauthorized access and manipulate critical vehicle functions, including steering, braking, and acceleration (Adly et al. 2023). Malicious actors may also exploit vulnerabilities in internet-to-vehicle commands. This was evidenced by a Kia vulnerability exposed in 2024, where attackers could send unauthorized commands to other vehicles simply by substituting a victim's identifier (e.g. an email address) into an Application Programming Interface (API) request, which the backend system failed to authenticate before routing the command to the victim's vehicle (Greenberg 2024).

When cars rely on GPS for navigation, sending false location data to an AV can be detrimental: inaccurate or manipulated location data compromises the vehicle's ability to navigate correctly. Not only is this disruptive and potentially harmful to the passengers in the AV, it can also disrupt the integrity of vehicle-to-vehicle (V2V) communications, vehicle-to-network (V2N) communications (which enable AVs to connect to the cloud for navigation and real-time updates), and vehicle-to-pedestrian (V2P) communications which enable AVs to interact with pedestrians through mobile devices or sensors. Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks can target the AV's network bandwidth or processing capacity, potentially impacting all of these safety-critical services and functions. The degradation of the AV's ability to properly receive, interpret, or transmit data and interface with external systems can result in severe consequences (Durlik et al. 2024).

THE LEGAL AND POLICY LANDSCAPE

The proliferation of AVs introduces critical legal and policy challenges. Examining these implications is crucial for a comprehensive understanding of the emerging AV landscape.

Legal Liability Standards

At a high level, legal liabilities for AVs follow in part traditional paths of product liability, strict liability, negligence, and, of course, breach of contract. While software embedded in commercial vehicles is not new in itself, the autonomous component alters the nature of risks and may impact the legal framework of responsibilities. Increasing levels of autonomy seem

to necessitate a shift in this legal framework, but is that necessary? Proponents of change may argue that responsibility and control no longer stem directly from a human decision-maker, as in a traditional vehicle. Additionally, causation becomes more attenuated and removed with increasing levels of autonomy. Conversely, some legal scholars argue that traditional legal frameworks are sufficiently robust to resolve the liability question. Regardless of the type of human control technology, is it not still true that the car manufacturer is responsible for its platforms, including embedded technology (joint liability considerations aside)?

The courts are still grappling with the conundrum of how to address AVs as more cases come to the fore. Many such cases have settled out of court, removing the opportunity for courts to set precedent where applicable. This question will undoubtedly become more critical as the levels of autonomy in commercially available vehicles increase and the number of such vehicles in use proliferates.

Policy

At the policy level, although federal legislation regarding autonomous vehicles has been proposed, no such framework currently exists. There is no single federal law that explicitly regulates AVs, though the National Highway Traffic Safety Administration (NHTSA, n.d.) provides guidance for best practices around AV safety . Many states have adopted legislation attempting to address AVs but this mirrors the piecemeal state-by-state approach that is present in privacy laws today (Baker Donelson 2024).

NIST has provided guidance on the evolving topic, although it does not create a binding set of standards as of this writing. Several relevant frameworks apply to the technology within AVs, including the NIST Cybersecurity Framework (CSF), to help address cyber risk and vulnerability management for the technologies within the AVs. NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations* (NIST 2020), provides a comprehensive catalog of security and privacy controls. Although not directly written for AVs, this document offers guidance on cyber risk management to support system resilience for such vehicles. NIST Internal Report (IR) 8534, *Feature Description for Assessing Autonomous Vehicle Performance* (Hajjaj et al. 2024), provides a standardized framework for evaluating AV features, specifically to help support consistent assessment of performance, safety, and cybersecurity. While there are other relevant publications and guidance, it is worth acknowledging that a specific framework for AVs could be a worthwhile endeavor.

CONCLUSION

AVs represent a significant technological advancement with far-reaching implications for both commercial and military operations. The implementation of AI, LiDAR, GPS, SLAM, and other emerging technologies continues to push AVs toward greater autonomy, yet fundamental challenges remain, particularly regarding security vulnerabilities and operational limitations.

While the commercial sector has made strides in deploying AVs for public and private use, the military's approach, as evidenced by initiatives like the leader-follower program and its successors, demonstrates a commitment to leveraging AVs for combat and logistics applications that strive for higher levels of autonomy.

As AVs become more integrated with and reliant upon critical infrastructure sectors and networks, their security is intricately linked to the resilience of these interconnected systems. Consequently, cybersecurity threats such as data breaches, remote hacking, and GPS manipulation pose mounting risks that must be addressed through AI-driven security models and real-time monitoring systems. Along with a more robust and transparent legal landscape, this will undoubtedly bolster cyber resilience. Ensuring the safe and ethical deployment of AVs requires continued investment in security infrastructure and AI governance to shape the future of autonomy across industries. Such coordinated efforts will enhance U.S. cyber resilience and mitigate vulnerabilities, playing a vital role in defining the evolution of autonomous technologies across both civilian and military domains.

ABOUT THE AUTHOR

Donna Artusy is an attorney at a cybersecurity public company in Silicon Valley and non-resident fellow in Cyber Law, Policy, and Strategy at the Army Cyber Institute at West Point. She is also an area editor for The Cyber Defense Review Journal. She was previously a non-resident fellow at the Center for Security and Emerging Technology for CyberAI. Prior to earning her J.D., Donna received her graduate degree from Georgetown University's Walsh School of Foreign Service, and dual undergraduate degrees from the University of California, Berkeley. Previously, she completed the International Security and Intelligence program at the University of Cambridge. Donna's other professional experiences include co-founder of a health tech startup with multi-patented technology, Center for Strategic International Studies (CSIS), the United States Department of Justice, Santa Clara County Superior Court (civil and criminal), and Wilson Sonsini Goodrich and Rosati. She has numerous publications and speaking engagements around cybersecurity policy, law, and emerging tech.

REFERENCES

Ackerman, Evan. 2021. "What Full Autonomy Means for the Waymo Driver." IEEE Spectrum, March 4, 2021. https://spectrum.ieee.org/full-autonomy-waymo-driver.

Adly, Salah, Ahmed Moro, Sherif Hammad, and Shady A. Maged. 2023. "Prevention of Controller Area Network (CAN) Attacks on Electric Autonomous Vehicles." *Applied Sciences* 13 (16): 9374. https://doi.org/10.3390/app13169374.

Baker Donelson. 2024. "Autonomous Vehicle Statutes and Regulations Across the 50 States," September 20, 2024. https://www.bakerdonelson.com/autonomous-vehicle-statutes-and-regulations-across-the-50-states.

Bojarski, Mariusz, et al. 2016. "End to End Learning for Self-Driving Cars." *arXiv preprint,* 1–9. https://arxiv.org/pdf/1604.07316.

CISA (Cybersecurity and Infrastructure Security Agency). 2022. *Autonomous Ground Vehicles Security Guide: Transportation Systems Sector.* http://www.cisa.gov/sites/default/files/publications/Autonomous%2520Ground%2520Vehicles%2520Security%2520Guide.pdf.

Demchak, Chris. 2021. "Achieving Systemic Resilience in a Great Systems Conflict Era." *The Cyber Defense Review* 6 (2).

Durlik, Irmina, Tymoteusz Miller, Ewelina Kostecka, Zenon Zwierzewicz, and Adrianna Łobodzińska. 2024. "Cybersecurity in Autonomous Vehicles - Are We Ready for the Challenge?" *Electronics* 13 (13): 2654. https://doi.org/10.3390/electronics13132654.

Durrant-Whyte, Hugh, and Tim Bailey. 2006. "Simultaneous Localization and Mapping: Part I." *IEEE Robotics and Automation Magazine* 13 (2): 99–110. https://doi.org/10.1109/MRA.2006.1638022.

Eversden, Andrew. 2023. "Army Closing Down 'Leader-Follower' Robotic Truck Development, Eyeing Commercial Solutions," June 5, 2023. https://breakingdefense.com/2023/06/army-closing-down-leader-follower-robotic-truck-development-eyeing-commercial-solutions/.

Feickert, Andrew. 2025. *The Army's Robotic Combat Vehicle (RCV) Program.* Technical report. Congressional Research Service, May 20, 2025. https://crsreports.congress.gov/product/pdf/IF/IF11876.

Greenberg, Andy. 2024. "Millions of Vehicles Could Be Hacked and Tracked Thanks to a Simple Website Bug." Wired, September 26, 2024.

Groves, Paul. 2013. *Principles of GNSS, Inertial, and Multi-sensor Integrated Navigation Systems.* Boston: Artech House.

Guttieri, Karen. 2025. "Fighting Through Disruption: Reframing Cyber Resilience for Power Projection and Strategic Credibility." *The Cyber Defense Review* 10 (1): 93–114. https://doi.org/10.55682/cdr/egvf-mkys.

Hajjaj, H., T. T. Gamage, E. R. Griffor, T. P. Roth, and W. W. Guo. 2024. *Feature Description for Assessing Autonomous Vehicle Performance.* Technical report NIST IR 8534. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8534.

Harper, Jon. 2023. "DIU Issues Solicitation for GEARS Program to Convert Older Vehicles into Unmanned Systems," May 26, 2023. https://defensescoop.com/2023/05/26/diu-issues-solicitation-for-gears-program-to-convert-older-vehicles-into-unmanned-systems.

John, Ashley. 2023. "Army Selects Four Companies for Robotic Combat Vehicle Prototypes," September 20, 2023. https://www.army.mil/article/270093/army_selects_four_companies_for_robotic_combat_vehicle_prototypes.

Joint Task Force. 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* Technical report 800-37 Rev. 2. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-37r2.

Luckenbaugh, Josh. 2023. "Army Pressing Forward With Autonomous Vehicle Transport System." National Defense Magazine, March 1, 2023. https://www.nationaldefensemagazine.org/articles/2023/3/1/army-pressing-forward-with-autonomous-vehicle-transport-system.

Muller, Joann. 2019. "The U.S. Army Is Looking to Autonomous Vehicles to Cut Casualties," April 12, 2019.

Muller, Joann. 2024. "Generative AI Could Power the Next Wave of Self-Driving Cars," June 18, 2024. https://www.axios.com/2024/06/18/self-driving-cars-generative-ai.

National Counterintelligence and Security Center. 2022. *Autonomous Automotive Vehicles Supply Chain Risk.* Technical report. Washington, DC: U.S. Department of Homeland Security.

NHTSA (National Highway Traffic Safety Administration). n.d. *Automated Driving Systems.* https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems. U.S. Department of Transportation.

NIST (National Institute of Standards and Technology). 2020. *Security and Privacy Controls for Information Systems and Organizations.* Technical report 800-53, Rev. 5. https://doi.org/10.6028/NIST.SP.800-53r5.

Papadimitratos, Panagiotis, et al. 2009. "Vehicular Communication Systems: Enabling Technologies, Applications, and Future Outlook on Intelligent Transportation." *IEEE Communications Magazine* 47 (11): 84–95. https://doi.org/10.1109/MCOM.2009.5307471.

Rossi, Tiffiny. 2019. "Fast, Secure File Systems for Autonomous Vehicles from Tuxera," January 3, 2019. https://community.arm.com/arm-community-blogs/b/embedded-and-microcontrollers-blog/posts/fast-secure-file-systems-for-autonomous-vehicles-from-tuxera.

SAE (Society of Automotive Engineers). 2021. *SAE J3016 Levels of Driving Automation Update.* SAE International, June. https://www.sae.org/blog/sae-j3016-update.

Shan, Tianyu, and Brendan Englot. 2018. "LeGO-LOAM: Lightweight and Ground-Optimized LiDAR Odometry and Mapping on Variable Terrain." In *IEEE/RSJ International Conference on Intelligent Robots and Systems,* 4758–4765. https://arxiv.org/pdf/1805.03766.

Stouffer, Keith, et al. 2023. *Guide to Operational Technology (OT) Security.* Technical report 800-82 Rev. 3. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3.

✧ Operational and Strategic Framing ✧

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 81-97
https://doi.org/10.55682/cdr/p4kg-88cm

RESEARCH ARTICLE

Pulling the Thread: A Campaign Approach to Mission Thread Defense of Force Projection

David L. McNatt[1], Eunseok (Sam) Yoo[2], Joshua J. Welte[3], Pete Sinclair[1]

[1]U.S. Army Cyber Command, Fort Gordon, GA, USA
[2]Defense Logistics Agency Energy Middle East, Naval Support Activity, Bahrain
[3]U.S. Transportation Command, Scott Air Force Base, IL, USA

The U.S. military's ability to rapidly project power around the globe is a cornerstone of American defense strategy, and adversaries leverage denial strategies across domains to disrupt this capability. Recent cyberspace exploitation campaigns have infiltrated U.S. critical infrastructure, raising concerns about the military's ability to project decisive force during crises. Increasing cyber resilience for force projection requires transitioning from an asset-focused approach to a more proactive, mission-driven approach for defensive cyberspace operations (DCO). U.S. Army Cyber Command (ARCYBER) is implementing a campaign approach to address the cross-organizational challenge of increasing cyber resilience by leveraging partnerships to facilitate collaboration, leading the process of identifying critical systems, and producing plans to align requirements with resources. ARCYBER works closely with the Total Army (Active, Guard, and Reserve) and Joint and Interagency partners to promote effective collaboration, providing a common framework to translate organizational missions into cyberspace defense priorities. ARCYBER defends the Army's mission threads by maneuvering forces and hardening networks. Beyond proactive mitigation, the logistics enterprise must be prepared to "fight through" or bypass disruptions that penetrate defenses, ensuring mission success even in contested environments.

Keywords: cyber resilience, force projection, logistics, critical infrastructure, mission thread analysis, defensive cyberspace operations, risk mitigation

INTRODUCTION

> "In any kind of operation, there are two things you must get right…you have got to have your command and control in place, and you have got to have a robust, reliable logistics system." - LTG (R) Paul Mikolashek [1]

In the summer of 2017, chaos erupted at the Copenhagen headquarters of Maersk, the multinational shipping giant, as employees scrambled across open-plan offices to unplug computers, watching in horror as more screens flickered to black. A Russian cyber actor deployed malicious software (malware) known as *NotPetya* against Ukraine, which spread far beyond the country's borders. The cyberattack exploited a vulnerability in the Windows update mechanism to irreversibly encrypt an infected computer's master boot record, preventing it from finding its own operating system. The infected systems and the data residing inside them were effectively destroyed. Maersk's operations, which accounted for a fifth of global shipping capacity across 76 ports and nearly 800 ships, came to a standstill, suffering over $300 million in damages. The disruption exposed the vulnerability of modern commerce's interconnected systems to cyberattacks (McQuade 2018). This scenario highlights the potential for similar disruptions to defense critical infrastructure (DCI) and the joint logistics enterprise (JLEnt) during a major contingency operation.

As America's rivals grow more adept at cyberspace exploitation, there is an ongoing debate about how the United States can best secure itself in this domain. Recently, multiple cyber exploitation campaigns have infiltrated U.S. critical infrastructure, raising concerns about the U.S. military's ability to respond in a crisis. Proposed responses to these threats include new regulations, adjustments to roles and responsibilities across the national security enterprise, expanding the cyber workforce, and placing greater emphasis on "defending forward" and imposing costs on rivals (Segal 2025). U.S. Army Cyber Command (ARCYBER), as the Army's service cyberspace component, is responsible for operating and defending the Army's portion of the Department of Defense Information Network (DODIN), and when directed, other DODIN and non-DODIN networks (HQDA 2017). How can ARCYBER contribute to these emerging solutions and proactively mitigate threats to U.S. military force projection? Addressing this requires understanding both the nature of cyber risks and ARCYBER's unique advantages.

The complexity of cyber threats and limited resources often creates a default organizational preference for relegating cyber risk to technical commands and staff directorates. This status quo approach relies on asset- and compliance-based cyberspace security measures, which are necessary but not sufficient for establishing cyber resilience. The intangible nature of the cyberspace domain and the lack of institutional cyber knowledge often exacerbate this incentive, making operational planners hesitant to integrate cyber considerations into their operations. Furthermore, the technical cyber workforce may not always be familiar with

1. Quoted in Klug (2023)

operational staff priorities and may struggle to communicate technical cyber information in a way that is useful to operational staff. This often results in a lack of shared cyber risk understanding across organizations. This separation creates a disconnect between operational mission requirements and technical asset dependencies, hindering the Army's ability to optimize its cyberspace defense posture in a contested environment.

The ability to project power across transoceanic distances is increasingly challenged by rivals working to disrupt this capability across domains. Increasing cyber resilience in Army force projection requires transitioning from an asset-based approach to a more proactive, mission-based approach for defensive cyberspace operations (DCO). ARCYBER's campaign approach involves partnering with key stakeholders, identifying defense requirements, and developing plans that align requirements with resources. Effective collaboration across organizations requires a shared understanding of the strategic environment, cyber threats, and the challenges inherent to the cyberspace domain. To achieve this, ARCYBER works closely with the Total Army (Active, Guard, and Reserve) and Joint and Interagency partners. Through this collaborative effort, ARCYBER leads the process to enable supporting commands to analyze their mission threads, identify critical systems, and submit defense requirements. Finally, ARCYBER develops plans that synchronize cyberspace defense requirements and resources to mitigate threats to Army missions proactively. Through this approach, ARCYBER aims to empower commanders to make risk-informed decisions and improve overall operational resilience. Ultimately, this approach enhances the Army's ability to project power in a contested cyberspace environment.

This article is organized into four main sections. The first section provides a foundational understanding of the strategic cyber threat to the JLEnt. The second section highlights the unique challenges associated with cyber resilience. The third section details ARCYBER's approach to enhancing cyber resilience through partnerships, process, and plans. The fourth section looks beyond cyber resilience in logistics to highlight other critical functions and discuss logistics concepts that aim to improve overall operational resilience in a contested environment.

UNDERSTANDING THE LANDSCAPE

The Cyber Strategic Environment

According to *cyber persistence theory* by Harknett, Fischerkeller, and Goldman (2023), cyber actors continuously pursue initiative persistence to shape the contemporary cyber strategic environment. This pursuit of initiative persistence is driven by the underlying structure of cyberspace—a set of ever-changing digital conditions that incentivize state actors to continuously engage in cyber operations against other states to set security conditions to their advantage. Unlike nuclear or conventional models, which rely on coercion, these cyberspace

operations occur within a framework of persistent engagement, allowing rivals to continuously exploit vulnerabilities in pursuit of strategic advantage. Consequently, cyberspace engagements are best seen as continuous bouts of constant competition between rivals seeking cumulative outcomes through, primarily, cyber *faits accomplis*, which are efforts to seize and exploit digital terrain before an adversary can react.

Since the early 2010s, the strategic cyberspace competition for initiative persistence has evolved as part of the intensifying security competition between U.S. alliance networks and an increasingly cooperative Eurasian entente comprising China, Russia, Iran, and North Korea. The U.S. military's ability to project power rapidly across the globe is the foundation for American defense policy in this dynamic security environment (Busler 2022). Force projection, or "the ability to [deploy and sustain] the military instrument of national power from the United States or another theater in response to requirements for military operations," relies on the JLEnt through DCI (Joint Chiefs of Staff 2022b, GL-10). Logistics is "planning and executing the movement and support of forces" (Joint Chiefs of Staff 2023b, GL-5), and DCI is the "Department of Defense and non-Department of Defense networked assets and facilities essential to project, support, and sustain military forces and operations worldwide" (Joint Chiefs of Staff 2023a, GL-5). Cyber persistence theory, along with the observed evidence, strongly suggests that the contemporary cyber strategic environment poses significant risks to the U.S. military's power projection. Prudent planning, therefore, demands that U.S. military planners anticipate that potential adversaries will not wait for a crisis to contest America's ability to generate, project, and sustain its forces. Instead, rivals will continuously seek to pre-position on DCI to enable denial-by-disruption strategies calibrated to degrade U.S. force projection (van Ovost 2022). In short, rivals will use cyber *faits accomplis* to shape security conditions to their advantage.

By contesting logistics and force projection, adversary denial strategies could significantly hinder operational effectiveness and strategic decision-making. A denial strategy is a military approach aimed at undermining an adversary's ability to achieve their objectives, particularly in territory or political goals, by making the costs of pursuit prohibitively high, thereby forcing them to reconsider or concede (Pape 1996; Borghard and Lonergan 2017). With respect to military strategy, "logistics remains a means, circumscribes the potential ways, and plays a vital role in determining the time horizon necessary to achieve the desired ends depending on the level of risk" (Klug and Leonard 2025, 2). By contesting U.S. military force projection, adversaries can impact strategic decision-making by reducing options, delaying responses, and increasing risk. This disruption extends to the operational level of warfare, where commanders and staff "use operational art through campaign design and planning to sequence and sustain battles" (Benson 2025, 100). Therefore, the U.S. military must increase its operational resilience, with cyber resilience as a critical component, to counter these adversary denial strategies and maintain its strategic edge.

The *2022 National Defense Strategy* (NDS) acknowledged that today's contested environment poses a threat to U.S. strategic coherence. To counter this, the NDS prioritized resilience as a cornerstone of America's ability to deter attacks and prevail in armed conflict. Defining resilience as "the ability to withstand, fight through, and recover quickly from disruption," the NDS emphasized the importance of cyber resilience in mitigating cyber risk across "a growing surface of vital networks and critical infrastructure" (DoD 2022, 8). Cyber risk involves the potential for damage caused by the exploitation of vulnerabilities in information systems, considering both the likelihood of an attack and the impact if it occurs (Jabbour and Poisson 2016). Cyber risk has a reciprocal relationship with cyber resilience, in which risk informs resilience, and resilience in turn mitigates risk. Cyber resilience involves anticipating, withstanding, recovering from, and adapting to disruptions to systems that utilize or depend on cyber resources (NIST 2021). Cyber resilience is essential for maintaining operational resilience. With military operations increasingly reliant on digital technology, cyber risks amplify overall operational risks (Thomas 2024). Mitigating these threats is an increasingly complex challenge, driven by the rapid proliferation of information systems and the growing sophistication of exploits from both rival nation states and cybercriminals.

Cyber Threats

The information technology (IT) and operational technology (OT) systems underpinning U.S. critical infrastructure and the JLEnt have become increasingly automated and interconnected. IT encompasses devices such as laptops, software, and networking tools for communication and productivity. OT encompasses systems such as industrial control systems (ICS), supervisory control and data acquisition (SCADA), and programmable logic controllers (PLC). These cyber-physical connections enable remote monitoring and control of dispersed equipment (Parfomak and Jaikaran 2021), but their interconnectivity introduces greater cyber risks.

In IT and OT systems, disconnects are often revealed between the desired functionality and the actual behavior of the implemented code. These discrepancies create vulnerabilities in the digital landscape which offensive and defensive cyberspace operations teams continuously vie over for advantage. The effectiveness of cyberspace operations depends on identifying these underlying weaknesses. Detecting weaknesses in a target system requires a skilled team of specialists; this team includes operators who gain and maintain access, analysts who identify vulnerabilities, and developers who create exploits for operators to deploy. Exploitation efforts must start long before a crisis arises because operational effectiveness demands deep system knowledge. Moreover, once an exploit is used, its discovery, followed by patching or system hardening, limits its effectiveness for future use (Libicki 2012; Lin 2010; Smeets 2022).

The ongoing struggle over exploiting and protecting vulnerabilities has led to the emergence of various types of offensive cyberspace operations (OCO), each with distinct objectives and

methods. To better understand how threats gain an advantage in cyberspace, it is essential to grasp the types of effects OCO can produce and the mechanisms used to achieve those effects. Unlike actions in the conventional strategic environment, vis-à-vis the application of land, sea, or air power, OCO cannot substitute force for exploitation. This is a consequence of the clandestine character of cyberspace exploitation, as actors must obscure their intentions and activities to prevent defenders from rapidly closing off vulnerable avenues of approach and to avoid escalation. Additionally, since OCO relies on subverting system vulnerabilities clandestinely, political scientist Lennart Maschmeyer (2021) argues that an operational trilemma constrains the effectiveness of cyberspace operations: the *speed* with which vulnerabilities can be identified and exploited; the *intensity* of the effects generated; and the degree of *control* over a system and the effects delivered. Achieving optimal results simultaneously in all three areas is not possible.

OCO consists of cyberspace exploitation and cyberspace attack activities. Cyberspace exploitation involves access creation; intelligence, surveillance, and reconnaissance (ISR) activities; and preparation for effects delivery (Joint Chiefs of Staff 2022a). One example of this activity is Volt Typhoon, a Chinese state-sponsored cyber actor that compromised the IT networks of multiple U.S. critical infrastructure sectors across the continental United States and territories such as Guam. In addition to ISR in cyberspace, Volt Typhoon's actions appear to be aimed at pre-positioning themselves within networks for potential lateral movement to OT assets, with the intent to disrupt critical functions during a moment of crisis or military conflict (Jaikaran 2024; CISA 2024). Cyberspace attacks deliver effects. U.S. military doctrine distinguishes between system *denial* effects—which reduce a system's functional capacity (*degrade*), temporarily deny access (*disrupt*), or irreparably deny access (*destroy*)—and system *manipulation* that creates physical effects (Joint Chiefs of Staff 2022a).

According to international relations scholar Max Smeets (2022), cyber effects are primarily generated through three mechanisms: Distributed Denial of Service (DDoS), data manipulation, and system manipulation. First, DDoS attacks overwhelm a target system with a flood of data packets from multiple compromised sources. DDoS attacks are among the simplest and cheapest to execute, typically affecting only publicly accessible websites. Though temporary, their impact can be significant (Borghard and Lonergan 2017). A notable example is the 2012-2013 DDoS attacks by Iranian cyber actors against nearly 50 U.S. financial institutions, which disrupted access to public websites and incurred substantial mitigation costs (Warner 2020).

The second mechanism is data manipulation, where an attacker with the necessary access can modify, delete, or encrypt data (Smeets 2022). This action destroys value and renders digital resources unusable. Depending on the nature of the data targeted, entire systems may be rendered non-functional, as seen in the *NotPetya* attacks on Maersk. A similar example is the May 2021 Colonial Pipeline cyberattack, in which the DarkSide ransomware group

encrypted the company's IT billing systems. While there was no evidence that the company's OT systems were compromised, they were also shut down as a precaution. This attack crippled the operation of the largest fuel pipeline in the United States, halting the flow of gasoline, diesel, and jet fuel along the East Coast. The resulting disruption led to widespread fuel shortages, price hikes, and panic buying, causing significant economic and logistical challenges. Ultimately, Colonial Pipeline paid a ransom to regain access to its systems, citing the critical importance of its infrastructure and its responsibility to the nation (Nakashima, Torbati, and Englund 2021; Bogage 2021).

The third mechanism is system manipulation, which is typically achieved through OT systems (Smeets 2022). Manipulating a system can cause it to perform a regular function at a time or in a way that is not desired. In 2000, a disgruntled former employee of Maroochy Water Services in Queensland, Australia, exploited vulnerabilities in the sewage control system, releasing over 750,000 gallons of raw sewage into public waterways over several weeks. In extreme cases, system manipulation can alter a system's processes in ways that result in physical destruction. For example, in 2007, researchers conducted the Aurora Generator Test at Idaho National Labs to demonstrate how a cyberattack could physically damage the electric grid. Using malware to manipulate a diesel generator's circuit breakers produced abnormal torques, ultimately causing its destruction. Perhaps most notably, in 2009, a cyber actor exploited the PLCs controlling the centrifuges at Iran's nuclear enrichment facility in Natanz. The malware modified the centrifuges' operation, causing physical damage to between 1,000 and 2,000 of the devices (Zetter 2014).

While cyber effects cannot entirely halt U.S. military force projection, these effects can introduce Clausewitz's "fog, friction, and chance" into critical nodes of the logistics enterprise, causing cascading disruptions across operations. Military cyberspace operations weaponize friction in the contest between opposing military systems (Rovner 2020). The intensity of cyber effects against DCI will, however, be constrained by Maschmeyer's trilemma. At the outset of a conflict, adversaries will have a finite number of exploits available. As these effects are delivered and mitigated, adversaries will need time to identify new vulnerabilities and develop additional exploits. They must choose whether to concentrate their effects early in the conflict or to sequence them for sustained disruption.

These cyber resource constraints make targeting vulnerabilities in military logistics particularly appealing. Logistics operations often rely on information sharing and partnerships with commercial entities that may have inconsistent cybersecurity measures. These inconsistencies can create exploitable conditions that offer adversaries high potential payoffs. Gaining insight into logistics operations early in a conflict through cyberspace exploitation offers invaluable intelligence on U.S. intentions. DDoS attacks on public-facing websites can hinder cooperation with commercial partners, while altering or destroying data can introduce inefficiencies and necessitate duplicative efforts. Logical and physical destruction effects require costly and

time-consuming mitigation efforts. These disruptions reverberate through tightly coordinated logistical operations, causing delays in the logistics chain and creating narrative vulnerabilities regarding U.S. capability and commitment (Dougherty 2023).

CROSS-ORGANIZATIONAL CHALLENGES FOR DEFENSIVE CYBERSPACE OPERATIONS

Enhancing cyber resilience for critical missions in the face of increasingly sophisticated cyber threats is a significant challenge for defense planning that requires extensive collaboration. In theory, the malleability of cyberspace should favor the defender, but in practice, the scale and complexity of modern information systems leave ample opportunity for exploitation (Libicki 2012). Adversaries seek to disrupt force projection by targeting dependencies within mission threads, where a cyber effect can create cascading delays, miscoordination, and mission failures. Mission threads are "operationally driven, technically supported descriptions of the end-to-end set of activities required to execute a mission or mission task" (CJCS 2022, A-5–A-6). Cyber resilience is a critical component of *mission assurance*, a doctrinal process that seeks to ensure that everything needed to carry out essential functions—including people, equipment, facilities, networks, and supply chains—remains operational and resilient, no matter the environment or situation (DoD 2018). The challenge of mitigating cyber risk lies in the requirement for "analysis beyond a specific portion of cyberspace, geographic area, or organizational responsibility," and the need for units to "apply systems thinking to understand the processes, components, dependencies, and interactions from both a technical and organizational perspective" (HQDA 2024, 1–2).

The traditional approach to managing cyber risk often focuses on network operations for functionality and security. However, this approach places too much reliance on the technical workforce to mitigate cyber risk. This tendency stems from the organizational and technical complexity of network analysis and risk communication. Operational planners often overlook cyber considerations due to the intangible nature of cyberspace and a general lack of institutional cyber knowledge. At the same time, technical personnel are often unfamiliar with operational priorities and struggle to communicate technical information in a way that is useful to operational planners. As a result, cyber risk is frequently relegated to specialized organizations such as the G-6/J-6 staff directorate or a cyberspace operations headquarters. The disconnect between operational and technical planners creates a gap in understanding between operational mission requirements and technical asset dependencies (Corbari et al. 2024).

The involvement of multiple stakeholders with varying roles and authorities further compounds the complexity of mitigating cyber risk to force projection. This challenge is particularly pronounced when Mission Relevant Terrain-Cyber (MRT-C) systems, such as logistics networks owned by private sector entities, reside outside of the DODIN. The authority to

address active threats on a network is fragmented, depending on whether the threat occurs on a private or public sector network and whether the nation is engaged in armed conflict. Consequently, responsibility for countering threats to Army networks is spread across Federal Law Enforcement, Homeland Security, and Homeland Defense activities. This fragmentation of authority impacts both preparedness and response times in peacetime and wartime, complicating the ability to address emerging threats swiftly.

ARCYBER has identified these challenges and adapted its approach to solving them over time. In 2020, a Homeland Defense planning effort in support of Headquarters, Department of the Army (HQDA) initially highlighted the complexities of determining and acting upon Army cyber protection interests in the homeland. This effort ultimately led to the Army Force Projection (AFP) planning effort. Utilizing Mission Thread Analysis (MTA), the AFP effort revealed the need for a broader Army-wide initiative to address these issues. This requirement, in turn, led to the development of the DCO-Optimization effort and the Army Defensive Cyberspace Optimization Conference (ADCyOC). These complementary planning efforts aim to define and document the Army's cyberspace defense requirements more accurately, empowering ARCYBER to direct forces and harden networks more effectively. Moreover, these efforts help identify dependencies where the Army requires Interagency support. While national cyber policy continues to evolve, the Army must be prepared to advocate for its interests with Interagency partners effectively.

ADOPTING A CAMPAIGN APPROACH TO INCREASE CYBER RESILIENCE

To address emerging challenges in cyberspace, ARCYBER has refined its partnerships, processes, and planning to mitigate cyber risk and de-conflict overlapping efforts. In response to increasingly sophisticated cyber threats, ARCYBER has refined the MTA process to better employ defensive cyberspace forces and close the gaps in cyberspace defense that traditional asset-based, compliance-driven, and reactive security measures leave unaddressed. By decomposing mission threads into operational and technical requirements, MTA enables proactive risk mitigation through the identification of MRT-C. MRT-C includes the components of the cyber terrain such as devices, links, applications, and protocols that are essential to the operation of a critical asset or the successful completion of a mission. Mapping MRT-C allows defensive cyberspace forces to maneuver more effectively and harden networks in support of mission owners (HQDA 2024; Corbari et al. 2024). DCO seeks to "defeat the threat of a specific adversary and/or to return a compromised network to a secure and functional state" (Joint Chiefs of Staff 2022a, II–4). Defensive cyberspace forces need a deep understanding of network architecture, cross-organizational mission dependencies, and prioritized directives to proactively mitigate risk and respond swiftly to incidents.

Leveraging Partnerships

The cross-organizational challenge of cyber resilience in force projection requires partnerships across the Department of War (DoW), the Total Army, and the Interagency. The unique knowledge, relationships, and authorities of these partners complement ARCYBER's capabilities. Building relationships with these partners before a crisis is crucial to their effectiveness in times of need. While Interagency partners and Total Army defensive cyberspace forces may not be ideal for emergency response, they are well-suited for cyberspace defense requirements that involve long-term collaboration with MRT-C owner and operators, both on and off the DODIN. Army Reserve and National Guard defensive cyberspace forces have developed capabilities leveraging their long-term relationships with MRT-C owners throughout the United States, as well as their experience with commercial technology partners.

Force projection requires a collaborative approach between service and joint stakeholders in cyberspace operations, homeland defense, logistics, and mobilization. While HQDA provides institutional oversight and coordination, key stakeholders span various operational functions. In cyberspace, this includes U.S. Cyber Command (USCYBERCOM), DoD Cyber Defense Command (DCDC), and ARCYBER. Homeland defense relies on the collaboration of U.S. Northern Command (USNORTHCOM) and U.S. Army North (ARNORTH). Logistics success hinges on the combined efforts of U.S. Transportation Command (USTRANSCOM), the Defense Logistics Agency (DLA), Army Materiel Command (AMC), U.S. Army Transportation Command (ARTRANS), and other service transportation components. Finally, effective mobilization necessitates seamless integration between Forces Command (FORSCOM), the Office of the Chief of Army Reserve (OCAR), the National Guard Bureau (NGB), and First Army. This intricate *system-of-systems* underscores the criticality of collaboration in protecting DCI and ensuring successful mobilization and force projection.

Cyber effects pose a significant threat to DCI; yet, without adequate support for collaboration, Interagency partners may lack the awareness and preparedness necessary to effectively mitigate these attacks, thereby increasing cyber risk. These partners include the Department of Homeland Security (DHS), which encompasses Homeland Security Investigations (HSI), the Federal Emergency Management Agency (FEMA), and the Cybersecurity and Infrastructure Security Agency (CISA); the Department of Justice (DOJ); and various state, local, and tribal governments, including their law enforcement components. Experience has shown that the Interagency is sometimes unaware of DoW and Army requirements, leaving them unprepared to respond to cyberattacks on DCI vital to DoW missions. This knowledge gap is a policy issue stemming from the unclear division of responsibilities between Homeland Security and Homeland Defense mission sets and authorities.

To address these coordination issues, engaging with interagency partners before a crisis is essential. By sharing off-DODIN DCI protection requirements with Interagency partners

while campaigning in competition, the Army can give them ample time to prepare and take proactive measures. This preparation can include collaborating with the private sector and developing legal strategies to counter malicious cyber actors (MCA) when necessary. Building relationships between the interagency and MRT-C owners and operators during this phase can also facilitate a more effective response to MCAs targeting MRT-C. This approach is analogous to how a local fire department works with businesses to identify potential fire hazards and develop tailored response plans, ensuring they are better equipped to respond in an emergency. Taking a proactive and collaborative approach strengthens collective defenses and improves the ability to respond to cyber threats.

Leading the Process

ARCYBER has adopted a campaign approach to optimize Army DCO and proactively mitigate risk to critical missions such as force projection. This approach is an iterative process of continuous improvement that requires collaboration across stakeholders to identify MRT-C and defend the Army's vital missions. This process is structured around the annual ADCyOC to facilitate a shared understanding across the Army enterprise, and bi-weekly working groups, which provide regular touchpoints with stakeholders. This structured process enables ARCYBER to collaborate with stakeholders across the Army, providing a common framework to translate Army missions into actionable cyberspace defense priorities. It enables stakeholders to advocate for their priorities, allowing ARCYBER to engage with units and gather the technical information needed to plan and execute DCO effectively.

MTA supports this campaign approach by providing a framework for organizations responsible for planning major operations, contingencies, or institutional functions to collaborate with ARCYBER. Through this analysis, organizations can translate their missions into mission threads, MRT-C, and actionable cyberspace defense requirements. This approach shifts the focus from individual assets to a more holistic understanding of mission vulnerabilities, encompassing those that extend beyond organizational boundaries. By clearly mapping MRT-C, MTA enables commanders to make better-informed decisions regarding resource allocation of defensive cyberspace forces and risk mitigation to support a mission (HQDA 2024).

To achieve this comprehensive understanding, operational planners and technical professionals must collaborate to identify and analyze mission threads. Operational planners from the G-3 and G-5 staff directorates work with technical signal and cyber professionals to decompose their mission essential tasks. MTA involves identifying, defining, and depicting mission process threads (MPT), which outline the conceptual flow of the task, and mission engineering threads (MEngT), which capture the technical components required to execute each step. Mission owners use the MPTs to "depict the process of a mission as a series of steps or actions required to achieve successful accomplishment" (Corbari et al. 2024, 42). The MEngT includes the components, both physical and digital, necessary to execute each

step in the MPT successfully. When analyzing the MEngT, planners must carefully scope the requirements to prevent over-analysis and avoid wasted effort. Common models for MEngT analysis include the cyberspace layer model (persona, logical, physical) and network layer models, such as the Open Systems Interconnection (OSI) Model. Critically, staff must also identify any external dependencies, such as electrical power and satellite connectivity (HQDA 2024; Corbari et al. 2024).

Effective MTA results in a clear depiction and understanding of the organization's MRT-C, highlighting the cross-organizational dependencies between mission owners and asset owners (Corbari et al. 2024). This information is captured within the Mission Assurance Risk Management System (MARMS) through the Mission Assurance Decision Support System (MADSS) and Strategic Mission Assurance Data System (SMADS) (CJCS 2023). Identifying and depicting this cyber terrain creates situational awareness of dependencies, uncovers vulnerabilities, and supports resource allocation decisions for maintaining operational continuity.

This comprehensive understanding of MRT-C, achieved through MTA, allows commanders to make informed risk assessments and operational decisions. With a clearer understanding of the cyber risks to their mission threads, commanders can more effectively decide whether to avoid, mitigate, or accept risk. Actions to address these risks "may include changing how the capability is employed, mitigating the risk throughout the mission thread, reengineering portions of the mission thread, or preparing to operate with diminished capabilities [or falling back on analog processes]" (HQDA 2024, 3). Commanders may also elevate the risk to a higher echelon for further action (HQDA 2024).

Furthermore, identifying MRT-C through MTA informs other critical processes such as determining defense requirements, positioning forces, informing task critical asset (TCA) nominations, and identifying DCI. A TCA is "an asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD or OSD Components to execute the capability or mission-essential task it supports" (DoD 2018, 19). In addition to TCA and DCI identification, MTA provides a more comprehensive understanding of the vulnerabilities tied to those resources. When cyberspace defense requirements are based on a detailed knowledge of MRT-C, intelligence collection efforts are more focused and defensive cyberspace forces can deploy sensors on the network more effectively, resulting in a more agile and responsive defense that enables defensive cyberspace forces to address incidents swiftly.

Beyond the tangible actions taken, fostering a psychological "perception of control" is crucial for cyber resilience. When effective staff collaboration empowers leaders to project a sense of control while they "fight through" a cyber disruption, it sustains trust and cohesion within their organizations, reducing the risk of cascading disruptions across their functions (Thomas 2024).

Producing Plans

ARCYBER increases cyber resilience across the Army enterprise by developing plans that align requirements and resources. First, ARCYBER advocates for resources by consolidating Defense Requirements Statements (DRS) from across the Army enterprise and facilitates their inclusion in USCYBERCOM's mission alignment process. The DRS uses a straightforward format, enabling mission owners to describe their cybersecurity needs clearly. This standardized approach facilitates a better understanding of individual requirements and guides mission owners in providing essential information for DCO planning and prioritization. USCYBERCOM's mission alignment process, in turn, leverages these DRS submissions to inform their decisions regarding mission prioritization and the alignment of cyber mission forces across military services and Joint Force Headquarters-Cyber (JFHQ-C) (Corbari et al. 2024). Finally, USCYBERCOM's Combatant Command Campaign Plan (CCP) and annual orders process operationalize these forces across the cyber enterprise.

Second, ARCYBER operationalizes near-term requirements to proactively mitigate cyber risk across the Army through its own annual orders process. When Army organizations identify their MRT-C and cyberspace defense requirements, they often lack the organic resources and expertise to fully defend their mission threads. Collaboration with supporting Army commands allows ARCYBER to capture defense requirements in its annual orders and align forces to missions. ARCYBER defends the Army's mission threads by maneuvering forces and hardening networks. These forces include cyber protection teams (CPTs), which can deploy mission elements forward to hunt and clear threats from networks and harden them against future compromise. CPTs can also monitor MRT-C on an ongoing basis. In addition to CPTs, Network Enterprise Technology Command's (NETCOM) Regional Cyber Centers (RCC) work with ARCYBER's G-36 and the Cyber Protection Brigade (CPB) to leverage enterprise-wide analytics in support of identified cyberspace defense requirements (Barrett 2024). ARCYBER also utilizes cyber red teams and cyber readiness inspection activity (CRIA) teams to identify vulnerabilities and enable defense of MRT-C. Requirements that exceed ARCYBER's capacity can be referred to the Cyber National Mission Force and Interagency partners (Corbari et al. 2024).

Lastly, ARCYBER captures long-term planning requirements to increase cyber resilience across the Army through its campaign support plan (CSP) and contingency planning. ARCYBER's CSP aligns with USCYBERCOM's CCP and HQDA's Army Campaign Plan (ACP). Through these processes, ARCYBER collaborates on longer-term operational and institutional initiatives to strengthen cyber resilience in critical Army missions such as force projection. These initiatives may include operational partnerships, network modernization, force structure adjustments, and the fielding of new capabilities. This planning is most effective when informed by MRT-C and cyberspace defense requirements from across the Army enterprise. ARCYBER also incorporates these requirements into its contingency plans, enabling a more

rapid response in a crisis to support operation plans (OPLANs). Effective collaboration across the Army enterprise facilitates planning that bolsters cyber resilience in both campaigning and contingency response efforts.

PREPARING TO "FIGHT THROUGH" DISRUPTIONS

Achieving broader operational resilience requires mission thread defense of other critical functions and more wholistic concepts for operational risk mitigation across the logistics enterprise. MTA allows other critical functions, such as multinational operations, ISR, long-range precision fires, command and control, and integrated air and missile defense (IAMD), to shift focus from individual assets toward a broader understanding of mission vulnerabilities.

While proactive mitigation of cyber risk enhances overall operational resilience, the logistics enterprise must be prepared to "fight through" disruptions caused by cyber effects that bypass efforts to protect and defend MRT-C. The logistics community recognizes the challenges of the current contested environment and is developing concepts to strengthen operational resilience in the face of denial effects across domains. Integrating logistics planners earlier in the planning process can improve operational resilience by ensuring that courses of action are more aligned with logistics capacity, rather than accepting risks to sustain operations that were conceived without proactive logistics input (Hughes 2024).

Chris Dougherty (2023), a researcher at the Center for a New American Security (CNAS), developed a framework for responding to the contested logistics environment through an adaptive logistics approach. Central to the framework is the persistent challenge that "reinforcements take too long to arrive from the United States or other theaters to defend allies and partners or counterattack from a position of strength" (11). To enable forward forces to persist and build combat power, Dougherty proposes an adaptive logistics strategy that can transition from efficient methods to more resilient ones, based on threats, operational needs, and the status of infrastructure.

Dougherty's (2023) adaptive logistics strategy has forward, theater, and enterprise components. He offers three elements in enhancing resiliency in forward logistics. First, forward forces should moderate their operational tempo to minimize attrition by doing less and avoiding destruction. Second, the U.S. military should preposition forces and materials in dispersed, secure locations to reduce reliance on resupply from rear areas. Third, Army forces should prepare to "live off the land" by sourcing fuel and other essential materials locally, thereby reducing their dependence on uninterrupted resupply. At the theater level, intermediate basing operations could further strengthen theater logistics by supporting multiple defensible lines of communication. At the enterprise level, accurate and timely information enables a responsive and efficient "pull" model where logistics meets operational demand "just-in-time." In a contested environment where information is degraded, logistics must shift to a robust

and sufficient "push" model, which relies on anticipating needs and moving resources during windows of opportunity. With a risk-informed understanding of the cyber threat, commanders are better equipped to "fight through" disruptions by combining cyber and operational mitigation activities.

CONCLUSION

As the Army navigates today's contested cyber environment and evolving fiscal realities, leaders must not lose sight of the fact that sustained investment in cyber resilience will remain a strategic necessity. The ability to project force and sustain operations will hinge on the Army's ability to mount effective cyber defenses that can anticipate, withstand, and recover from persistent threat activity. ARCYBER's campaign approach provides a starting point, but its success will depend upon a long-term commitment from military leaders, planners, and technical experts. By prioritizing proactive cyberspace defense measures, integrating cyber resilience into force planning, and fostering collaboration, the Army can ensure that its logistics enterprise remains resilient in the face of ever-changing threats. The alternative—waiting until a crisis to react—risks ceding the initiative to adversaries already operating in a persistent state of cyber engagement. The Army's ability to fight and win in a cyber-contested battlespace is precisely what hangs in the balance.

ABOUT THE AUTHORS

Colonel David L. McNatt is an Army Strategist serving at U.S. Army Cyber Command as the G-5 Director for Strategy, Plans, and Policy. He ensures ARCYBER's near-term efforts support future objectives. He is a graduate of Boston University as well as the Naval War College where he also studied as a Cyber & Innovation Policy Institute (CIPI) Gravely student.

Lieutenant Colonel Eunseok (Sam) Yoo is an Army Logistician currently commanding the Defense Logistics Agency Energy Middle East. Previously, he served as the Strategic Operations Division Chief (G-5) at U.S. Army Cyber Command, focusing on Global Force Management, Security Cooperation, and implications of Defensive Cyberspace Operations for the Army enterprise. He holds an M.S. in Logistics Management from Florida Institute of Technology and is a graduate from the School of Advanced Military Studies (SAMS), the Joint Cyberspace Operational Planners Course, and the College of Naval Command and Staff at the Naval War College.

Major Joshua J. Welte is an Army Strategist at U.S. Transportation Command. While contributing to this article, he served as a strategic planner at U.S. Army Cyber Command. At ARCYBER, he led initiatives in areas such as Indo-Pacific plans, Army cyber posture, expeditionary cyberspace operations, cyberspace security cooperation, and defensive cyberspace operations. MAJ Welte holds an M.A. in Security Studies from Kansas State University and a Certificate in Social Influence from Augusta University. He is a graduate of the School of Advanced Military Studies (SAMS), the Joint Cyberspace Operational Planners Course, and the Joint Logistics Planners Course.

Mr. Pete Sinclair is currently employed by Peraton as a Cyberspace Operations Planner in support of the U.S. Army Cyber Command G-5. He retired from the Army after serving in three different branches over 21 years and six deployments. He is a graduate of Northern Michigan University and the School of Advanced Military Studies (SAMS). He is also a graduate of the Harvard Kennedy School's Executive Education Leadership in Homeland Security program and the Homeland Protection Course at the Massachusetts Institute of Technology's Lincoln Laboratory. This is his second contribution to *The Cyber Defense Review*.

REFERENCES

Barrett, Maria B. 2024. "Operational Perspectives from the Field – ARCYBER in the Cyberspace Domain." *The Cyber Defense Review* 9 (1): 19–30. https://www.jstor.org/stable/48770661.

Benson, Kevin. 2025. "The Operational Level of War and Logistics." In *Professionals Talk Logistics: Sustaining Strategy and Operations,* edited by John Klug and Steve Leonard, 100–115. Havant, UK: Howgate Publishing.

Bogage, Jacob. 2021. *Colonial Pipeline CEO Says Paying $4.4 Million Ransom Was 'the Right Thing to Do for the Country'.* The Washington Post, May 19, 2021. https://www.washingtonpost.com/business/2021/05/19/colonial-pipeline-ransom-joseph-blunt/.

Borghard, Erica D., and Shawn W. Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26 (3): 275–305. https://doi.org/10.1080/09636412.2017.1306396.

Busler, Bruce. 2022. "Strategic Mobility in the Context of U.S. National Defense Strategies." *Joint Force Quarterly* 107 (4th Quarter): 75–84. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/3197251/strategic-mobility-in-the-context-of-us-national-defense-strategies/.

CISA (Cybersecurity and Infrastructure Security Agency). 2024. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* Technical report. February 7, 2024. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a.

CJCS (Chairman of the Joint Chiefs of Staff). 2022. *Universal Joint Task List Program.* Technical report CJCSI 3500.02C. Washington, DC: U.S. Department of Defense. https://www.jcs.mil/Portals/36/Documents/Doctrine/training/cjcsi_3500_02c.pdf.

CJCS (Chairman of the Joint Chiefs of Staff). 2023. *Mission Assurance Construct Implementation.* Technical report CJCSI 3209.01A. Washington, DC: U.S. Department of Defense. https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203209.01A%20(JS-221219-T8WP)%20VDJS%20Signed.pdf.

Corbari, George, Neil Khatod, John Popiak, and Pete Sinclair. 2024. "Mission Thread Analysis: Establishing a Common Framework in a Multi-discipline Domain to Enhance Defensive Cyberspace Operations." *The Cyber Defense Review* 9 (1): 42–50. https://www.jstor.org/stable/48770663.

DoD (U.S. Department of Defense). 2018. *Mission Assurance (MA),* DoD Directive 3020.40. U.S. Department of Defense, Washington, DC. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/302040p.pdf.

DoD (U.S. Department of Defense). 2022. *National Defense Strategy.* U.S. Department of Defense, Washington, DC. https://apps.dtic.mil/sti/trecms/pdf/AD1183514.pdf.

Dougherty, Chris. 2023. *Buying Time: Logistics for a New American Way of War.* Technical report. Washington, DC: Center for a New American Security. https://www.cnas.org/publications/reports/buying-time.

Harknett, Richard J., Michael P. Fischerkeller, and Emily O. Goldman. 2023. *Cyber Persistence Theory: Redefining National Security in Cyberspace.* Oxford: Oxford University Press.

HQDA (Headquarters, Department of the Army). 2017. *Army Commands, Army Service Component Commands, and Direct Reporting Units.* Technical report Army Regulation 10-87. Washington, DC.

HQDA (Headquarters, Department of the Army). 2024. *Mission Thread Defense.* Technical report Training Circular 3-12.2.90. Washington, DC.

Hughes, Zachary. 2024. "Giving Our 'Paper Tiger' Real Teeth: Fixing the U.S. Military's Plans for Contested Logistics Against China." *Joint Force Quarterly* 115 (4th Quarter): 38–47. https://digitalcommons.ndu.edu/joint-force-quarterly/vol115/iss3/20/.

Jabbour, Kamal, and Jenny Poisson. 2016. "Cyber Risk Assessment in Distributed Information Systems." *The Cyber Defense Review* 1 (1): 91–102. https://www.jstor.org/stable/26267301.

Jaikaran, Chris. 2024. *Salt Typhoon Hacks of Telecommunications Companies and Federal Response Implications.* Technical report. Congressional Research Service, November. https://crsreports.congress.gov/product/pdf/IF/IF12798.

Joint Chiefs of Staff. 2022a. *Cyberspace Operations.* JP 3-12. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. 2022b. *Joint Campaigns and Operations.* JP 3-0. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. 2023a. *Joint Homeland Defense.* JP 3-27. Washington, DC: Joint Chiefs of Staff.

Joint Chiefs of Staff. 2023b. *Joint Logistics.* JP 4-0. Washington, DC: Joint Chiefs of Staff.

Klug, John, and Steve Leonard. 2025. "Introduction." In *Professionals Talk Logistics: Sustaining Strategy and Operations,* edited by John Klug and Steve Leonard, 1–10. Havant, UK: Howgate Publishing.

Klug, Jon. 2023. "Establishing the Realm of the Possible: Logistics and Military Strategy." *Military Strategy Magazine* 9 (1). https://www.militarystrategymagazine.com/article/establishing-the-realm-of-the-possible-logistics-and-military-strategy/.

Libicki, Martin C. 2012. "Cyberspace Is Not a Warfighting Domain." *I/S: A Journal of Law and Policy for the Information Society* 8 (2): 321–36.

Lin, Herbert S. 2010. "Offensive Cyber Operations and the Use of Force." *Journal of National Security Law & Policy* 4 (1): 63–86. https://nationalsecurity.law.georgetown.edu/wp-content/uploads/2010/08/06_Lin.pdf.

Maschmeyer, Lennart. 2021. "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security* 46 (2): 63–90. https://doi.org/10.1162/isec_a_00418.

McQuade, Mike. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Nakashima, Ellen, Yeganeh Torbati, and Will Englund. 2021. "Ransomware Attack Leads to Shutdown of Major U.S. Pipeline System." *The Washington Post* (May 8, 2021). https://www.washingtonpost.com/business/2021/05/08/cyber-attack-colonial-pipeline/.

NIST (Standards, National Institute of, and Technology). 2021. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* NIST Special Publication 800-160, Volume 2, Revision 1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1.

Pape, Robert. 1996. *Bombing to Win: Air Power and Coercion in War.* Ithaca, NY: Cornell University Press.

Parfomak, Paul W., and Chris Jaikaran. 2021. *Pipeline Cybersecurity: Federal Programs.* Technical report. Congressional Research Service, September 9, 2021. https://crsreports.congress.gov/product/pdf/R/R46903.

Rovner, Joshua. 2020. "Cyberspace and Warfighting." In *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 85–104. Newport, RI: Naval War College Press.

Segal, Adam. 2025. "China Has Raised the Cyber Stakes: The 'Salt Typhoon' Hack Revealed America's Profound Vulnerability," January 21, 2025. https://www.foreignaffairs.com/united-states/china-has-raised-cyber-stakes.

Smeets, Max. 2022. *No Shortcuts: Why States Struggle to Develop a Military Cyber-Force.* London: C. Hurst & Co. Ltd.

Thomas, Ria. 2024. "Redefining Cyber Resilience: Through the Risk Register Lens." *Journal of Business Continuity & Emergency Planning* 18 (1): 75–83.

van Ovost, Jacqueline D. 2022. "Statement of General Jacqueline D. Van Ovost, United States Air Force Commander, United States Transportation Command Before the Senate Armed Services Committee On the State of the Command," March 29, 2022. https://www.armed-services.senate.gov/download/van-ovost-statement-03/29/2022.

Warner, Michael. 2020. "A Brief History of Cyber Conflict." In *Ten Years In: Implementing Strategic Approaches to Cyberspace,* edited by Jacquelyn G. Schneider, Emily O. Goldman, and Michael Warner, 21–38. Newport, RI: Naval War College Press.

Zetter, Kim. 2014. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* New York: Broadway Books.

Received 14 March 2025; Revised 29 October 2025; Accepted 7 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 99-114
https://doi.org/10.55682/cdr/sgyw-5r5p

PROFESSIONAL COMMENTARY

Toward a Global Framework for Cyber Threat Intelligence Sharing

Diane M. Janosek*

Janos LLC, USA

Establishing a trusted global framework for cyber threat intelligence (CTI) sharing is essential to collective cyber resilience, deterrence, and defense. The lack of a global framework for CTI sharing hampers timely prevention of, and response to, cyberattacks. Governments, allies, and the private sector must collaborate across borders to establish secure, standardized, and legally compliant mechanisms for CTI exchange. Policy disparities and resistance to change remain key obstacles. This article examines essential elements of effective CTI sharing—data security with validation, anonymization, and authorization— and proposes trust-based practices that can be implemented within existing legal frameworks. As cyber threats grow in sophistication and complexity, routine, responsible CTI sharing must become a global norm. International and U.S. law permit such cooperation, enabling nations and organizations to enhance resilience, protect critical infrastructure, and strengthen collective defense. Transparent, trusted sharing not only improves cyber readiness but also projects power by enabling allies to deter adversaries and deny them the element of surprise.

Keywords: power projection, cyber threat intelligence (CTI), information sharing, cyber resilience, collective defense, international law, trust frameworks, deterrence

* Corresponding author: diane@dianejanosek.com

INTRODUCTION

In 2025, the global strategic landscape is constantly transforming, characterized by shifting international alliances, emerging and cooling conflicts, and changes in U.S. leadership expectations and policies. As the U.S. Department of War (DoW) focuses on its core warfighting mission, its ability to project power globally has become critically dependent on the successful cyber defense of critical infrastructure at the civil-military seam. This critical defensive mission falls largely to civilian agencies, the private sector, and international partners, making their collective resilience a critical component of national power. To meet these demands, the U.S. and its treaty allies, along with close security partners in Europe and the Indo-Pacific, should advocate for a clear, legal, and workable blueprint for CTI sharing.

In the United States, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-150, *Guide to Cyber Threat Information Sharing*, is the standard that defines CTI (cyber threat information) and its associated concepts. It defines CTI as "any information that can help an organization identify, assess, monitor, and respond to cyber threats. [CTI] includes indicators of compromise; tactics, techniques, and procedures [TTPs] used by threat actors; suggested actions to detect, contain, or prevent attacks; and the findings from the analyses of incidents" (NIST 2016, ii). NIST SP 800-150 provides foundational guidelines for organizations to establish goals, develop rules, and effectively participate in CTI sharing communities. NIST SP 800-61r3, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, later adapted the definition of CTI (cyber threat intelligence) to refer to "threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes" (NIST 2025). For the purposes of this paper, CTI refers to the actionable knowledge derived from collecting and analyzing threat data, which provides the necessary context for an organization to make informed decisions to predict, prevent, and mitigate cyberattacks. CTI for purposes of this article does not include traditional intelligence, such as human intelligence or signal intelligence, for which their intelligence is under the ownership, control, and direction of the respective nation-state government.

NIST SP 800-160 Volume 2, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach* defines cyber resilience as the ability to maintain required capability in the face of adversity (NIST 2021, 65). As such, based upon the ability and need to maintain a certain level of defensive posture, one could view resilience as a dynamic state (Guttieri 2025). Similarly, coordinated CTI sharing is a practice intended to deter adversaries, demonstrate readiness through allied joint responses, and shape the cyber environment by denying attackers the element of surprise.

This article asserts that by understanding and simplifying legal frameworks, diminishing fear, and fostering trusted CTI sharing mechanisms, nations and industries can overcome

political and operational barriers to cyber defense collaboration. Effective CTI sharing directly enhances cyber resilience and enables power projection in the classic sense – assured movement from fort to port to theatre – by ensuring the availability, trustworthiness, and synchronization of digital systems that run rail, air, and sea lift, terminals, pipelines, distribution nodes, and weapons systems.

The article begins with a discussion of the need for CTI sharing and introduces prevalent frameworks, and then proceeds in parts. First, it defines the legal and policy mandates shaping CTI sharing in the United States and the European Union, while acknowledging areas of uncertainty. Second, it addresses implementation, focusing on data security and validation, anonymization, and authorization. Third, it evaluates structural and practical challenges to implementation. The article concludes by reaffirming the strategic necessity of CTI sharing for resilience and power projection.

THE NEED FOR CTI SHARING

Effective cyber defense requires shared situational awareness across the entire digital ecosystem, a state unachievable by any single entity operating in isolation. CTI sharing creates this collective understanding by disseminating critical digital artifacts, such as IoCs and adversary TTPs, that inform stakeholders on what to look for and what defensive measures to implement. Early dissemination of CTI is paramount, as it allows defenders to proactively address threats before they can fully materialize, transforming one organization's detection into another's prevention. This proactive, collaborative posture is especially vital for protecting critical infrastructure, where the consequences of a successful attack can cascade across society, impacting everything from financial stability to public safety.

From a military perspective, when allies and industry effectively share CTI, mission commanders are better able to keep to schedules, reduce friction at strategic mobility nodes, and avoid cascading delays. In other words, they can deliver the right forces, equipment, and munitions to the fight on time. Failure not only reduces resilience and ability to project power but also risks mission accomplishment and endangers the warfighter.

Allied states and their industries operate under different statutory and regulatory frameworks, complicating cross-border and public-private CTI exchange. As a general rule, practitioners appreciate the clarity in rules and trusted processes, as expectations are stated upfront (*Washington State Department of Licensing v. Cougar Den, Inc.* 2019). Clear expectations and clear consequences for not meeting expectations can therefore improve the overall effectiveness of CTI sharing (Feinman 2014, 527–529). Establishing CTI sharing functions in an organization requires an abundance of resources, including highly skilled practitioners and trained professionals (Berndt and Ophoff 2020).

Entities Coordinating CTI Sharing

In the U.S., non-profit Information Sharing and Analysis Centers (ISACs) have been established as member-driven organizations to facilitate CTI sharing within specific critical infrastructure sectors and sub-sectors. The National Council of ISACs was formed in 2003 and currently coordinates between 28 sector-specific ISACs. The Council strives to maximize the flow of information between owners and operators of private-sector critical infrastructure, as well as with the government. ISACs help protect facilities, personnel and customers from cyber and physical security threats and other hazards by maintaining situational awareness throughout the sector (National Council of ISACs 2025). The European counterpart is a government-appointed multi-national non-governmental organization (NGO) called Connect2Trust, which facilitates CTI sharing between governmental and private sources. Thus, on both continents, an intermediary acts as a broker and organizer of CTI sharing and disclosure processes. The utility and effectiveness of the structure, operation, and development of ISACs are the subject of ongoing research (Buckley et al. 2024).

CTI Sharing in Action

Although ISACs and NGOs had been established to provide valuable services, cyber events such as NotPetya in 2017 and SolarWinds in 2020 exposed their limitations. They highlighted the need for smaller, more agile trust communities that operate without a third-party intermediary. Such groups, built on carefully vetted membership, could share real-time information on adversary tactics, trends, and actors with greater agility. The NotPetya and SolarWinds incidents illustrate how delays in detection and disclosure allowed adversaries to amplify damage across industries and borders.

NotPetya initially targeted Ukrainian systems before cascading worldwide, demonstrating the need for international CTI dissemination to manage crises. Early indicators of malware release and spread were available, but the lack of timely cross-border exchange further exposed multinational companies such as Maersk and FedEx, which sustained billions of dollars in damages. The total global damage from NotPetya is estimated at more than $10 billion (Greenberg 2018). Furthermore, it was reported that the National Security Agency (NSA) was aware for five years that security breaches had released the EternalBlue hacking tool that Russian hackers employed on NotPetya, but had not shared the information globally or with Microsoft, the company most directly affected (Nakashima and Timberg 2017).

In the 2020 SolarWinds compromise, the Russian Foreign Intelligence Service (SVR) corrupted a routine and trusted Orion software update to create a backdoor for their espionage. The compromise affected roughly 18,000 Orion customers, including numerous governments and commercial enterprises. Slow detection and uneven disclosure across sectors allowed the campaign to persist for months, suggesting that more agile and trusted CTI sharing might have reduced its impact (Bueno 2021). The U.S. Government Accountability Office (GAO)

cited federal agencies' technical and bureaucratic information-sharing restrictions, lack of a centralized forum for communication, and limited evidence collection as having led to undesirable outcomes in the SolarWinds response (GAO 2022).

Although it found fault with many aspects of the SolarWinds response, the GAO also noted some ways in which CTI was effective in that case. Where there was cooperation, the GAO found that federal agencies more quickly identified the scale of the incident and were able to provide increased access to patching. The collective response also provided a valuable opportunity for the government and the private sector to build mutual trust in a critical moment (33–34).

The response to global disruptions caused by the Emotet and Trickbot botnet campaigns are two examples of effective international responses enabled by CTI sharing. The take down of the Emotet botnet in 2021 was the result of a coordinated, years-long multinational effort (Department of Justice 2021). European Union (EU) agencies Europol (for law enforcement cooperation), Eurojust (for criminal justice cooperation), and UK's National Crime Agency facilitated the sharing of technical indicators, including server locations, IP addresses of infected hosts, and malware update routines. This information enabled multiple countries to coordinate legal and technical actions in real time, playing a key role in taking down the global botnet. Without cross-border CTI and judicial cooperation, Emotet would likely have persisted (Bisson 2021). Its takedown is often cited as a model for future international cyber operations (Europol 2021).

In the months leading up to the 2020 U.S. elections, United States Cyber Command and industry partners disrupted one of the world's largest botnets, TrickBot, from attacking American targets. The disruption was not just a crime-fighting action but also a matter of national security (Vavra 2020). The U.S. Department of the Treasury (2023) identified TrickBot's alignment with Russian objectives and members' ties to the Russian SVR. The botnet's command and control (C2) servers were distributed across multiple countries. Legal orders were obtained in several jurisdictions instructing internet service providers (ISPs) to cut off communications and block access to the content on the botnet's servers. Microsoft's Digital Crimes Unit led the takedown in coordination with industry partners (ESET, Symantec, the Financial Services ISAC, ISPs, telecom providers) and governmental entities, including cybersecurity emergency response teams (CERTs) and law enforcement. Intelligence sharing was critical; partners exchanged C2 server IP addresses, domains, malware samples, infected host telemetry, and actor TTPs (Microsoft Threat Intelligence 2020). Microsoft used this intelligence to obtain a U.S. court order, which allowed the lawful seizure of TrickBot infrastructure inside the United States. At the same time, global partners synchronized sink-holing, server takedowns, and domain blocking actions abroad.

Highlighted by these examples, real-time sharing of intelligence, tactics, trends, and known adversarial actors in cyber defense is necessary to stay ahead of cyber adversaries. National

security and economic security are bolstered by solidified multinational cross-sector collaboration within established trust communities (Europol 2021).

LEGAL AND POLICY MANDATES

As countries and partners aspire to share CTI, it is crucial to consider the common denominators of international frameworks and the legal standards they must meet. Partners and trusted circles that share CTI must adhere to these frameworks and standards to ensure compliance with international law. This section surveys U.S. and EU legal instruments most relevant to CTI sharing; it does not attempt a comprehensive global survey. Where appropriate, it notes implications for close allies in other regions. The author has found nothing in U.S. and international law that prohibits CTI sharing. There are minimum standards and expectations for sharing CTI established by the initiatives and mandates described in the following sections.

European Union

The EU's approach to CTI sharing is built upon a triad of key regulations. The NIS2 Directive mandates a standard level of cybersecurity across critical sectors. It facilitates voluntary threat information exchange, while the Digital Operational Resilience Act (DORA) provides a more specific framework to ensure the operational continuity of the financial industry. Both of these frameworks operate under the strict data privacy requirements of the General Data Protection Regulation (GDPR), which governs the lawful processing of any CTI that contains personal data.

EU Directive 2022/2555, known as the NIS2 Directive (Network and Information Systems), establishes a unified legal framework to enhance cybersecurity in 18 critical sectors across the EU. It also calls on member states to implement national cybersecurity strategies and collaborate with the EU for cross-border reaction and enforcement (European Commission 2025). Compared to its predecessor, the NIS2 Directive expands the scope of 'essential' and 'important' entities. It strengthens incident-reporting obligations for these entities, which enhances CTI sharing by establishing timelines for early warnings and incident notifications. The EU Agency for Cybersecurity (ENISA) supports the implementation of NIS2 as part of its mandate and work program (European Union Agency for Cybersecurity 2023). NIS2 incidents reported by one sector of essential services can be a valuable source of threat intelligence for others (European Commission 2025).

DORA is a regulation introduced by the EU to harmonize and strengthen the digital resilience of information and communications technologies (ICT) supporting the financial sector. An EU regulation is directly applicable law across all EU member states, and it went into effect in January 2025 (EU DORA 2023). For the financial industry, DORA acts as a sector-specific law that takes precedence over the more general NIS2 Directive. The regulation establishes a comprehensive framework built on five key pillars: ICT risk management, incident management

and reporting, digital operational resilience testing, ICT third-party risk management, and information sharing arrangements. DORA explicitly encourages financial entities to establish arrangements to voluntarily exchange CTI to bolster collective resilience (EU DORA 2023). Given that banking security is critical to market confidence and the daily operation of the economy, sanctioned CTI sharing is vital for proactive defense and operational continuity.

GDPR establishes uniform data-protection standards across the EU and sets conditions for lawful processing and cross-border transfers, controlled by the individual member states (European Union 2018). As of May 25th, 2018, individual data privacy is a fundamental right in all EU member states. GDPR's harmonized rules give organizations legal certainty about how to share and give individuals control of their data through enforceable rights. The GDPR contains 173 detailed recitals that explain the purpose, context, and intent, and 99 binding, enforceable articles, or rules. Although transfers within the European Economic Area (EEA), consisting of the EU plus Iceland, Liechtenstein, and Norway, are treated as domestic, transfers from the EEA to non-EEA countries require a valid international transfer mechanism. These include Standard Contractual Clauses (SCCs)—the EU's model data-protection clauses—accompanied by transfer impact assessments and supplementary measures such as strong encryption with EU-held keys.

Sharing is GDPR-compliant when the processing has a lawful basis, respects purpose limitation and data minimization, and applies appropriate security. Thus, CTI sharing should be structured to reduce or avoid the inclusion of protected personal data. For example, in the author's experience, reports can pseudonymize user identifiers by hashing emails or hostnames, or by aggregating event details. Instead of raw log lines detailing specific IPs, user identifiers, or exact timestamps, CTI reports might summarize using an Autonomous System Number (ASN) to identify a network on the internet (such as a cloud provider) and then summarize activity per hour.

United States

The United States CTI sharing regime is anchored by the Cybersecurity Information Sharing Act of 2015, referred to as CISA 2015, which provides liability protections to encourage voluntary, bidirectional threat intelligence exchange between the private sector and the government (De et al. 2025). This framework is operationally managed by the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security. This incentive-based system is underpinned by foundational standards from NIST, whose frameworks guide organizational security practices. For sectors like the Defense Industrial Base (DIB), participation is further structured by mandatory compliance programs such as the Cybersecurity Maturity Model Certification (CMMC), which verifies that contractors meet the required NIST standards to protect sensitive government information.

The U.S. government encourages industry to share both information and threat data to enhance resilience and preparedness (National Security Agency 2023). The former Director of NSA, General Paul Nakasone, stated at page 5 of the 2023 Report: "Our intelligence and cybersecurity relationships with our allies and partners are a strategic asset that will increasingly factor into our competition with our rivals, especially in technological competition." NSA increasingly advocates for public-private partnerships.

CISA operates voluntary no-cost programs that facilitate near real-time sharing through its Automated Indicator Sharing (AIS) platform. CISA also provides liability protections that encourage industry partners to share actionable CTI with the government in ways that protect sources and methods (De et al. 2025). CISA's liability protection for industry partners' sharing CTI with the government includes an immunity provision. This provision is recommended for consideration by all trusted partners and their home countries to facilitate sharing without fear, provided certain parameters are met.

U.S. DoW's CMMC 2.0 is a tiered cybersecurity program for defense contractors (Department of Defense Chief Information Officer). CMMC 2.0 maps required practices to the NIST security control families, which are categories of related security requirements, including access control, incident response, and system and information integrity. These obligations shape how contractors collect, store, share, and retain sensitive cyber data (Department of Defense Chief Information Officer; NIST 2016). The DoW Chief Information Office (CIO) requires its vendor base to satisfy CMMC 2.0 requirements within a defined timeline in order to conduct defense business with the DoW. This CMMC 2.0 certification dictates how Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) must be managed and defines requirements for how it can be shared. Under CMMC 2.0, handling data of higher sensitivity and classification triggers increasingly rigorous standards. The levels range from 1 to 3, with level 3 being the most strenuous in terms of achieving and sustaining the security of the DIB (Department of Defense Chief Information Officer). The CMMC 2.0 requirements align with NIST compliance standards and frameworks, which aid in both alignment and assurance of compliance in storing, handling, and sharing of data (NIST 2016).

Implications of the Transatlantic Divide

While both the U.S. and EU frameworks aim to enhance collective cyber defense through the voluntary exchange of CTI, they are built on fundamentally different philosophies. The U.S. model is incentive-based, using the liability shields in CISA 2015 to remove legal barriers and encourage market-driven, public-private collaboration. Contrast this to the EU philosophy which employs a regulatory, top-down approach through the NIS2 Directive, which includes cybersecurity mandates for critical entities to create a trusted, harmonized ecosystem where structured, voluntary sharing can occur. This distinction reflects the differences between the U.S. and EU approaches.

The Center for Strategic and International Studies (CSIC) published an article, "U.S.-EU Tech Tensions: Escalation or Diffusion?", characterizing the differences in cultural attitudes toward technology regulation:

> The European Union governs primarily through the precautionary principle, which is the idea that technologies should not be deployed until proven safe for public use. The United States, on the other hand, has pursued an approach more closely aligned with the "move fast and break things" ethos, wherein technology is deployed and then regulated later if deemed harmful (CSIS 2025).

This fundamental divergence in international CTI frameworks is a microcosm of a broader transatlantic divide over the regulation of modern digital technology. This systemic friction impedes global cooperation. The EU's precautionary, ex-ante approach, which seeks to regulate technologies like artificial intelligence (AI) and protect intellectual property before widespread harm can occur, clashes with the U.S.'s more ex-post, market-driven model that prioritizes innovation and addresses harms after they arise. This conflict is playing out as a form of economic warfare, characterized by threats of retaliatory tariffs and competing standards for critical technologies like semiconductors. Thus, U.S. digital technology export controls create highly dynamic and complex geopolitical dilemmas that complicate CTI sharing. This regulatory battleground extends directly into the Indo-Pacific, where key allies are forced to navigate between the competing U.S. and EU models, further fragmenting the digital ecosystem and creating legal and technical barriers that prevent the seamless, trusted CTI exchange necessary for a truly effective global defense.

Lastly, mutual interest enhances collective cyber defenses, economic security, and national security of all partners, especially with allies. According to *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Rule 5 specifies that nation-states cannot use their cyber infrastructure in a manner that will produce adverse consequences to another nation-state (Schmitt 2013, 11–12), and it follows that partners in a trusted community should likewise not seek to harm a partner's infrastructure or reputation.

ENHANCING INTERNATIONAL CTI SHARING AND COORDINATION

Enhancing international CTI sharing and coordination will require more than navigating these complex geopolitical dilemmas and disparate regulatory frameworks; other tensions must also be addressed—for example, between GDPR data-minimization requirements and some U.S. sharing practices, and between differing breach-notification timelines. These frictions can be mitigated through technical and procedural safeguards such as anonymization, pseudonymization, role-based access, and clear purpose limitations documented in a sharing agreement (NIST 2016). Entities operating critical infrastructure or supporting national security should structure CTI exchange around a set of common principles, including establishing a lawful basis to process and share, data minimization and anonymization, ensuring secure

transfer and storage, defining clear decision rights and accountability mechanisms, and consulting local counsel for outlier jurisdictions.

The *Journal of Cybersecurity* recently published an article promoting research on CTI sharing. The authors, Abraham, Bélanger, and Daultrey (2025), observed that the "unique nature of CTI, where the fusion of raw threat data with human insight [occurs], distinguishes itself from other forms of information exchange, complicating traditional models of data sharing".

Key Pillars for International CTI Agreement Implementation

Successful implementation of international CTI sharing will require three key ingredients: data security and validation, anonymization, and authorization to maintain and share. These key pillars of implementation are derived from the author's experience as a deputy CISO and CEO, and the sharing of CTI best practices for an effective program.

Data Security with Validation. All participating entities must demonstrate a clear commitment to maintaining the integrity and accuracy of shared data. Such due diligence is essential to prevent false positives and reduce alert fatigue within cybersecurity operations. Prior to dissemination, contributors should conduct fundamental validation checks to ensure data reliability. This due diligence includes confirming that indicators are current and functioning correctly (for example, verifying that a detection rule triggers an alert in a controlled environment); ensuring that the observed activity is corroborated across multiple data sources (such as device logs, network logs, and centralized logging systems); verifying that traffic from shared gateways is not being double-counted; and confirming that timestamps are properly synchronized and aligned across all sources.

Anonymization. Masking sensitive data that companies and individuals want to keep secret and that cannot be traced to the original source is key. Trusted partners must agree to anonymization unless exigent circumstances exist. The exceptions and exigent circumstances should include definitions and scenarios, along with collaborative processes for swift resolution. Emergencies evolve quickly. One challenge of anonymization is that the affected entity or victim can still be identified in high-profile incidences or breaches. This has been confirmed to the author by the Federal Bureau of Investigation. This risk remains even if all parties adhere to anonymization protocols. This risk has been confirmed to the author by Connect2Trust, an official public-private information sharing entity in the Netherlands. Another concern for effective anonymization is attribution. Members of the trusted community should agree, in addition to not sharing anonymized data, that they will similarly not disclose attribution without explicit permission. Likewise, issues related to disclosure outside of the trusted community are lessons learned from the author, FBI, and Connect2Trust.

To ensure consistent and legally sound coordination, participating entities should establish clear decision rights, specifying which legal determinations fall within their authority and under what conditions a quorum is required. In addition, organizations should define escalation paths and notification timelines governing when and how CTI may be shared beyond the trusted community. Establishing these protocols in advance helps prevent uncertainty and delays during time-critical events. The incorporation of pre-built decision trees further enhances responsiveness by enabling automated or semi-automated decision-making in complex situations. As noted in recent research by BytePlus (2025), automating decision processes through decision trees and other AI-driven mechanisms has become "an essential component of modern cybersecurity strategy," allowing security teams to maintain agility and outpace malicious actors in an evolving threat environment.

Authorization. Authorization is a key tenet in privacy law and regulation. Each member must have explicit authorization to possess and disseminate the CTI under applicable law and contracts. Authority may be either blanket (standing authorization under the charter) or case-specific (per-incident approvals). Government entities, which are often bound by records and classification rules, must be distinguished from private firms, which are alternatively bound by contract, privacy, and procurement law. Secondly, each member needs to explicitly authorize or not authorize the trust community to reveal details of any incident. Having clear roles and boundaries will ensure the community is self-regulated and behaves as expected, thereby sustaining trust. The trusted community agreement will include non-disclosure agreements and should also provide detailed elaboration on authorization. For example, in the United States, under HIPAA, an entity must obtain the individual's written authorization for any use or disclosure of protected health information that is not for treatment, payment, or health care operations. Strict handling rules apply to access and authorization, as well as strict prohibitions on sharing beyond consent provided (U.S. Department of Health and Human Services 2025).

Practical Considerations

Moving from theoretical frameworks to operational reality requires addressing a series of practical considerations to build durable and effective CTI sharing communities. This involves proactively establishing clear agreements that define the scope and membership of the trusted community, creating the necessary legal and financial incentives to foster sustained collaboration, and formalizing processes for handling sensitive information. These foundational steps are essential for building the trust and operational agility required to outpace modern cyber threats.

Agreement upfront. Holistic agreements should be developed in advance to align the interests of the trusted partners. These agreements may be scoped for a sector or location or tailored

to address the unique needs of more complex organizations. The shared functionality of the trusted community matters, so narrowing the scope of partners and data types will streamline CTI sharing and increase timeliness and efficacy. Businesses with the largest market share, and thus utmost cyber risk, will benefit because cyber criminals tend to focus on businesses with the same or similar services and thus target and repeat tactics. The trusted partners will benefit, as will the overall resilience of the entire sector increase. For example, the Office of the Director of National Intelligence confirmed in 2024 that Iran-affiliated criminals and pro-Russia cyber actors gained access to and manipulated critical US industrial control systems (ICS) in the food and agriculture, healthcare, and water and wastewater sectors in late 2023 and 2024. These attacks highlight sector-focused malicious attacks (Director of National Intelligence 2024).

Organizations that cover multiple geographies (countries, provinces, or otherwise) or span multiple sectors may desire to establish and participate in cross-geographical or cross-sector CTI-sharing organizations and sharing agreements. According to Connect2Trust of the Netherlands, a proposal is circulating in the EU to consider these sorts of partnerships for 'organizationally complex' businesses. This CTI trusted community could, if desired, partner with non-profits, NGOs, or governmental entities. The trusted community could act as one "entity" in sharing. Single-entry of CTI for complex organizations will help avoid the additional work of deduplication and promote expediency and clarity. This is not yet on the radar in the United States. However, there may be an appetite as global harmonization is a long-term goal for many stakeholders in the CTI sharing ecosystem.

State secrets. A universal agreement among trusted partners should include provisions for handling state secrets or information related to national security that may be uncovered during CTI sharing, if the parties anticipate this challenge based on the sensitivity and criticality of the business. While challenging, this information would need to be submitted to the appropriate government authority for oversight as the privilege permits the government to withhold information from disclosure when its release would jeopardize national security interests such as implicating classified operations or intelligence sources (Cassman 2015). In the context of CTI sharing, the doctrine presents both a safeguard and a constraint: it protects sensitive methods and data from exposure yet can also inhibit the transparency and collaboration essential to building collective cyber resilience. Balancing the protection of state secrets with the need for trusted cross-sector CTI exchange remains a critical policy and legal challenge. Establishing clear guidelines for declassification, anonymization, and authorized sharing can help reconcile national security imperatives with the broader goal of global cyber defense.

Aligned incentives and immunity protection. Private companies should be encouraged to share CTI with incentives that increase their willingness to collaborate. Companies would be compensated through tax credits, benefits, or other forms of compensation deemed appropriate. Without market incentives, the private sector will see less investment in CTI sharing, weakening its effectiveness. The importance of incentives were discussed decades ago in a hearing of the United States House Select Committee on Homeland Security:

> In homeland security, private markets do not automatically produce the best result. We must therefore alter the structure of incentives so that market forces are directed toward reducing the costs of providing a given level of security for the nation, instead of providing a lower level of security than is warranted. Given the significance of the private sector in homeland security settings, structuring incentives properly is critical (Orszag 2003).

Creating incentives for cross-border CTI sharing is a greater challenge. One idea is for governments to provide tax incentives to organizations for sharing CTI within sanctioned operational trusted communities. Trusted partner agreements should provide legal immunity if certain approvals can be given. Further, encouraging companies to share more effectively and legally will be seen as an added protection measure. More exploration and research are needed so that the most effective incentive structures can be defined, evaluated, and achieved through strategy, diplomacy, and advocacy.

Based on the author's direct experience, it is critical that participation is agreed to in advance. Tightly held, smaller, and highly trusted partner arrangements are likely to be most effective. Trust between people is the key ingredient in life (Science News Today 2025). A tightly woven trust community may not need intermediary brokers, the absence of which may, in some cases, increase agility, effectiveness, sustained trust, and consistent sharing.

CONCLUSION

Establishing a robust framework for CTI sharing is no longer optional—it is a strategic necessity as adversaries grow more sophisticated and persistent. Nations and organizations that prioritize structured, lawful CTI exchanges strengthen collective defense, enhance the security of global commerce, and reinforce national resilience. Existing international and domestic legal frameworks provide a foundation for cooperation rather than a barrier, though occasional restrictions on the disclosure of certain vulnerabilities must be addressed through policy refinement. With appropriate safeguards for data protection, anonymity, and accountability, both public and private entities can leverage CTI sharing to mitigate risks and improve situational awareness across sectors.

Trusted, authorized partners must institutionalize these mechanisms to protect critical infrastructure and economic stability. As the digital battlespace continues to evolve, proactive,

transparent, and trust-based CTI sharing remains central to deterring adversaries, safeguarding the global digital ecosystem, and projecting credible cyber power. Future policy efforts should focus on harmonizing cross-border CTI governance, while research should explore operational models that translate trust and accountability into sustained, multinational collaboration.

ABOUT THE AUTHOR

Dr. Diane M. Janosek is a dedicated cybersecurity leader, board member, and author. As CEO of Janos LLC, she leverages her law degree and PhD in Cyber Leadership to focus on the intersection of law, policy, and technology. Areas of expertise include data policy, cyber law, compliance, governance, space security, and privacy. Dr. Janosek served as a member of the U.S. Defense Intelligence Senior Executive Service (SES) for 12 years with leadership roles at the National Security Agency, to include Commandant of the National Cryptologic University, Deputy Director of Compliance, Chief Information Security Officer, and other legal, policy, and executive management positions. She also served as Chief Legal Officer of the Privacy and Civil Liberties Oversight Board, and Legal Counsel at both the White House and the Pentagon. Dr. Janosek holds a Master of Science in Strategic Intelligence from National Intelligence University, is admitted to the U.S. Supreme Court, and is certified in information and network security (CISSP) and ethics and compliance (LPEC). Dr. Janosek is highlighted in *The Dawn of Cyber Warfare* and *Women Know Cyber* documentaries and is on the Board of Advisors for the Military Cyber Professionals Association.

REFERENCES

Abraham, C., F. Bélanger, and S. Daultrey. 2025. "Promoting research on cyber threat intelligence sharing in ecosystems." *Journal of Cybersecurity* 11 (1): yaf016. https://doi.org/10.1093/cybsec/tyaf016.

Berndt, A., and J. Ophoff. 2020. "Exploring the Value of a Cyber Threat Intelligence Function in an Organization." In *Information Security Education. Information Security in Action,* edited by Lynn Drevin, S. Von Solms, and M. Theocharidou, 579:106. IFIP Advances in Information and Communication Technology. Cham: Springer.

Bisson, David. 2021. "Emotet Botnet Infrastructure Disrupted in International Takedown." Cybereason. https://www.cybereason.com/blog/emotet-botnet-infrastructure-disrupted-in-international-takedown.

Buckley, Ruth, Liliana Pasquale, Bashar Nuseibeh, and Markus Helfert. 2024. *A Review of Cyber Information Sharing in Information Sharing Analysis Centres (ISACs).* SSRN Working Paper. https://doi.org/10.2139/ssrn.4770617.

Bueno, Felipe. 2021. "Solarwinds Attack." Belfer Center for Science and International Affairs, June 21, 2021. https://www.belfercenter.org/publication/solarwinds-attack.

BytePlus. 2025. "What Decision Trees Means for Cybersecurity," August 22, 2025. https://www.byteplus.com/en/topic/471640?title=what-decision-trees-means-for-cybersecurity.

Cassman, Daniel. 2015. "Keep It Secret, Keep It Safe." *Stanford Law Review* 67 (May): 1173. https://www.stanfordlawreview.org/wp-content/uploads/sites/3/2015/05/67_Stan_L_Rev_1173_Cassman.pdf.

CSIS (Center for Strategic and International Studies). 2025. "U.S.-EU Tech Tensions: Escalation or Diffusion?" Center for Strategic and International Studies, September 10, 2025. https://www.csis.org/analysis/us-eu-tech-tensions-escalation-or-diffusion.

De, Rajesh, Stephen Lilley, Howard W. Waltzman, Sasha Keck, and Aaron Futerman. 2025. *Cybersecurity Information Sharing Act of 2015 Lapses.* MayerBrown, October 3, 2025. https://www.mayerbrown.com/en/insights/publications/2025/10/cybersecurity-information-sharing-act-of-2015-lapses.

Department of Defense Chief Information Officer. *Cybersecurity Maturity Model Certification (CMMC) Model Overview.* version 2.13. Department of Defense Chief Information Officer, September 2024. https://dodcio.defense.gov/Portals/0/Documents/CMMC/ModelOverview.pdf.

Department of Justice. 2021. *Emotet Botnet Disrupted in International Cyber Operation.* Press Release. Justice.gov, January 28, 2021. https://www.justice.gov/archives/opa/pr/emotet-botnet-disrupted-international-cyber-operation.

Director of National Intelligence. 2024. *Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems, November 2023–April 2024.* DNI.gov.

EU DORA. 2023. "Digital Operational Resilience Act (DORA)." esma.europa.eu. https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/digital-operational-resilience-act-dora.

European Commission. 2025. *NIS2.* Website. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

European Union. 2018. "General Data Protection Regulation (GDPR)." https://gdpr-info.eu/.

European Union Agency for Cybersecurity. 2023. *NIS Directive 2 | ENISA.* Website. Europa.eu. https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/cybersecurity-policies/nis-directive-2.

Europol. 2021. "World's most dangerous malware EMOTET disrupted through global action." https://www.europol.europa.eu/media-press/newsroom/news/world%e2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action.

Feinman, Jay. 2014. "Good Faith and Reasonable Expectations." *Arkansas Law Review* 67:525–570. https://law.uark.edu/alr/PDFs/67-3/ALR-67-3-525-570Feinman.pdf.

GAO (Government Accountability Office). 2022. *Cybersecurity: Federal Response to SolarWinds and Microsoft Exchange Incidents.* GAO-22-104746. January 13, 2022. https://www.gao.gov/products/gao-22-104746.

Greenberg, Andy. 2018. "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," August 22, 2018. https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Guttieri, Karen. 2025. "Fighting through Disruption: Reframing Cyber Resilience for Power Projection and Strategic." *The Cyber Defense Review* (August). https://doi.org/10.55682/cdr/egvf-mkys.

Microsoft Threat Intelligence. 2020. "Trickbot Disrupted." Microsoft Security Blog, October 12, 2020. https://www.microsoft.com/en-us/security/blog/2020/10/12/trickbot-disrupted/.

Nakashima, Ellen, and Craig Timberg. 2017. "NSA Officials Worried about the Day Its Potent Hacking Tool Would Get Loose. Then It Did." *The Washington Post* (May 16, 2017). https://www.washingtonpost.com/business/technology/nsa-officials-worried-about-the-day-its-potent-hacking-tool-would-get-loose-then-it-did/2017/05/16/50670b16-3978-11e7-a058-ddbb23c75d82_story.html.

National Council of ISACs. 2025. *National Council of Information Sharing and Analysis Centers.* https://www.nationalisacs.org.

National Security Agency. 2023. "2023 Cybersecurity Year in Review," December 19, 2023. https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3621654/nsa-publishes-2023-cybersecurity-year-in-review/.

NIST (National Institute of Standards and Technology). 2016. *Guide to Cyber Threat Information Sharing.* NIST Special Publication 800-150. Gaithersburg, MD: National Institute of Standards and Technology, October. https://doi.org/10.6028/nist.sp.800-150.

NIST (National Institute of Standards and Technology). 2021. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* NIST Special Publication 800-160 Vol. 2 Rev. 1. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1.

NIST (National Institute of Standards and Technology). 2025. *Incident Response Recommendations and Considerations for Cybersecurity Risk Management.* NIST Special Publication 800-61 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology, April. https://doi.org/10.6028/nist.sp.800-61r3.

Orszag, Peter. 2003. *Critical Infrastructure Protection and the Private Sector: The Crucial Role of Incentives - Testimony before the Subcommittee on Cybersecurity, Science, and Research & Development and the Subcommittee on Infrastructure and Border Security.* House Select Committee on Homeland Security. https://www.brookings.edu/wp-content/uploads/2016/06/20030904-1.pdf.

Schmitt, Michael N. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Cambridge: Cambridge University Press. https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE.

Science News Today. 2025. "Why Trust is the Foundation of Every Strong Relationship (And How to Build It)," August 30, 2025. https://www.sciencenewstoday.org/why-trust-is-the-foundation-of-every-strong-relationship-and-how-to-build-it.

U.S. Department of Health and Human Services. 2025. "Summary of the HIPAA Privacy Rule." HHS.gov. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html#authorize.

U.S. Department of the Treasury. 2023. "The United States and United Kingdom issue historic joint cyber sanctions," February 9, 2023. https://home.treasury.gov/news/press-releases/jy1256.
Vavra, Jeff. 2020. "Cyber Command, Microsoft Take Action against TrickBot Botnet before Election Day." CyberScoop, October 12, 2020. https://cyberscoop.com/trickbot-takedown-cyber-command-microsoft/.
Washington State Department of Licensing v. Cougar Den, Inc. 2019. Legal Case. 586 U.S. (2019). https://www.justice.gov/d9/briefs/2018/05/16/16-1498_washington_state_dept_of_licensing_ac_pet.pdf.

Received 14 January 2025; Revised 17 October 2025; Accepted 5 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 115-138
https://doi.org/10.55682/cdr/p1ty-dmdy

RESEARCH ARTICLE

Ensuring the Cyber Resilience of Critical Infrastructure Serving Domestic Military Installations: Questions for Senior Leadership

James X. Dempsey*, Andrew J. Grotto

Stanford University, Stanford, CA, USA

Department of War (DoW) installations in the United States are heavily dependent for electricity, natural gas, drinking water and wastewater treatment, telecommunications, and rail transportation on critical infrastructure owned and operated by contractors, whether inside or outside the fence. The availability of these services is controlled by operational technology (OT) that is uniquely vulnerable to cyberattack. The regulatory structure for U.S. critical infrastructure cybersecurity is spotty, with jurisdiction divided among federal, state, and local governments. Assets inside-the-fence fall outside the utility regulatory structure entirely. DoW can use its procurement power, through contract clauses or requirements, to improve the cybersecurity of the OT in the critical infrastructures it depends on. However, there is no contract clause for the OT of utilities outside the fence, and the standard that DoW currently relies on for utilities inside the fence was not designed for OT. Key questions need to be addressed by senior leadership, beginning with a survey of the OT of utilities to identify internet-capable products or configurations, the presence of China-made equipment, and the use of OT devices with known security vulnerabilities. The DoW needs to accelerate the development of contract clauses or requirements that specify a set of prioritized controls for OT.

Keywords: cybersecurity, resiliency, procurement, operational technology, critical infrastructure

* Corresponding author: jdemps@stanford.edu

POWER PROJECTION DEPENDS ON CONTRACTOR-OWNED AND -OPERATED CRITICAL INFRASTRUCTURE

Department of War (DoW) installations in the United States—our "readiness platforms" to fight and win wars—depend upon civilian critical infrastructure for essential services.[1] Installations use procurement contracts to buy electricity, natural gas, drinking water, wastewater treatment, telecommunications, rail transportation and other services from non-DoW providers outside the fence. These span a range of business models, including investor-owned utilities, non-profit cooperatives, and bureaus or departments of municipalities or regional governments.

In addition to purchasing critical utility services from commercial providers outside the fence, the DoW has a long-running program of privatizing and expanding inside-the-fence services, including electricity generation and storage, drinking water distribution, and wastewater treatment. Often the entities that build and operate on-base capacity are the same utilities that operate off-base. DoW has invested and is continuing to invest billions of dollars to improve the resilience of these on-base assets through investments in backup capacity and efficiency (DoD Comptroller 2023, 2024).

Whether on-base or off, critical infrastructure serving domestic military installations operates within a cyber-contested environment, exposed to adversaries seeking to disrupt the deployment of military resources by interrupting the critical utility services necessary for timely operations. "A sophisticated adversary can disrupt force deployment and cause units to miss the Required Delivery Date (RDD) by targeting commercially owned critical infrastructure and local municipal sectors" (Army Cyber Institute 2021, 42).

The Army's Critical Infrastructure Dependencies Are Easy to Map

Detailed information about outside-the-fence critical infrastructure service providers for Army installations is easily found online using basic to intermediate open-source research techniques. Information about inside-the-fence infrastructure is patchier but often discoverable through open-source methods as well. As a proof of concept, our graduate research assistant compiled detailed (unpublished) dossiers on two Army installations, focusing on their electricity, natural gas, water, and freight rail dependencies.

The research drew on a mix of publicly available resources, including documents posted on the installations' websites; local, state, and federal environmental and other reports; government databases at all levels; corporate press releases and news articles; and open-source maps and satellite images. For example, the U.S. Energy Information Administration's

1. The phrase "readiness platforms" was used by a senior leader at an Army installation we visited as part of our research for this article.

Energy Atlas includes a map of electric generation facilities and transmission lines, giving anyone a starting point for identifying the resources that serve DoW installations (EIA, n.d.).

The dossiers assembled by our graduate student included maps, descriptions of specific equipment, and supply chain dependencies. The student was even able to identify one critical infrastructure provider's use of a specific industrial control system with a known, internet-facing vulnerability (later patched). Each dossier took an estimated 20-30 hours to develop. We assume that adversaries have spent more time than that and have complied dossiers of much greater depth. (We do not address here the reasons why so much information about critical infrastructure is readily available from public sources.)

Adversaries Are Pre-Positioning in Domestic Critical Infrastructure, with Intent

In February 2024, federal agencies warned that cyber actors sponsored by the People's Republic of China had pre-positioned themselves on the networks of U.S. critical infrastructure with the goal of conducting disruptive or destructive cyberattacks in the event of a major crisis or conflict with the United States (CISA 2024f). Earlier, Russia too was found in U.S. critical infrastructure (CISA 2018), and there have been several successful, albeit small-scale, Iranian attacks on local water supply systems. In 2024, it became apparent that the PRC state-sponsored group known as Salt Typhoon had burrowed deep into America's telecommunications networks, listening to audio calls in real-time and obtaining call records data on millions of users (Sanger and Barnes 2024; CISA 2025).

The intent of America's adversaries to use infrastructure compromise to support their military objectives has been on display throughout Russia's campaign against Ukraine, beginning in 2015 and continuing, though largely unsuccessfully, through the 2022 invasion (Colling 2024; Mueller et al. 2023). The threat has come directly to the doorstep of the U.S. military: In October 2024, American Water Works Company, a public utility that supplies drinking water and wastewater treatment services to 18 DoW installations in the U.S., reported that it had discovered "unauthorized activity" in its computer systems (Industrial Cyber 2024). While the company said that none of its water or wastewater facilities or operations had been negatively impacted, it did not specify the number or nature of systems affected or provide any details about the attack vector. Among the company's contracts with the U.S. military is a 50-year agreement to operate water and wastewater utility services for the Army Garrison at West Point (American Water 2025).

One threat vector is the presence in U.S. critical infrastructure of equipment made in China. For example, 80% of the ship-to-shore cranes at U.S. ports were produced in China. Many of these cranes are internet-connected, meaning that, by design, they may be controlled, serviced, and programmed from remote locations and thus are vulnerable to cyberattack (U.S. Coast Guard 2024). From 2006 through 2023, the U.S. imported almost 450 electrical transformers from China. Of these, more than 360 were the large transmission system transformers

necessary for the operation of the grid. The U.S. has also imported from China hundreds of millions of inverters, many with internet connection features, used in solar panels, electric grids, manufacturing, and water and wastewater systems (Weiss 2024). On-base resources are not immune. Projects intended to "island off" DoW installations from dependency on commercial networks may themselves use products made in China (Select Committee on the Chinese Communist Party 2024).

Awareness of the cybersecurity risks of China-made products has grown in recent years, but regulatory responses have emerged more slowly and only on a sector-by-sector basis, with major gaps. China-made switches are now banned from U.S. telecommunications networks, and a mandate to rip-and-replace the huge embedded base of China-made switches is underway, at a cost just shy of $5 billion (FCC 2025). In contrast, there is no option to rip-and-replace China-made ship-to-shore cranes, because there are no feasible alternative sources, so the regulatory response focuses on risk mitigation (U.S. Coast Guard 2024). It has been reported that the Department of Energy (DoE) has been examining electric power equipment for security vulnerabilities (Mcfarlane 2025), but the scope and outputs of the reviews have not been made public and in any case there is no regulatory mandate to heed them. A 2020 DoE order that prohibited certain utilities from procuring specific bulk power equipment from China was revoked in 2021 (DoE 2021). While China is a major supplier of equipment used in drinking water systems (Shinde 2025), we could find no program specifically aimed at vetting China-made devices in drinking water infrastructure.

THE UNIQUE VULNERABILITY OF OPERATIONAL TECHNOLOGY

Whether a critical infrastructure asset is on-base or off-base, it relies on operational technology (OT). OT systems, also called industrial control systems (ICS), measure and control vital parameters of physical devices essential to the operation of real-world processes (NIST 2023, 8). OT systems control electricity generation and distribution, oil and natural gas pipelines, drinking water and wastewater systems, and rail systems, among many others. A cyberattack on an OT system could transfer control over these critical parameters to the attackers, enabling malicious alteration that could cause malfunction or even total system outage (Microsoft Threat Intelligence 2024).

Many OT systems lack security measures. They often contain legacy products that are no longer supported by vendors and cannot be patched or updated to protect against new vulnerabilities (NIST 2023, 37). As the Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) warned in 2020, "Legacy OT assets that were not designed to defend against malicious cyber activities, combined with readily available information that identifies OT assets connected via the Internet … are creating a 'perfect storm' of 1) easy access to unsecured assets, 2) use of common, open-source information

about devices, and 3) an extensive list of exploits deployable via common exploit frameworks …" (NSA and CISA 2020).

"Forget the myth of the air gap"

Traditionally, OT devices had no connectivity and the air gap between OT and an enterprise's information technology (IT) infrastructure was relied on as the primary guarantor of OT security. That has long since changed. Many OT systems are now routinely connected to corporate networks via Ethernet, Internet Protocol, and wireless devices. (One of the challenges of critical infrastructure cybersecurity is that often no one fully knows how the OT and IT of a given system are connected or could be connected.) While this integration supports new capabilities, it significantly reduces isolation for OT from the outside world, making components discoverable by attackers through internet scanning tools (NIST 2023, 28) and increasing the likelihood that their vulnerabilities can be exploited by determined adversaries.

It is likely that even on-base capabilities have network connections that allow remote access, despite the DoW's goal of "islanding" its installations from public networks. As long ago as 2011, Stefan Woronka, Siemens' director of Industrial Security Services, said, "Forget the myth of the air gap – the control system that is completely isolated is history" (Byres 2011). As another analyst concluded, "The benefits of remote access connections into ICS are so significant that many organizations now rely on these types of connections in their day-to-day operations" (Mathezer 2021). Adding to the problem, the discovery of rogue communication devices embedded in some China-made solar power inverters (Mcfarlane 2025) suggests that connectivity features can be secretly built into products that are assumed to have no such capability.

And yet, security frameworks for OT still recommend air-gapping. Unified Facilities Code (UFC) 4-010-06, the DoW's standard for cybersecurity of the control systems of on-base facilities, states, "Do not allow control systems to be publicly accessible over the Internet," but in the very same sentence it recognizes that internet connectivity is a reality, saying, "if this capability is required, it must be restricted access and carefully implemented by IT professionals" (DoD 2023).

The vulnerability of OT systems is evidenced by the steady stream of alerts and advisories issued by CISA announcing newly discovered flaws in ICS devices (CISA, n.d.[b]). Not infrequently, OT devices use default passwords or are not even password-protected (Swidch 2024; CISA 2023, 2024e). Others do not protect the integrity of messages during transmission, either by utilizing strong encryption or implementing other sufficiently mitigating controls (CISA 2024b). One industrial control product that was the subject of a recent CISA advisory (CISA 2024c) has four software vulnerabilities attributable to weaknesses on the list of the 25 most dangerous software weaknesses compiled by the MITRE Corporation (2024). Microsoft reported in 2023 that 78% of industrial network devices monitored by Microsoft Defender for

IoT (Internet of Things) had known vulnerabilities (Microsoft 2023). Many of these devices had default passwords or no passwords at all. On top of these product flaws, human operators may fail to implement controls, such as robust passwords, override or disable security features, misconfigure systems, or take other actions that render systems vulnerable (Ribeiro 2024).

Adversarial Attacks on OT: A Closer Look

In July 2020, CISA and the NSA warned that cyber actors had shown their willingness to conduct malicious cyber activity against critical infrastructure in the U.S. by exploiting internet-accessible OT (NSA and CISA 2020). In May 2024, U.S. and allied agencies warned that pro-Russia hacktivists were targeting and gaining remote access to small-scale OT systems in North American and European water and wastewater systems, dams, energy, and food and agriculture sectors (CISA 2024a). The attackers exploited modular, internet-exposed ICS through vulnerable software and human-machine interfaces, often using default passwords or guessing weak passwords. In October 2024, CISA and partner agencies warned that Iranian cyber actors were using brute force and other techniques to compromise organizations across multiple critical infrastructure sectors, including healthcare and public health, government, information technology, engineering, and energy (CISA 2024d).

An April 2024 report from Mandiant concluded that Russian hackers had infiltrated a Texas water facility and caused a system malfunction that forced a water tank to overflow (Mandiant 2024). Mandiant linked the activity to Sandworm, a hacking operation affiliated with Russia's military intelligence. This was not the first attack on a water system. In November 2023, "CyberAv3ngers," a cyber actor connected to the Islamic Revolutionary Guard Corps, attacked the Aliquippa, Pennsylvania water plant, shutting down a pressure regulation pump, requiring operators to take manual control of the system (Vasquez and Vicens 2023). In a detailed analysis, CISA and partners later warned that CyberAv3ngers were targeting and compromising an ICS device made by the Israeli manufacturer Unitronics, used not only in water and wastewater systems but also in energy, food and beverage manufacturing, and healthcare (CISA 2023). The targeted devices were exposed to the internet and were still using their default passwords.

Microsoft researchers found that other OT-focused threat actors used the same methodology in multiple other attacks: "Attackers can, and do, obtain visibility on OT devices that are open to the internet using search engines, identify vulnerable models and open communication ports, and then use the contextual metadata to identify devices that are of special interest, such as ICS systems in water plants or other critical facilities. At that point, a weak password or an outdated system with an exploitable vulnerability is all that stands between them and remote access to the system" (Microsoft Threat Intelligence 2024).

THE DOW ENERGY RESILIENCE PROGRAM

Historically, DoW built, owned, operated, and maintained its inside-the-fence utility systems. In the 1990s, however, the DoW accelerated a move to privatize its on-base utilities (Converge Strategies 2024, 9–10). The privatization effort was promoted by Congress in 1997 with the adoption of 10 U.S.C. § 2688, granting to the secretaries of the military departments the authority to convey a utility system, or part of one, under their jurisdiction to a municipal, private, regional, district, or cooperative utility company or other entity (United States Congress 1997). As of January 2017, DoW had transferred ownership of more than 600 of its electricity, water, natural gas, and wastewater utilities to private entities (GAO 2018, 2020b). (The number today is undoubtedly higher.) According to a 2024 report, investor-owned utilities serve more than 300 major military installations, while more than 125 rural electric cooperatives serve DoW installations in 41 states (Converge Strategies 2024, 10). Under this transformation, the non-DoW civilian provider is responsible for any investments required to upgrade and maintain the on-base utilities.

Congress has adopted a series of laws addressing DoW dependencies, especially with respect to energy resilience, starting at least as early as 2006 with the adoption of 10 U.S.C. § 2911, Public Law 109–364, Sec. 2851 (United States Congress 2006). As amended over the years, § 2911 directs the Secretary of War to "ensure readiness of the armed forces for their military missions by pursuing energy security and energy resilience." It encourages installations to develop energy-production infrastructure inside the fence and implement energy resilience features, such as microgrids, to ensure energy availability even when the installation is not connected to sources located off the installation. In another provision, 10 U.S.C. § 2926, Congress directed DoD to "ensure the types, availability, and use of operational energy promote the readiness of the armed forces."

Congress took a further step with Section 316 of the 2021 National Defense Authorization Act (NDAA), Public Law 116-283, codified at 10 U.S.C. § 2920: "The Secretary of Defense shall, by the end of fiscal year 2030, provide that 100 percent of the energy load required to maintain the critical missions of each installation have a minimum level of availability of 99.9 percent per fiscal year" (United States Congress 2021). "Energy" is defined as electricity, natural gas, steam, chilled water, and heated water. 10 U.S.C. § 2920 also requires that "black start" exercises be conducted to evaluate the ability of installations to perform critical missions without access to off-installation energy resources. In a "black start exercise," delivery of energy provided from off an installation is terminated before backup generation assets on the installation are turned on, to assess the ability of the backup systems to start independently, transfer the load, and carry the load until energy from off the installation is restored.

Each of the military departments has issued policies requiring critical missions to operate independently of the grid for up to 14 days (Converge Strategies 2024, 4). The law requires

the Secretary of each military department and the head of each defense agency to plan for the provision of energy resilience and energy security for installations, emphasizing the use of full-time installed energy sources rather than emergency generation. The Army has set a target requiring each installation to install a microgrid by 2035 (Converge Strategies 2024, 4).

In response, DoW is investing billions to build more energy facilities on military bases. For FY 2025 alone, the budget request included $732.2 million ($636 million in construction projects and $96.2 million in planning and design funds) to prioritize projects that support energy resilience for critical mission requirements (Owens 2024; DoD Comptroller 2024). Further information about the progress of the effort can be found in annual reports that DoD filed with Congress, at least through fiscal year 2023 (DoD 2024a).

However, from a cybersecurity perspective, efforts to expand on-base energy capacity may be irrelevant because the very same utilities that provide services from outside the fence may be selected for inside-the-fence construction and they may incorporate the very same ICS devices and China-made components that make them vulnerable outside the fence. A recent experience at Camp Lejeune illustrates the problem. In 2022, the Marine Corps awarded Duke Energy a $22 million utility energy service contract for the design and construction of a microgrid at the base (Duke Energy 2022). The project included upgraded electrical infrastructure, 5 megawatts of on-site natural gas-fired generation, a 5.4-megawatt battery energy storage system, integration of an existing solar photovoltaic system, and a microgrid controller. The project was based on the premise that, while many installations have backup generators, microgrids offer performance advantages that help operators manage the power load and everything plugged into the grid, in order to be able to redirect power to critical missions that require an uninterrupted energy supply during outages. However, Duke Energy installed batteries manufactured in China that had features making them vulnerable to remote compromise (Select Committee on the Chinese Communist Party 2024). In an effort to create on-base resilience and independence from the public grid, the Marine Corps had ended up bringing a cyber vulnerability inside the fence.

Even with these efforts and others to build inside-the-fence capacity, in 2020 the GAO estimated that nearly all military installations in the U.S. still depend on outside-the-fence providers for some of their electricity and 63 percent rely to some degree on their surrounding communities for each of five commodities: electricity, water, wastewater, telecommunications, and natural gas (GAO 2020a). Also, the 600 utilities that had been privatized as of January 2017 represented only 23 percent (601 of 2,574) of the DoD's utility systems (GAO 2018). While the number of privatized systems is certainly higher today, it seems likely that the DoW continues to own and operate substantial inside-the-fence critical infrastructure.

THE REGULATORY LANDSCAPE: A PATCHWORK QUILT, WITH MAJOR GAPS

Utilities outside the fence from which DoW acquires essential services (electricity, natural gas, water, wastewater treatment, telecommunications, and rail transportation) are governed by a patchwork of federal, state, and local regulations. Privatized utility systems on DoW installations are not regulated by utility commissions (Converge Strategies 2024, 10). The U.S. does not have a single, comprehensive cybersecurity law that applies across all sectors. Instead, it relies on sector-specific rules, some of which are based on specific statutory authority, some of which are based on pre-internet laws. Many of the sectoral cybersecurity laws and regulations that do exist—such as those for health records, for financial services data, and for federal government information systems, plus a growing number of state laws—focus solely on IT systems, not OT, and aim only to protect personal information, not the availability of the underlying services. For critical infrastructure, the regulatory framework is spotty, with significant gaps.

Electric Power Systems

Responsibility for cybersecurity of the electric power system is shared among the Federal Energy Regulatory Commission (FERC), state public utility commissions, and local governments. The Federal Power Act is one of the few federal statutes expressly granting a regulator (FERC) authority to adopt cybersecurity requirements. Working with an industry body, the North American Electric Reliability Corporation, FERC has developed and regularly updates a set of critical infrastructure protection (CIP) standards. However, these requirements apply to only part of the electric power grid, known as the "bulk electric system." Although some utilities may apply the CIPs throughout their networks, they do not formally cover smaller generation resources or the local facilities that deliver power to DoW installations. Facilities outside the scope of the FECR CIPs are subject to state and local regulation.

Natural Gas Pipeline Network

The regulatory framework for the U.S. natural gas pipeline network is likewise segmented, creating a significant jurisdictional seam between high-capacity transmission and local distribution. Following the 2021 Colonial Pipeline ransomware incident, the Transportation Security Administration (TSA) issued a series of Security Directives that impose mandatory cybersecurity and incident reporting requirements on the owners and operators of critical interstate natural gas transmission pipelines. However, the mandate of these federal directives terminates where transmission systems connect to local distribution companies (LDCs). These LDCs, which are typically regulated at the state level, manage the final delivery of gas to end-users, including military installations.

Railroads

U.S. railroad regulation is bifurcated between two primary federal agencies, creating a complex compliance landscape for rail operators. The TSA has issued security directives for freight and passenger rail. Concurrently, the Federal Railroad Administration (FRA) has issued detailed rules, standards and instructions governing the installation and maintenance of signal and train control systems, notably 49 C.F.R. Part 236, specifically including processor-based systems and components. A critical limitation of this framework, however, is that these FRA provisions are focused on the safety and reliability of traditional electro-mechanical systems and do not fully address the distinct cybersecurity vulnerabilities inherent in the newer, internet-connected OT devices that are becoming more prevalent across the rail network.

Telecommunications

In the telecommunications sector, the Federal Communications Commission (FCC) has largely left cybersecurity to voluntary industry decisions (Dempsey 2025). The FCC has a rule requiring notification to the Commission and to affected customers when there has been a breach of customer identifying information and call detail records, but the Commission has no rule aimed to protect the security of communications themselves. As of this writing, the Senate's version of the intelligence authorization act for fiscal year 2026, S.2342, includes a provision aimed at the cybersecurity of providers of telecommunications service to the intelligence community (United States Senate 2025), but there is no comparable language in the House bill and it is uncertain whether the provision will survive industry opposition.

Drinking Water and Wastewater Treatment

The federal legal framework for the safety of the nation's drinking water, including systems serving military installations, is primarily based on the America's Water Infrastructure Act (AWIA) of 2018, Public Law 115-270. Section 2013 of the AWIA, codified at 42 U.S.C. § 300i-2, required community water systems serving more than 3,300 people to conduct a one-time risk and resilience assessment and to review it every five years to determine whether it should be revised. Section 2013 also requires covered systems to develop an emergency response plan that shall include strategies and resources to improve the resilience of the system, including the physical security and cybersecurity of the system (United States Congress 2018). However, the law only obliges utilities to certify their completion of the assessment and emergency plan to the Environmental Protection Agency (EPA). It does not require submission of the assessments or plans themselves, limiting the agency's oversight of their substance and effectiveness.

Under a separate provision of the federal Safe Drinking Water Act, states are required to conduct surveys of the facilities, equipment, and operations of public water systems to evaluate their ability to deliver safe drinking water. In March 2023, the EPA attempted to

enhance this framework by issuing an interpretation that would have included cybersecurity in these state-led audits. However, several states and water sector groups challenged the rule in court, alleging the agency had exceeded its authority, and the EPA withdrew its interpretation in October 2023 (Horne and Dempsey 2023). This left only voluntary action. CISA and the EPA offer resources, threat intelligence, and technical assistance, but there are no specific federal laws or regulations requiring any cybersecurity controls for drinking water and wastewater treatment.

Executive Orders

In addition to the above, executive orders and statutes related to cybersecurity could have application to the procurement of critical infrastructure services. Exec. Order 13800 (2017), *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, requires that each agency head "shall use" the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST) "to manage the agency's cybersecurity risk," which could include the OT of critical utilities on which the agency depends. In addition, under the Federal Information Security Modernization Act (FISMA) (United States Congress 2014), the NIST Risk Management Framework (RMF) is considered mandatory for federal information systems (NIST 2018, 2016). However, we are not aware of any direct use of these authorities to regulate the OT cybersecurity of utilities providing service to the federal government. Moreover, as discussed in more detail below, the CSF and RMF are not standards but rather open-ended frameworks best thought of as planning and oversight guides that organizations can use to develop cybersecurity plans and conduct self-assessments.

A 2024 mandate from the Office of Management and Budget, based on Exec. Order 14028 (2021), *Improving the Nation's Cybersecurity*, requires developers providing software to the federal government to attest that they followed certain secure software development practices (CISA 2024g). However, this requirement applies only to software purchased by federal agencies, not to software used by the utilities from which the government purchases electric, water or other services. Exec. Order 14144 (2025a), *Strengthening and Promoting Innovation in the Nation's Cybersecurity*, included measures intended to promote the use of artificial intelligence to identity vulnerabilities in OT, but those provisions were repealed by President Trump in June 2025 with Exec. Order 14306 (2025b), *Sustaining Select Efforts To Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144*.

In addition, there is a NIST guide on OT security described in greater detail below, NIST Special Publication (SP) 800-82r3, *Guide to Operational Technology (OT) Security* (NIST 2023). It is not directly mandatory but has been relied on by the DoW for inside-the-fence utility construction.

Local Regulation

This patchwork of regulatory coverage means that the cybersecurity of critical infrastructure supplying utility services to military installations is highly fragmented. For example, in the case of Ft. Carson, the installation receives gas, electricity, water, and wastewater treatment services under a General Services Administration (GSA) area-wide contract with Colorado Springs Utilities (CSU), a municipally-owned entity. The regulator for CSU is the city council of the City of Colorado Springs. Title 12 of the Code of the City of Colorado Springs establishes certain rules for utilities under the city's jurisdiction. In addition, the city council has adopted Utilities Rules and Regulations (URR) (CSU 2024). The URR is organized into a general section, affecting all services, followed by service-specific sections: electric, natural gas, water, and wastewater service. The city council of Colorado Springs periodically reviews and approves tariffs for CSU, such as the Natural Gas Rate Schedules (CSU 2023a). Each tariff incorporates by reference a set of Line Extension and Service Standards (LESS), one each for water, wastewater, gas and electric service, written by the utility (CSU 2025, 2023b). Collectively, the URR, the tariffs, and the LESSs establish the regulations, rates, and terms and conditions for the CSU's services, including those provided to Ft. Carson.

However, we found nothing in any of these documents (the URR, the tariffs, or the Line Extension and Service Standards) that specifically addresses the cybersecurity of the OT that manages the operation of the electrical, natural gas, or water systems that serve Ft. Carson. Nor is there anything regarding OT cybersecurity in the City Code of Colorado Springs, city ordinances, or Colorado state statutes.

THE PROCUREMENT FRAMEWORK

In the absence of a comprehensive regulatory framework for critical infrastructure cybersecurity, the DoW can use its procurement contracts to impose cybersecurity standards on the utilities from which it procures goods and services, whether on-base or off. However, at present there is no contract clause specifically addressing OT.

To purchase electricity, natural gas, water, wastewater treatment, and steam from utilities outside the fence, the DoW normally works through the GSA. The GSA's authority to procure utility services for U.S. federal executive agencies is outlined in 40 U.S.C. § 501 (United States Congress 2002) and Part 41 of the Federal Acquisition Regulation (FAR) (GSA, DoD, and NASA 2025). GSA frequently uses a type of long-term master agreement called an "areawide public utility contract" (GSA, n.d.), which lists the terms and conditions for the specific service and incorporates all applicable federal contract clauses. Areawide contracts provide a pre-established contractual vehicle for ordering utility services. Under FAR Part 41, federal contracting officers for a particular agency and location are generally required to procure utility services through the applicable GSA areawide public utility contract. Generally, the

price of the service and other conditions are detailed in a tariff or rate schedule approved or established by a utility regulatory body (not the GSA).

Most federal government contracts—including the GSA areawide utility contracts—must include a clause requiring contractors to apply specified cybersecurity controls to their IT systems. For civilian agencies, this is FAR 52.204-21, which mandates 15 basic security controls derived from NIST SP 800-171, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations* (NIST 2024). As its name indicates, NIST SP 800-171 is aimed at IT and its purpose is to ensure that contractors implement cybersecurity controls to protect any controlled unclassified information (CUI) they receive from the government. NIST SP 800-171 is not designed for the OT that monitors and controls the physical functions associated with electricity generation, natural gas delivery, or water and wastewater systems. When the DoW obtains utility services under a GSA areawide public utility contract, it must add Clause 252.204-7012 from the DoD Federal Acquisition Regulations Supplement (DFARS), *Safeguarding Covered Defense Information and Cyber Incident Reporting* (DoD 2025), which imposes for more high-risk situations the full 110 controls in NIST SP 800-171. However, DFARS 252.204-7012, like FAR 52.204-21, does not directly address OT. Its controls are designed to protect information on IT systems, not to ensure the availability and integrity of physical processes controlled by OT.

For utility assets inside the fence, the DoW uses a variety of contract vehicles, including Utilities Privatization Contracts, Energy Savings Performance Contracts, Utility Energy Services Contracts, and contracts under the Energy Resilience and Conservation Investment Program (SERDP/ESTCP, n.d.[b]). For utility assets formerly owned by the DoW but since sold to the private sector or a local government, 10 U.S.C. § 2688 requires that they be operated in a manner "consistent with energy resilience and cybersecurity requirements and associated metrics provided to the conveyee." All Installation Energy Plans must incorporate detailed cybersecurity plans applicable to any energy projects included in the plan, including any installation or modification of OT, including control systems (SERDP/ESTCP, n.d.[b]). DoD Instruction 4715.28, *Military Installation Resilience*, cites forty-seven references (DoD 2024b).

In a 2019 memo focused on the Utilities Privatization Program (that is, inside-the-fence resources), the Undersecretary of Defense for Acquisition and Sustainment (2019) directed all DoD components to ensure that all new and existing utility service contracts included comprehensive cybersecurity requirements as outlined in twenty-one referenced DoD directives. These included DFARS Clause 252.204-7012, which, as noted, does not cover OT. They also included the UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems*, discussed in the next section.

UFC 4-010-06: the DoW's Risk Management Framework for OT

To pursue a contract-based approach to the OT security of vital critical infrastructure, the DoW needs a standard with clear, measurable and enforceable requirements. So far, the DoW has relied on NIST SP 800-82 Revision 3, *A Guide to Operational Technology (OT) Security* (NIST 2023). NIST SP 800-82 is non-prescriptive. It is a risk management framework that describes issues to be considered, but it specifies neither technologies nor outcomes. It grants considerable discretion to individual project managers.

Moreover, NIST SP 800-82 Revision 3 was not developed from the bottom up for OT specifically. Instead, it relies on three other NIST publications designed for IT systems:

- NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, which provides a framework for an enterprise-level risk management program (Joint Task Force 2011).
- NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, which provides a structured process for managing security and privacy risk, including system categorization and control selection (NIST 2018).
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, which contains a comprehensive list of cybersecurity controls for information systems and is the ultimate source for NIST cybersecurity documents (Joint Task Force 2020b). It is supplemented by NIST SP 800-53B, *Control Baselines for Information Systems and Organizations* (Joint Task Force 2020a).

NIST SP 800-82 takes the cybersecurity controls in NIST SP 800-53, designed for IT systems, and considers how they might be applied to OT using the framework of NIST SP 800-37. It is not intended to serve regulatory or enforcement purposes. It starts with an overview of OT system topologies and vulnerabilities. Like other NIST cybersecurity documents, it emphasizes management processes, such as having an OT governance strategy and an OT cybersecurity policy and communicating them effectively within the organization, coordinating and aligning OT cybersecurity roles and responsibilities internally and with external partners, and integrating cybersecurity risks into corporate risk management processes.

Appendix F, an "OT overlay," takes the NIST SP 800-53 Revision 5 security controls for information systems and considers which of them apply to OT and how, with enhancements and supplemental guidance that apply specifically to OT systems as guided by NIST SP 800-37 (the risk management framework that was also designed for IT).

The challenge for both contractors and project managers is that these NIST documents are open-ended, leaving it to users to define their own risk tolerances and even their own criteria for applying the controls. This is a feature of many NIST publications in the field of cybersecurity; they are not really "standards" but frameworks or guides that tolerate a broad

range of practices (Choi 2024). For example, the NIST SP 800-53 control for least privilege (AC-6(1)) states: "Authorize access for [Assignment: organization-defined individuals or roles] to: (a) [Assignment: organization-defined security functions (deployed in hardware, software, and firmware)]; and (b) [Assignment: organization-defined security-relevant information]," with the bracketed parts to be filled in by each organization. Similarly open-ended is AC-3: "Enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies." Of course, an organization must define its own access control policies, but an organization with dangerously generous allocation of access authorizations could comply with this control, as long as it "enforced" those authorizations.

NIST SP 800-82, for OT, piles additional discretion on top of this indeterminacy. For example, regarding the key issue of network connectivity, it recommends separating OT networks from corporate networks, expressly acknowledging that using the corporate network for OT communication could expose OT components to cyberattacks, but, at the same time, it allows networking: "Practical considerations – such as digital transformation, the cost of OT installation, or maintaining a homogenous network infrastructure – often mean that a connection is required between OT and corporate or other IT networks" (NIST 2023, 66). It allows what it considers a major security control to be bypassed in the pursuit of other interests.

Based on NIST SP 800-82, DoW has developed three reference documents for its on-base utility systems:

- UFC 4-010-06, *Cybersecurity of Facility-Related Control Systems (FRCS)* (DoD 2023). This document defines a process for identification of cybersecurity requirements suitable for control systems of any impact rating, with more specific guidance suitable for control systems of low or moderate impact level. It applies to all planning, design, construction, renovation, and repair of both new and existing facilities. The control lists in UFC 4-010-06 were generated using the NIST SP 800-82 overlay for low impact systems and the RMF Technical Advisory Group (TAG) Overlay for moderate impact systems.
- *Control System Overlay for Moderate Impact Systems*. Published by the RMF TAG, this document supplements the standard security control baseline with specialized implementation guidance for moderate-impact systems, addressing the specific vulnerabilities and requirements of OT. To further refine these standards, both the Navy and Air Force have developed their own distinct overlays to accommodate their unique control system architectures and mission-specific contexts (DoD 2023, 23).
- UFGS-25 05 11, *Cybersecurity for Facility-Related Control Systems*. This Unified Facilities Guide Specifications (UFGS) document applies broadly to control systems, but it does not specifically address electrical generation and distribution. It leaves controls for electrical power system devices blank, stating "Use this subpart if needed to add requirements for a specific control system type (e.g. electrical distribution etc.), similar to how other control

> systems are covered above" (DoD 2024c). UFGS-25 05 11 includes a set of schedules to document interconnections with other systems, communications within the network, wireless, and IP connection, along with an inventory spreadsheet intended to capture information about every device in a system for review and approval by the appropriate official (U.S. Army Corps of Engineers 2024; SERDP/ESTCP, n.d.[a]).

UFC 4-010-06 does not dictate specific controls. This is partly because the selection of controls must be based on a risk assessment that is unique to each system. Also, it is because the security control baseline that UFC 4-010-06 draws on was developed for standard information systems and contains security controls that UFC 4-010-06 itself says are inapplicable to control systems, or "are impractical to implement due to technical or resource constraints." The RMF process allows these baselines to be tailored for any given project by removing or adding specific controls, subject to final approval of the Authorizing Official.

It remains uncertain whether UFC 4-010-06 has resulted in more resilient systems. As the experience with DFARS 252.204-7012 shows, many contractors fail to implement contractually-required cybersecurity standards. Even though failure to implement these standards is a breach of contract exposing contractors to the full range of contractual remedies, up to and including contract termination, as well as liability under the False Claims Act, contracting authorities rarely go behind contractor assurances of compliance. The Cybersecurity Maturity Model Certification (CMMC) process aims to address this problem for certain contracts through third-party certification. However, CMMC applies only to IT systems. The 2019 guidance from the Undersecretary of Defense for Acquisition and Sustainment (2019) on utility service contracts mandated compliance with 21 DoD directives or memos, but there is no publicly available data on the extent to which contractors have been able to reconcile and comply with all 21 of them. Moreover, the guidance document that is perhaps most important (certainly most detailed) regarding OT security, UFC 4-010-06, is a risk management document, meaning that specific controls are required on a specific project only to the extent required by the official overseeing that project.

Cybersecurity Standards for Operational Technology

UFC 4-010-06 does not require specific controls and, as explained, the controls it discusses were not initially designed for OT. To strengthen its use of the procurement power to address the cybersecurity of the utilities it relies on, the DoW should consider using cybersecurity controls and practices specifically designed for OT systems. This can be achieved through a DFARS clause or by issuing requirements or specifications that can be added to contracts. Given the length of time required to amend the DFARS, it would probably be quicker to issue requirements or specifications. We understand that the DoW is currently developing requirements for OT that can be incorporated in contracts.

One source for such controls is the comprehensive family of standards and technical reports developed by the International Society of Automation (ISA) specifically for industrial automation and control systems. ISA standard 62443, *Security for Industrial Automation & Control Systems*, applies to all industry sectors, including electric power generation and distribution. (The International Electrotechnical Commission has adopted 62443, which is now commonly referred to as ISA/IEC 62443.) ISA/IEC 62443 is not a single document but a series, defining in a structured fashion the layers of an OT security program. It is designed around concepts central to ICS, such as security zones and conduits, and focuses on safety and operational availability, which are different priorities from those of the confidentiality-focused IT world. Within the ISA/IEC 62443 family, the most detailed reference may be Part 4-2: *Technical Security Requirements for IACS Components*. It provides detailed technical control system component requirements and organizes security into seven foundational areas: identification and authentication, use control, system integrity, data confidentiality, restricted data flow, timely response to events and resource availability.

A less comprehensive source of OT controls, but one that may offer prioritized incremental steps for a phase-in period, was published in January 2025 by CISA and a wide range of U.S. and international partners. *Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products* describes how OT owners and operators should integrate security into their procurement process when purchasing industrial automation and control systems as well as other OT products. Also, CISA has produced cross-sector cybersecurity performance goals, including a range of actionable controls (CISA, n.d.[a]), which apply to both IT and OT systems and could serve as the source of specific controls in a contract-based effort to improve the cybersecurity of critical infrastructure serving DoW installations in the U.S. Other controls and best practices specifically designed for OT have been issued by CISA (n.d.[c]), by the NSA and CISA (2020), and by the Department of Energy (DoE, n.d.).

Finally, the National Association of Regulatory Utility Commissioners (NARUC) has partnered with the U.S. Department of Energy, Office of Cybersecurity, Energy Security, and Emergency Response to develop a set of cybersecurity baselines for electric distribution systems and distributed energy resources. The NARUC baselines allow flexibility to system operators. On interconnection, they state that IT and OT networks should be separated, but they go on to say that connections may be explicitly allowed for specific system functionality, without addressing whether additional controls should be implemented to protect connected OT systems (DoE and NARUC 2020).

IMPLICATIONS FOR SENIOR LEADERSHIP

Senior DoW leadership could start advancing OT cybersecurity by posing some key questions to relevant components throughout the department:

Inventory. Is there an inventory and assessment of the DoW's critical infrastructure dependencies, with specific attention to ICS devices and internet connections? Whether an asset is inside or outside the fence–

- Is the OT of the utility connected to the internet?
- Is there a bridge between OT and the IT network of its owner or operator?
- Does the utility use ICS devices or other products made in China?
- Was Camp Lejeune the only micro-grid installed for energy resiliency that used China-made products?
- Does the utility use ICS devices for which CISA has issued a vulnerability alert or advisory?

For inside-the-fence utilities, the inventories collected pursuant to UFC 4-010-06 may be a good source of this data.

Contract Requirements. Has UFC 4-010-06 in fact been incorporated into contracts for inside-the-fence construction of energy assets?

- If it has, has anyone assessed whether and how contractors are actually adhering to its provisions?
- How many contractors subject to UFC 4-010-06 have been granted a POAM (Plan of Action and Milestones) to address cybersecurity shortfalls and has anyone assessed whether contractors are meeting them?
- Is there a set of prioritized controls that could be required of outside-the-fence utilities?
- What is the status of the DoW effort to develop OT cybersecurity requirements for critical infrastructure procurements? Can the process be accelerated?

Paying for Cybersecurity. Efforts aimed at outside-the-fence utilities will have to address the question of costs. One approach is to ensure that cybersecurity costs are classified as recoverable. The other is to build security costs into a utility's rate base so the utility can earn a rate of return on the expenditures.

The Human Factor. A major challenge in securing OT is the human element, in at least two regards. First, security standards are meaningless if they can be ignored or overridden by humans. Second, the DoW, like other government agencies and the private sector, faces a cybersecurity skills gap, including in terms of contracting officers responsible for procurement of critical infrastructure and project managers responsible for inside-the-fence construction.

- Does DoW have the skilled personnel to audit OT security for on- and off-base critical infrastructure?
- Could or should the CMMC system of third-party assessments be extended to critical infrastructure providers?

Matching Requirements to the Threat. Is there any evidence that the cybersecurity controls in UFC 4-010-06 are effective in addressing the vulnerabilities of operational technology?

- Has there been efforts to map the controls in UFC 4-101-06 to OT vulnerabilities and threats?
- Would the controls in ISA/IEC 62443 be more effective in achieving some desired level of cybersecurity?

In 2020, CISA was planning an effort to map discovered ICS vulnerabilities to product lines and configurations to understand the impact and potential consequences of specific vulnerabilities with the goal of developing configuration gold standards (CISA 2020). This effort should be revived. DoW should work though available inter-agency processes to support development of prioritized and measurable controls for OT.

CONCLUSION

Lethality depends on some pretty mundane things, such as electricity, natural gas, drinking water, and rail lines. An interruption in the availability of any one of these or other critical infrastructures could disrupt and delay force projection. Yet these services are controlled by OT that is every bit as vulnerable—possibly even more vulnerable—than the IT that has been the focus of national cybersecurity policy in recent years. On top of that, we know foreign adversaries have targeted and succeeded in gaining access to the OT of critical infrastructure. Efforts to island-off military installations with on-base capabilities may be of no avail, since inside-the-fence assets may still be connected to IT systems and the internet and may use the same vulnerable OT devices used outside the fence.

The landscape of critical infrastructure serving domestic military installations is highly complex and inconsistently governed. The U.S. legal framework for critical infrastructure cybersecurity is fragmented, with significant gaps. It is unlikely that a comprehensive system of laws and regulations for OT cybersecurity will be stitched together anytime soon.

Therefore, the DoW should use the lever that, for all its limitations, may be the most flexible and most impactful: the power to set standards for the services it purchases. The process of addressing OT cybersecurity should begin, as all cybersecurity should begin, with an inventory of assets, inside and outside the fence, to identify pathways between OT systems and the internet as well as vulnerable equipment, including not only China-made devices but also products made outside of China that contain known vulnerabilities. Such an inventory could drive mitigation efforts. It could also spur DoW efforts to develop prioritized and measurable controls for OT that can be required in critical infrastructure procurement contracts, inside and outside the fence. The field of OT cybersecurity has evolved considerably in recent years; what was once an off-shoot of IT security now has a growing library of controls and practices.

Having put so much effort into securing contractor IT with the CMMC process, DoW should give similar attention to contractor OT.

ABOUT THE AUTHORS

James X. Dempsey is senior policy advisor at the Stanford Program on Geopolitics, Technology and Governance. He also holds positions as managing director of the IAPP Cybersecurity Law Center and lecturer at the UC Berkeley School of Law. From 2012 to 2017, Dempsey served, after Senate confirmation, as a member of the U.S. Privacy and Civil Liberties Oversight Board, an independent federal agency charged with advising senior policymakers and overseeing the nation's counterterrorism programs. Other experience includes executive director of the Berkeley Center for Law & Technology, leadership positions (including executive director) at the Center for Democracy & Technology, and assistant counsel to the House Judiciary Committee. He is co-author, with John Carlin, of Cybersecurity Law Fundamentals (IAPP, 2d ed. 2024) and a frequent contributor to Lawfare. He is a graduate of Yale College and Harvard Law School.

Andrew J. Grotto is a research scholar at the Center for International Security and Cooperation at Stanford University. Previously, Grotto was the Senior Director for Cybersecurity Policy at the White House in the Obama and Trump Administrations. His portfolio included defense of the financial services, energy, communications, transportation, healthcare, electoral infrastructure, and other vital critical infrastructure sectors; cybersecurity risk management policies for federal networks; consumer cybersecurity; and cyber incident response policy and incident management. He also coordinated development and execution of technology policy topics with a nexus to cyber policy, such as encryption, surveillance, privacy, and the national security dimensions of artificial intelligence and machine learning. Grotto joined the White House after serving as Senior Advisor for Technology Policy to Commerce Secretary Penny Pritzker. Prior experience includes work on Capitol Hill as a member of the professional staff of the Senate Select Committee on Intelligence and as a Senior National Security Analyst at the Center for American Progress. Grotto received his JD from the University of California at Berkeley, his MPA from Harvard University, and his BA from the University of Kentucky.

REFERENCES

American Water. 2025. *Military Services Site Locations.* https://www.amwater.com/corp/Products-Services/Military-Services/site-locations.

Army Cyber Institute. 2021. *Jack Voltaic 3.0: Cyber Research Report.* https://cyber.army.mil/Portals/3/Documents/JackVoltaic/3.0/JackVoltaic_ResearchReport3.0.pdf.

Byres, Eric. 2011. *SCADA Security's Air Gap Fairy Tale.* Automation (August 2011). https://www.automation.com/en-us/articles/2011-2/scada-securitys-air-gap-fairy-tale.

Choi, Bryan. 2024. *NIST's Software Un-Standards.* Lawfare (March 7, 2024). https://www.lawfaremedia.org/article/nist's-software-un-standards.

CISA (Cybersecurity and Infrastructure Security Agency). 2018. *Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors.* CISA (March 16, 2018). https://www.cisa.gov/news-events/alerts/2018/03/15/russian-government-cyber-activity-targeting-energy-and-other-critical-infrastructure-sectors.

CISA (Cybersecurity and Infrastructure Security Agency). 2020. *Securing Industrial Control Systems: A Unified Initiative, FY 2019–2023.* CISA (July 2020). https://web.archive.org/web/20200909094158/https://www.cisa.gov/sites/default/files/publications/Securing_Industrial_Control_Systems_S508C.pdf.

CISA (Cybersecurity and Infrastructure Security Agency). 2023. *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities.* CISA (December 1, 2023). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a.

CISA (Cybersecurity and Infrastructure Security Agency). 2024a. *Defending OT Operations Against Ongoing Pro-Russia Hacktivist Activity.* CISA (May 2024). https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf.

CISA (Cybersecurity and Infrastructure Security Agency). 2024b. *ICS Advisory: Schneider Electric EcoStruxure Control Expert, EcoStruxure Process Expert, and Modicon M340, M580 and M580 Safety PLCs.* CISA (November 26, 2024). https://www.cisa.gov/news-events/ics-advisories/icsa-24-331-03.

CISA (Cybersecurity and Infrastructure Security Agency). 2024c. *ICS Advisory: Siemens RUGGEDCOM APE1808.* CISA (December 3, 2024). https://www.cisa.gov/news-events/ics-advisories/icsa-24-338-02.

CISA (Cybersecurity and Infrastructure Security Agency). 2024d. *Iranian Cyber Actors' Brute Force and Credential Access Activity Compromises Critical Infrastructure Organizations.* CISA (October 16, 2024). https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-290a.

CISA (Cybersecurity and Infrastructure Security Agency). 2024e. *IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities.* CISA (December 18, 2024). https://www.cisa.gov/sites/default/files/2024-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors.pdf.

CISA (Cybersecurity and Infrastructure Security Agency). 2024f. *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.* CISA (February 7, 2024). https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf.

CISA (Cybersecurity and Infrastructure Security Agency). 2024g. *Secure Software Development Attestation Form Version 1.0.* https://www.cisa.gov/sites/default/files/2024-04/Self_Attestation_Common_Form_FINAL_508c.pdf.

CISA (Cybersecurity and Infrastructure Security Agency). 2025. *Countering Chinese State-Sponsored Actors Compromise of Networks Worldwide to Feed Global Espionage System.* CISA (August 27, 2025). https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-239a.

CISA (Cybersecurity and Infrastructure Security Agency). n.d.(a). *Cross-Sector Cybersecurity Performance Goals.* CISA. https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

CISA (Cybersecurity and Infrastructure Security Agency). n.d.(b). *Cybersecurity Alerts and Advisories.* CISA. https://www.cisa.gov/news-events/cybersecurity-advisories.

CISA (Cybersecurity and Infrastructure Security Agency). n.d.(c). *ICS Recommended Practices.* https://www.cisa.gov/ics/Recommended-Practices.

Colling, Jackson. 2024. *Recapping 'Cyber in War: Lessons from the Russia-Ukraine Conflict.'* Articles of War (January 8, 2024). https://lieber.westpoint.edu/recapping-cyber-war-lessons-russia-ukraine-conflict/.

Converge Strategies. 2024. *Defense Energy Resilience Engagement Framework for Utility Regulators.* National Association of Regulatory Utility Commissioners (September 2024). https://pubs.naruc.org/pub/DB2D5176-9778-E86D-EC47-9539E5624A29.

CSU (Colorado Springs Utilities). 2023a. *City Council Volume No. 6, Third Revised Sheet No. 1, Natural Gas Rate Schedules, Resolution No. 186-23.* Approval: November 14, 2023; Effective: January 1, 2024. https://www.csu.org/Documents/NaturalGasTariff.pdf?csf=1&e=zsszBY.

CSU (Colorado Springs Utilities). 2023b. *Line Extension and Service Standards: Water.* https://www.csu.org/Documents/WaterLESS2023.pdf.

CSU (Colorado Springs Utilities). 2024. *Utilities Rules and Regulations Tariff.* Effective January 1, 2025. https://www.csu.org/hubfs/39606065/Document%20Library/UtilitiesRulesRegsTariff.pdf.

CSU (Colorado Springs Utilities). 2025. *Line Extension and Service Standards: Gas.* https://39606065.fs1.hubspotusercontent-na1.net/hubfs/39606065/Document%20Library/GasStandardBook.pdf.

Dempsey, Jim. 2025. *The MAGA Case for Software Liability.* Lawfare (February 19, 2025). https://www.lawfaremedia.org/article/the-maga-case-for-software-liability.

DoD (U.S. Department of Defense). 2023. *Unified Facilities Criteria (UFC 4-010-06): Cybersecurity of Facility-Related Control Systems (FRCS).* Whole Building Design Guide, National Institute of Building Sciences (October 10, 2023). https://www.wbdg.org/FFC/DOD/UFC/ufc_4_010_06_2023.pdf.

DoD (U.S. Department of Defense). 2024a. *Annual Energy Performance, Resilience, and Energy Report, Fiscal Year 2023.* June 2024. https://acqweb.staging.acqebiz.mil/eie/ero/ier/docs/aeprr/FY23-AEPRR-Report.pdf.

DoD (U.S. Department of Defense). 2024b. *DoD Instruction 4715.28: Military Installation Resilience.* Executive Services Directorate (December 17, 2024). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/471528p.PDF.

DoD (U.S. Department of Defense). 2024c. *Unified Facilities Guide Specifications (UFGS-25 05 11): Cybersecurity for Facility-Related Control Systems.* Whole Building Design Guide, National Institute of Building Sciences (August 2024). https://www.wbdg.org/FFC/DOD/UFGS/UFGS%2025%2005%2011.pdf.

DoD (U.S. Department of Defense). 2025. *Defense Federal Acquisition Regulation Supplement (DFARS).* Title 48, Code of Federal Regulations, Chapter 2 (48 C.F.R. 2). https://www.acquisition.gov/dfars.

DoD Comptroller. 2023. *FY 2024 Energy Resilience and Conservation Investment Program (ERCIP) Project List by State/Country,* March. https://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/07_Military_Construction/15-Energy_Resilience_and_Conservation_Investment_Program.pdf.

DoD Comptroller. 2024. *Energy Resilience and Conservation Investment Program (ERCIP) FY 2025 Military Construction, Defense-Wide Project List by State/Country,* March. https://comptroller.defense.gov/Portals/45/Documents/defbudget/FY2025/budget_justification/pdfs/07_Military_Construction/14-Energy_Resilience_and_Conservation_Investment_Program.pdf.

DoE (U.S. Department of Energy). 2021. *Revocation of Prohibition Order Securing Critical Defense Facilities.* Federal Register 86:21308 (April 22, 2021).

DoE (U.S. Department of Energy). n.d. *Cybersecurity Capability Maturity Model (C2M2) Program.* https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0.

DoE and NARUC (U.S. Department of Energy and National Association of Regulatory Utility Commissioners). 2020. *Cybersecurity Baselines for Electric Distribution Systems and DER.* NARUC (February 2020). https://pubs.naruc.org/pub/35247A70-0C45-9652-C6D9-99A77C87200F.

Duke Energy. 2022. *Duke Energy to install microgrid at Camp Lejeune.* Duke Energy News (November 10, 2022). https://news.duke-energy.com/releases/duke-energy-to-install-microgrid-at-camp-lejeune.

EIA (U.S. Energy Information Administration). n.d. *U.S. Energy Atlas: Electricity Energy Infrastructure and Resources.* https://atlas.eia.gov/apps/895faaf79d744f2ab3b72f8bd5778e68/explore.

Exec. Order 13800 (Executive Office of the President). 2017. *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.* Federal Register 82:22391 (May 11, 2017). https://www.federalregister.gov/documents/2017/05/16/2017-10004/strengthening-the-cybersecurity-of-federal-networks-and-critical-infrastructure.

Exec. Order 14028 (Executive Office of the President). 2021. *Improving the Nation's Cybersecurity.* Federal Register 86:26633 (May 12, 2021). https://www.federalregister.gov/documents/2021/05/17/2021-10490/improving-the-nations-cybersecurity.

Exec. Order 14144 (Executive Office of the President). 2025a. *Strengthening and Promoting Innovation in the Nation's Cybersecurity.* Federal Register 90:6755 (January 16, 2025). https://www.federalregister.gov/documents/2025/01/17/2025-01470/strengthening-and-promoting-innovation-in-the-nations-cybersecurity.

Exec. Order 14306 (Executive Office of the President). 2025b. *Sustaining Select Efforts to Strengthen the Nation's Cybersecurity and Amending Executive Order 13694 and Executive Order 14144.* Federal Register 90:24723 (June 6, 2025). https://www.federalregister.gov/documents/2025/06/11/2025-10804/sustaining-select-efforts-to-strengthen-the-nations-cybersecurity-and-amending-executive-order-13694.

FCC (Federal Communications Commission). 2025. *Secure and Trusted Communications Networks Reimbursement Program.* https://www.fcc.gov/supplychain/reimbursement.

GAO (U.S. Government Accountability Office). 2018. *Defense Infrastructure: Guidance Needed to Develop Metrics and Implement Cybersecurity Requirements for Utilities Privatization Contracts (GAO-18-558).* GAO (September 2018). https://www.gao.gov/assets/gao-18-558.pdf.

GAO (U.S. Government Accountability Office). 2020a. *Climate Resilience: DOD Coordinates with Communities, but Needs to Assess the Performance of Related Grant Programs (GAO-21-46).* GAO (December 2020). https://www.gao.gov/assets/gao-21-46.pdf.

GAO (U.S. Government Accountability Office). 2020b. *DOD Utilities Privatization: Improved Data Collection and Lessons Learned Archive Could Help Reduce Time to Award Contracts (GAO-20-104).* GAO (April 2, 2020). https://www.gao.gov/products/gao-20-104.

GSA (U.S. General Services Administration). n.d. *GSA Areawide Public Utility Contracts.* https://www.gsa.gov/real-estate/facilities-management/utility-services/areawide-public-utility-contracts.

GSA, DoD, and NASA (U.S. General Services Administration, U.S. Department of Defense, and National Aeronautics and Space Administration). 2025. *Federal Acquisition Regulation (FAR).* https://www.acquisition.gov/browse/index/far.

Horne, Jacob, and Jim Dempsey. 2023. *A Cyber Threat to U.S. Drinking Water.* Lawfare (December 21, 2023). https://www.lawfaremedia.org/article/a-cyber-threat-to-u.s.-drinking-water.

Industrial Cyber. 2024. *American Water Works reports cybersecurity incident following unauthorized hacker activity.* Industrial Cyber (October 8, 2024). https://industrialcyber.co/utilities-energy-power-water-waste/american-water-works-reports-cybersecurity-incident-following-unauthorized-hacker-activity/.

Joint Task Force. 2011. *Managing Information Security Risk: Organization, Mission, and Information System View.* NIST Special Publication 800-39. Gaithersburg, MD: National Institute of Standards and Technology, March. https://doi.org/10.6028/NIST.SP.800-39.

Joint Task Force. 2020a. *Control Baselines for Information Systems and Organizations.* NIST Special Publication 800-53B. Gaithersburg, MD: National Institute of Standards and Technology, October. https://doi.org/10.6028/NIST.SP.800-53B.

Joint Task Force. 2020b. *Security and Privacy Controls for Information Systems and Organizations.* NIST Special Publication 800-53 Rev. 5. Gaithersburg, MD: National Institute of Standards and Technology, September. https://doi.org/10.6028/NIST.SP.800-53r5.

Mandiant. 2024. *Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm.* Google Cloud (April 17, 2024). https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm.

Mathezer, Stephen. 2021. *Introduction to ICS Security – Part 3.* SANS (October 1, 2021). https://www.sans.org/blog/introduction-to-ics-security-part-3/.

Mcfarlane, Sarah. 2025. *Rogue communication devices found in Chinese solar power inverters.* Reuters (May 14, 2025). https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/.

Microsoft. 2023. *Digital Defense Report 2023,* October. https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

Microsoft Threat Intelligence. 2024. *Exposed and vulnerable: Recent attacks highlight critical need to protect internet-exposed OT devices.* Microsoft (May 30, 2024). https://www.microsoft.com/en-us/security/blog/2024/05/30/exposed-and-vulnerable-recent-attacks-highlight-critical-need-to-protect-internet-exposed-ot-devices/.

MITRE Corporation. 2024. *2024 CWE Top 25 Most Dangerous Software Weaknesses.* https://cwe.mitre.org/top25/archive/2024/2024_cwe_top25.html.

Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. 2023. *Cyber Operations during the Russo-Ukrainian War.* CSIS (July 13, 2023). https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

NIST (National Institute of Standards and Technology). 2016. *Federal Information Security Modernization Act (FISMA) Background,* September. https://csrc.nist.gov/Projects/risk-management/fisma-background.

NIST (National Institute of Standards and Technology). 2018. *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* NIST Special Publication 800-37 Rev. 2. Gaithersburg, MD, December. https://csrc.nist.gov/pubs/sp/800/37/r2/final.

NIST (Stouffer, Keith, Michael Pease, CheeYee Tang, Timothy Zimmerman, Victoria Pillitteri, Suzanne Lightman, Adam Hahn, Stephanie Saravia, Aslam Sherule, and Michael Thompson). 2023. *Guide to Operational Technology (OT) Security.* NIST Special Publication 800-82 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology, September. https://doi.org/10.6028/NIST.SP.800-82r3.

NIST (Ross, Ron, and Victoria Pillitteri). 2024. *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* NIST Special Publication 800-171 Rev. 3. Gaithersburg, MD: National Institute of Standards and Technology, May. https://doi.org/10.6028/NIST.SP.800-171r3.

NSA and CISA (National Security Agency and Cybersecurity and Infrastructure Security Agency). 2020. *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems.* July 2020. https://media.defense.gov/2020/Jul/23/2002462846/-1/-1/0/OT_ADVISORY-DUAL-OFFICIAL-20200722.PDF.

Owens, Brendan. 2024. *Statement of The Honorable Brendan Owens, Assistant Secretary of Defense (Energy, Installations & Environment).* Senate Committee on Appropriations, Subcommittee on Military Construction and Veterans Affairs (May 1, 2024). https://www.appropriations.senate.gov/imo/media/doc/download_testimony34.pdf.

Ribeiro, Anna. 2024. *Emphasizing key strategies and best practices for managing human behavior to enhance OT security.* Industrial Cyber (September 8, 2024). https://industrialcyber.co/features/emphasizing-key-strategies-and-best-practices-for-managing-human-behavior-to-enhance-ot-security/.

Sanger, David, and Julian Barnes. 2024. *China's Hacking Reached Deep Into U.S. Telecoms.* New York Times (November 21, 2024). https://www.nytimes.com/2024/11/21/us/politics/china-hacking-telecommunications.html.

Select Committee on the Chinese Communist Party. 2024. *Gallagher, Rubio, Murphy on Duke Energy's Decision to Decommission Camp Lejeune CATL Battery Systems.* Press Release (February 9, 2024). https://selectcommitteeontheccp.house.gov/media/press-releases/gallagher-rubio-murphy-duke-energys-decision-decommission-camp-lejeune-catl.

SERDP/ESTCP (Strategic Environmental Research and Development Program / Environmental Security Technology Certification Program). n.d.(a). *Commissioning.* https://serdp-estcp.mil/page/f7ad68b7-e8ef-11ec-9685-026db1cbe810.

SERDP/ESTCP (Strategic Environmental Research and Development Program / Environmental Security Technology Certification Program). n.d.(b). *Utility Privatization Program, Energy Projects, Third-party Financing, and Cybersecurity.* https://serdp-estcp.mil/page/f7ad7dda-e8ef-11ec-9685-026db1cbe810.

Shinde, Sonali. 2025. *Water Treatment Systems at a Crossroads: How Trade Tariffs Are Driving Cost Volatility and Strategic Realignments.* Cognitive Market Research (May 2, 2025). https://www.cognitivemarketresearch.com/blog/water-treatment-systems-at-a-crossroads-how-trade-tariffs-are-driving-cost-volatility-and-strategic-realignments.

Swidch. 2024. *Default Passwords: The Silent Threat to Critical Infrastructure.* October 1, 2024. https://www.swidch.com/resources/blogs/default-passwords-the-silent-threat-to-critical-infrastructure.

U.S. Army Corps of Engineers. 2024. *Unified Facilities Guide Specifications, Section 25 05 11: Cybersecurity for Facility-Related Control Systems.* National Institute of Building Sciences, August. https://www.wbdg.org/FFC/DOD/UFGS/UFGS%2025%2005%2011.pdf.

U.S. Coast Guard. 2024. *Issuance of Maritime Security (MARSEC) Directive 105-4; Cyber Risk Management Actions for Ship-to-Shore Cranes Manufactured by People's Republic of China Companies.* Federal Register 89:13726 (February 23, 2024). https://www.federalregister.gov/documents/2024/02/23/2024-03822/issuance-of-maritime-security-marsec-directive-105-4-cyber-risk-management-actions-for-ship-to-shore.

Undersecretary of Defense for Acquisition and Sustainment. 2019. *Supplemental Guidance for the Utilities Privatization Program.* February 7, 2019. https://sepub-prod-0001-124733793621-us-gov-west-1.s3.us-gov-west-1.amazonaws.com/s3fs-public/documents/USD%2BA%2526S%2BSupplemental%2BUP%2BGuidance%2B07%2BFeb%2B19.pdf.

United States Congress. 1997. *Pub. L. 105–85, div. B, title XXVIII, §2812(a) (Nov. 18, 1997), 111 Stat. 1992.* https://www.congress.gov/105/plaws/publ85/PLAW-105publ85.pdf.

United States Congress. 2002. *Services for Executive Agencies, Pub. L. 107–217 (Aug. 21, 2002), 116 Stat. 1079; codified at 40 U.S.C. §501.* https://www.govinfo.gov/app/details/USCODE-2020-title40/USCODE-2020-title40-subtitleI-chap5-subchapI-sec501.

United States Congress. 2006. *John Warner National Defense Authorization Act for Fiscal Year 2007, Pub. L. 109–364, §2851, (Oct. 7, 2006), 120 Stat. 2489.* https://www.govinfo.gov/content/pkg/STATUTE-120/pdf/STATUTE-120-Pg2083.pdf.

United States Congress. 2014. *Federal Information Security Modernization Act of 2014, Pub. L. 113–283 (Dec. 18, 2014), 128 Stat. 3073.* https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

United States Congress. 2018. *America's Water Infrastructure Act of 2018, Pub. L. 115–270 (Oct. 23, 2018), 132 Stat. 3765.* https://www.congress.gov/115/bills/s3021/BILLS-115s3021enr.pdf.

United States Congress. 2021. *Pub. L. 116–283, div. A, title III, §316(a) (Jan. 1, 2021), 134 Stat. 3516; codified at 10 U.S.C. §2920.* https://www.law.cornell.edu/uscode/text/10/2920.

United States Senate. 2025. *S. 2342, Intelligence Authorization Act for Fiscal Year 2026, Sec. 328, 119th Cong., 1st Sess. (2025).* https://www.congress.gov/bill/119th-congress/senate-bill/2342.

Vasquez, Christian, and AJ Vicens. 2023. *Pennsylvania water facility hit by Iran-linked hackers.* Cyberscoop (November 28, 2023). https://cyberscoop.com/pennsylvania-water-facility-hack-iran/.

Weiss, Joe. 2024. *The U.S. electric industry is not responding to cyber-vulnerable Chinese equipment.* Control (February 29, 2024). https://www.controlglobal.com/blogs/unfettered/blog/33038009/the-us-electric-industry-is-not-responding-to-cyber-vulnerable-chinese-equipment.

Received 2 February 2025; Revised 8 September 2025; Accepted 11 September 2025

✧ Exercising Resilience ✧

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 141-158
https://doi.org/10.55682/cdr/r5tj-8fph

PROFESSIONAL COMMENTARY

Voices from Cyber Yankee: Lessons for Strengthening Critical Infrastructure Cyber Protection

Sarah J. M. Lohmann[1,2], Jason C. Brown*†[1]

[1]Army Cyber Institute, United States Military Academy, West Point, NY, USA
[2]University of Washington, Seattle, WA, USA

Cyberattacks on critical infrastructure increasingly threaten national security, public safety, and economic stability. This commentary analyzes Cyber Yankee—a regional, multi-agency cyber exercise in New England (United States)—as a model exercise for the U.S. Department of War (DoW) and its partners. Drawing on perspectives from senior military and National Guard leaders, it traces the evolution of the exercise since 2014 and examines its distinctive integration of utilities and operational technology (OT) operators through a collaborative Blue–Orange Team format. The paper situates Cyber Yankee within the broader cyber Unified Coordination Group (UCG) framework and identifies opportunities to adapt its principles for active-duty operations under the Defense Support of Civil Authorities (DSCA) model. Findings highlight the enduring value of long-term public–private partnerships, the cultivation of trust and interoperability before crises, and the replicability of the UCG model for coordinated cyber response. The commentary concludes with recommendations to enhance readiness nationwide, including deeper engagement with critical-infrastructure operators in exercise design, routine practice of Request for Support and Cyber 9-Line processes, expanded OT- and ICS-focused training for Guard cyber teams, alignment of these skills within Joint Qualification Records, and the development of flexible, modular response packages that reflect real-world incident needs.

Keywords: cyber defense readiness, cyber defense exercise, U.S. National Guard cyber operations, critical infrastructure protection, unified coordination group (UCG), Operational Technology (OT) security

* Corresponding author: jason.brown@westpoint.edu
† Both authors contributed equally to this research.

INTRODUCTION

When the University of Vermont Medical Center was unable to provide critical patient services for over two weeks due to a massive cyber-attack in 2020, Emergency Services called the Vermont National Guard to help with incident response (Barry and Perlroth 2020; Leffler 2023). Responding to this kind of cyber emergency that impacts critical infrastructure was something the Guardsmen had already trained for together in a training exercise called *Cyber Yankee*. It is the involvement of the utilities and critical service operators in the exercises that makes Cyber Yankee stand apart from others.

"*There was a personal relationship between the National Guard and the municipal level and the infrastructure partners. They understood the capabilities, the experience and the exposure,*" said Col. (Ret.) Richard Berthao. "*It is not just the value of the point-in-time training. The cyber-attack on the Vermont hospital with ransomware where the Vermont National Guard helped, is a demonstration of a coordinated response of how the exercises help provide training and support for assessments and resiliency work.*"

Col. (Ret.) Berthao, then the IT Director for the Massachusetts National Guard, started Cyber Yankee in 2014 as a regional exercise among the six New England states. He designed it to simulate cyber-attacks on civilian infrastructure. Unlike traditional military cyber drills, Cyber Yankee focuses on real-world systems—power plants, water treatment facilities, hospitals, and transportation networks—that make up the systems and assets essential to national security, public health, and economic stability.

In this paper, we share a "voice from the field" that demonstrates how New England states collaborate across the public-private divide to secure and defend critical infrastructure from cyber threats. As part of the team that supported training the Unified Coordination Group (UCG) portion of the exercise, we provided unique and experimental modules on futures-oriented thinking and a roleplaying cyber tabletop workshop that generated many insightful comments about the readiness of the UCG to respond to local and state-level cyber incidents. As we will demonstrate later, personal involvement, either as an observer or as a participant, is the most impactful factor in developing the relationships that make the UCG, and Cyber Yankee, a model exercise. We also share challenges and points of friction that make this kind of collaboration *hard*, but *necessary*.

Our observations are based on semi-structured interviews with several founders of Cyber Yankee, senior cyber leaders within both Active and Guard organizations, and on personal attendance at Cyber Yankee 2025. In these conversations, we explored questions such as:

- What are best practices and coordination frameworks for active duty military to train and be prepared to provide cyber incident response together with utilities and civil institutions?

- Can the Unified Coordination Group concept as defined by CISA's recently released Cyber Incident Response Plan (CISA 2025)[1] and also practiced by Cyber Yankee serves as a model, and how can this be improved?
- Does NORTHCOM (U.S. Northern Command)[2] already have coordination frameworks in place for U.S. active duty military defense support of civil authorities that could serve as a training and preparedness model?

In addition, the authors developed and delivered hands-on workshops for participants in the Unified Coordination Group track. These workshops facilitated Chatham House rules conversations about the opportunities and challenges that arise when cyber incident response spans public, private, government, and military responsibilities, and how the collective cyber force can address these issues in the future. While Cyber Yankee is not the *only* way to train for a compromising cyber event on defense critical infrastructure, its experiments with Orange Teams, operational technology, joint and multi-national partnerships, and the Unified Coordination Group track are demonstrably worth sharing with the rest of the cyber force.

Cyber Yankee represents a distinctive innovation within the National Guard's cyber readiness program, offering realistic, experimental training that directly addresses the growing threat to critical infrastructure. Drawing on insights from participating leaders and organizers, the paper argues that the exercise's principal contribution lies in its deliberate incorporation of the Unified Coordination Group framework into regional training. Embedding this UCG component across future National Guard and interagency exercises would significantly enhance the coherence and effectiveness of Defense Support to Civil Authorities (DSCA) during complex and large-scale cyber incidents.

CYBER YANKEE: A MODEL FOR PUBLIC–PRIVATE CYBER COLLABORATION

How the Cyber Yankee Exercise Unfolds

Cyber Yankee is an annual, multi-state cyber defense exercise hosted by the National Guard across the New England region. Established in 2014, it brings together military cyber units, federal agencies, state partners, and critical infrastructure utilities to rehearse coordinated responses to complex cyber incidents. Designed to strengthen public–private collaboration and to integrate operational technology environments into training, Cyber Yankee serves as one of the most advanced regional exercises in the United States.

Cyber Yankee typically unfolds over several days and follows a structured progression from individualized training, team-level orientation, then full-scale operations. The exercise begins

1. The National Cyber Incident Response Plan (NCIRP) describes a national approach to handling significant cyber incidents. It addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents. It also describes how the actions of all these stakeholders fit together to provide an integrated response.

2. U.S. Northern Command is the Department of War combatant command responsible for homeland defense, civil support, and security cooperation within its area of responsibility, which includes the continental United States, Alaska, Canada, Mexico, and surrounding waters.

with a scenario briefing, during which cyber teams of the National Guard, utility partners, and state/federal observers receive intelligence updates, threat indicators, and operational constraints that frame the simulated crisis. The teams then move into network familiarization and baseline establishment, analyzing the exercise environment—an emulated but functionally realistic network with industrial control system (ICS) components representing power, water, and oil/gas infrastructure.

Daily activities often include situation updates, interagency coordination meetings, and facilitated discussions with observers from the Cybersecurity and Infrastructure Security Agency (CISA), U.S. Cyber Command (USCYBERCOM), state fusion centers, and private-sector utilities. The final day typically involves a culminating event—a coordinated multi-vector attack designed to stress-test response capacity—followed by an after-action review (AAR) where teams identify gaps, lessons learned, and recommendations for real-world improvements.

Cyber Yankee uses a red team (cyber adversary) vs. blue team (cyber defender) format for training the "on keyboard" skills of cyber operators. Once the exercise transitions into active play, the red team mimics real-world adversaries using tactics like phishing, malware, and exploitation of industrial control systems (ICS). Blue teams, composed of cyber units-including members of cyber protection teams (CPTs)-individuals, and civilian defenders of the National Guard, must detect, respond to, and recover from these attacks.

Blue teams also advise a unique arrangement of Orange Teams, which represent real utility operators like power and water, and must approve, deny, or request support in accordance with the current cyber national response framework. Orange teams are normally used as security educators and knowledge managers to build a culture of good code reviews and develop training workshops (Mag 2025). At Cyber Yankee, cyber response experts from an actual utility fill the Orange team and become the person receiving daily situation updates from the Blue team assigned to their sector. This framework requires that utility owners make a formal request for assistance to the National Guard just as they would in a real incident (CISA, n.d.). During this phase, participants must submit Cyber 9-Line reports, escalate incidents to federal partners, and practice collaborative decision-making under time pressure.

Exercise scenarios are structured to evaluate the effectiveness of incident response coordination [3], the robustness of legal and policy frameworks, the quality of public–private communication, and the technical resilience of Operational Technology (OT) systems. Cyber Yankee's Blue Team–Orange Team configuration has increasingly attracted participants from across the nation to play roles or assess the exercise, including officials from the U.S. Army, Air Force, Navy, Space Force, Coast Guard, Department of Homeland Security, FBI, and a range of critical infrastructure utilities. In recent years, organizers have also made deliberate efforts

3. Research on cyber defense teams provides validated metrics to assess team performance during exercises (Maennel, Ottis, and Maennel 2017; Granåsen and Andersson 2016).

to expand participation among industry partners and utilities—particularly in the energy and water sectors—to strengthen realism and foster broader engagement. Cyber Yankee also extends participation to State Partnership Program countries that are aligned to the New England states. In 2025, eleven partner nations sent participants to join Blue teams or to observe and prepare to join teams in future exercises.

Landscape of National Guard–Led and Participatory Cyber Exercises

Across the United States, comparable cyber exercises are conducted annually at the national level and in regional formats, as shown in Table 1. These cyber exercises are led either by National Guard units or are characterized by strong National Guard participation. Collectively, these initiatives reflect the varied approaches adopted across states and international partnerships to address evolving cybersecurity challenges. Each exercise is shaped by its regional context, operational objectives, and the specific capabilities of participating organizations, illustrating the adaptive nature of cyber readiness training within the United States.

While these initiatives share similar goals, Cyber Yankee remains distinctive in its integration of diverse stakeholders and experimental objectives. An international review of sixteen cyber defense exercises published in 2019 already identified Cyber Yankee as having a high level of maturity (Brajdić, Kovačević, and Groš 2021). The broader literature also contrasts multiple exercises, drawing out insights into how they differ in scope, design, and impact on cyber preparedness (Dewar 2018).

Over time, these exercises illustrate a clear evolution in U.S. and allied cyber defense readiness. Early initiatives such as *Locked Shields* (CCDCOE) and *Cyber Guard* focused primarily on building technical proficiency, multinational interoperability in simulated environments, and NATO's collective defense doctrine (Smeets 2022). Mid-decade efforts, including *Cyber Yankee* and *Jack Voltaic* (ACI 2025), expanded the scope to include public–private collaboration and the protection of critical infrastructure, highlighting the growing role of the National Guard as a bridge between federal and state authorities. More recent exercises, such as *Cyber Discovery* and *Balikatan*, demonstrate a shift toward realistic, live-network testing and international coalition building across the Indo-Pacific. Taken together, these developments reveal a trajectory from technical training toward integrated resilience-building—linking military, civil, and industry actors in a unified approach to cyber defense.

As Maj. Gen. Terin Williams, the Special Assistant to the Director of the Army National Guard for U.S. Army Cyber Matters observed: "*What sets Cyber Yankee apart from other non-Guard cyber exercises is that you have critical infrastructure partners, private, state, and local entities and the Guard*". She participated in the most recent Cyber Yankee exercise by roleplaying as an operational technology (OT) operator for the scenario's fictional city. She emphasized the importance of maintaining this collaborative model: "*That needs to continue with the other regional exercises.*"

Table 1. Chronological Overview of Major Cyber Defense Exercises Involving the U.S. National Guard and Partners

Exercise	Started	Lead / Host Organization(s)	Geographic Scope	Core Focus / Features	Recent Developments (2024–2025)
Locked Shields	2010	NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)	International	Live-fire cyber defense; multinational interoperability; complex joint operations	U.S. contingent led by West Virginia National Guard (2025); emphasis on rapid decision-making under attack (Bodker 2025).
Cyber Guard	2012	U.S. Cyber Command (CYBERCOM), DHS, FBI	National / International	Offensive and defensive operations; federal–state coordination; interagency readiness	22 countries represented (2017); globally coordinated, multi-domain training event (2025) (R. Johnson 2012; U.S. Department of War 2017).
Cyber Flag	2011	U.S. Cyber Command (CYBERCOM)	National / International	Training for Cyber Mission Force (CMF) teams; advanced defensive and offensive cyberspace operations; federal-level readiness	Cyber Flag 24-2 was the first iteration to integrate Offensive Cyberspace Operations (OCO); Guard participation occurs only when activated under Title 10.
Cyber Shield	2013	National Guard Bureau	National / State Partner Program	Education, defensive skills, and capture-the-flag events; validation of Cyber Protection Teams (CPTs)	>42 states and partner nations participating (2025) (Martin 2025; Roudabush 2025; Tarkelly 2025); expanded CPT validation framework (Estrada 2022).
Cyber Yankee	2014	Six New England State National Guards	Regional (USA)	Protection of critical infrastructure; integration of utilities and Operational Technology (OT) systems; Unified Coordination Group (UCG) training	Linked with U.S. CYBERCOM via Cyber 9-Line (2022); expanded OT simulation and interagency interoperability (2023) (Pomerleau 2022).
Jack Voltaic™	2016	U.S. Army Cyber Institute (West Point)	National / Public–Private	Cyber preparedness and critical infrastructure interdependencies; multi-city, public–private collaboration	5.0 iteration (2025) advancing toward a Homeland Defense cyber readiness ecosystem (ACI 2025).
Vigilant Guard	2017	U.S. Northern Command and State National Guards	Regional (Hawai'i / Alaska)	All-hazards incident response integrating cyber and physical disruptions	2025 exercise combined environmental and cyber crises; linked to *Jack Voltaic*™ methodology (Bedard 2025).
Cyber Tatanka	2019	Nebraska National Guard	Regional (Midwest USA)	Anomaly detection and incident response on simulated networks; collaboration with public power utilities	Continued partnerships with utilities; expanded red-team training modules (Hynes 2025).
Cyber Dawn	2019	California National Guard	Regional (West USA)	Red-vs-blue competitions; simulated attacks on public services and essential digital infrastructure	Added municipal and smart-city scenarios (2025) (A. H. Johnson 2022; Loeffler 2025).
Cyber Fortress	2022	Virginia Defense Force, 91st Cyber Brigade	State	Simulated attacks on state level infrastructure	Validation exercises for state cyber protection teams (CPT) (Puryear 2023; StateDefenseForce.com 2025).
Cyber Discovery	2022	Idaho National Guard	State / Regional	Controlled attacks on real networks; high-fidelity incident response training	Expanded to private-sector networks (2025) (Edinger 2025; Eisenbrandt 2025).
Balikatan / CYDEX	2023	Guam & Hawai'i National Guards / Philippine Armed Forces	Multinational (Indo-Pacific)	Cyber defense, threat hunting, education, and critical infrastructure protection	Ongoing CYDEX series reinforcing regional partnerships (2025) (Scott 2025; Jeney 2025).

UNDERSTANDING THE CYBER UNIFIED COORDINATION GROUP (UCG)

In 2021, the Cyber Yankee organizers increased the level of inter- and intragovernmental cooperation by formally incorporating and exercising the concept of a Cyber Unified Coordination Group (UCG)—the national mechanism through which federal lead agencies coordinate their response to a significant cyber incident. A UCG brings together the three federal leads identified in U.S. cyber incident doctrine: the FBI as the lead for threat response, CISA as the lead for asset response, and the Office of the Director of National Intelligence (ODNI) through the Cyber Threat Intelligence Integration Center as the lead for intelligence support.

When an incident affects a specific industry, the relevant Sector Risk Management Agencies (SRMAs) also join the UCG, along with state, local, tribal, territorial, and affected private-sector partners as needed. Examples of these SRMAs include the Department of Energy for the Energy Sector, the Department of Homeland Security for sectors such as Communications and Critical Manufacturing, the Environmental Protection Agency for Water and Wastewater Systems, the Department of War for the defense industrial base, and the Department of the Treasury for Financial Services.

The federal framework underpinning these roles (Table 2) was first established in Presidential Policy Directive 21 (PPD-21) on Critical Infrastructure Security and Resilience, which clarified federal and sector responsibilities and formalized the role of Sector Risk Management Agencies (Executive Office of the President 2013). Subsequent legislation, including the National Cybersecurity Protection Act of 2014 (United States Congress 2014), reinforced the need for adaptable national cyber incident response structures.

Building on this foundation, Presidential Policy Directive 41 (PPD-41) issued during the Obama administration in 2016 (Executive Office of the President 2016) defined the federal government's approach to coordinating responses to major cyber incidents and formally established the UCG as the mechanism for integrating threat, asset, and intelligence response functions. CISA's most recent National Cyber Incident Response Plan (NCIRP) (CISA 2025), further operationalizes this model, describing the UCG as the primary forum for ensuring unity of effort during a cyber crisis. By integrating a UCG-like structure into its design, Cyber Yankee provides participants with the opportunity to rehearse these national coordination processes on a regional scale and under realistic operational conditions.

According to CISA, these Sector-Specific Agencies (SSAs)—the predecessors to today's SRMAs [4]— are incorporated into a Cyber UCG whenever a cyber incident affects or is likely to affect the sectors they represent. SSAs were directed through Presidential Policy Directive 21 in 2013 to ensure that "institutional knowledge and specialized expertise about the sector" is

4. Although the 2013 Presidential Policy Directive 21 referred to federal sector-leads as "Sector-Specific Agencies (SSAs)", subsequent legislation and policy clarified and codified the term "Sector Risk Management Agencies (SRMAs).

available to the President to "carry out incident management responsibilities" and "mitigate incidents" (Executive Office of the President 2013).

Table 2 provides an overview of these key federal policies and laws—ranging from PPD-21 to the National Cyber Incident Response Plan—that establish the legal and operational foundations for the UCG model.

Table 2. Key U.S. Policy and Legal Foundations for Cyber Incident Coordination

Document	Year	Focus
Presidential Policy Directive 21 (PPD-21): *Critical Infrastructure Security and Resilience*	2013	Establishes the modern federal framework for critical infrastructure security and resilience; clarifies federal roles and defines Sector Risk Management Agencies (SRMAs).
National Cybersecurity Protection Act	2014	Requires development and regular updating of adaptable cyber incident response plans for critical infrastructure; provides statutory support for national cyber incident coordination.
Presidential Policy Directive 41 (PPD-41): *United States Cyber Incident Coordination*	2016	Defines federal agency roles in significant cyber incidents; formalizes the Unified Coordination Group (UCG) as the mechanism for integrated threat, asset, and intelligence coordination.
National Cyber Incident Response Plan (NCIRP)	2016–2024	Operational plan implementing PPD-41; details how UCGs function, including activation criteria, membership, and coordination processes for major cyber incidents.

CYBER YANKEE AND THE UCG APPLICABILITY FOR ACTIVE-DUTY FORCES

The U.S. National Guard within the UCG

Because Cyber Yankee incorporates federal, state, military, and private-sector partners, it raises the question of whether its coordination model could inform active-duty approaches to cyber incident response. Could this format work as a tool for active-duty military to train, mitigate and respond to cyber threats impacting the Department of War?

"*Yes, it can,*" said Brig. Gen. Christine Rummel, the J-6 director of cyberspace operations at the North American Aerospace Defense Command (NORAD) and USNORTHCOM. "*At the heart of all incident response, regardless of domain, is trust... The benefit of the National Guard's cyber exercises, such as Cyber Yankee, is that it builds that trust; develops tactics, techniques, and procures (TTPs); builds relationships; and develops contact rosters all before a disaster occurs so that teams are not trying to determine who is who and what capabilities are available to bring to bear on the problem set.*" Rummel's emphasis on pre-established trust highlights a core advantage of National Guard-centric training models: their ability to build interpersonal and interorganizational relationships long before a crisis.

These relationships are most effective when they are developed and exercised well in advance of a cyber incident. During the 2020 SolarWinds attack and subsequent federal response, the National Security Council did not enlist the National Guard Bureau to respond. According to one analysis, "This failure likely stemmed from a lack of knowledge of the capabilities of or the process for engaging National Guard entities" (Ihme et al. 2025). Ihme

et al. (2025) describe the actions the federal C-UCG (Cyber UCG) took in response to SolarWinds, and they point out that there was some amount of dysfunction within the federal government's post-SolarWinds reporting requirements. They state,

> Conducting regular interagency training exercises among cyber response agencies, such as the National Guard's Cyber Yankee exercise, can simulate real-world cyber responses, enhance interagency coordination and communication, and promote a culture of collaboration across all levels of government that breaks down silos and fosters transparency. Finally, by leveraging Department of War (DoW) entities under Title 32 and defense support to civil authorities, the National Guard can assist state and federal governments in cyber protection, detection, and red teaming" (Ihme et al. 2025).

This is precisely the type of assistance the National Guard is meant for.

Under the current NCIRP, CISA may serve as the executive secretariat for a Cyber UCG, coordinating with the FBI, ODNI's Cyber Threat Intelligence Integration Center, Sector Risk Management Agencies, and affected federal departments as needed (CISA 2025). National Guard support to these efforts is usually authorized under U.S. Code Title 32 (*U.S. Code* 1956b), which allows National Guard forces to remain under state control while being federally funded. Activation under Title 10 authorities (*U.S. Code* 1956a), which governs federal active-duty military forces and are used during war or national emergencies, is reserved for rare cases (see Figure 1).

One such case occurred during the COVID-19 pandemic, when Title 10 authorities were used to activate both active-duty forces and the National Guard during Operation Warp Speed: "*We were activated on Title 10 during Operation Warp Speed and deputized under DHS Title 6 to protect networks associated with the distribution of COVID [vaccines] to protect the Industrial Control Systems of American manufacturers of the vaccine,*" said Lt. Col. Peter Kurek, a member of the Massachusetts National Guard. Having been involved with the Cyber Yankee exercise for years, he noted that the level of trust developed in the exercise helped execute the mission more effectively.

Active Duty Support to Domestic Cyber Incidents

Although Cyber Yankee incorporates elements of the UCG model, active-duty involvement in domestic incidents follows a different mechanism. For missions outside the Department of War Information Network (DoWIN), USNORTHCOM operates under the Defense Support of Civil Authorities (DSCA) framework, which governs how and when DoW forces may assist civil agencies. The Cyber DSCA process includes participation from CISA, the Department of War, USCYBERCOM, and USNORTHCOM, and reflects legal authorities distinct from those used by National Guard units.

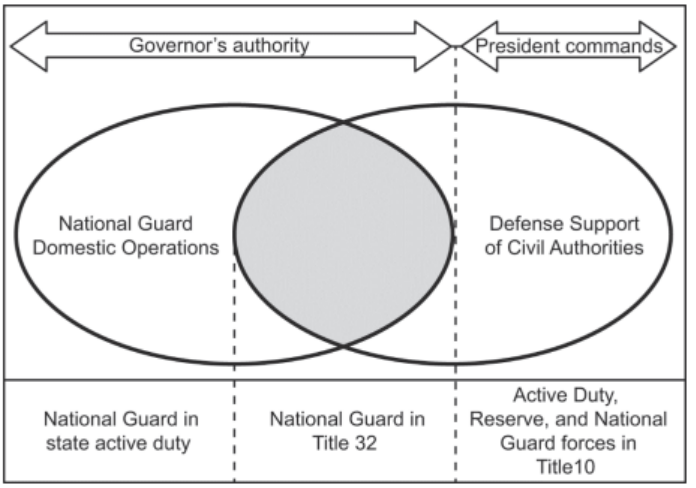


Figure 1. National Guard T10/T32 Authorities, (reproduced from Air Land Sea Application Center (2021)

.

Fortunately, the legal structure for active-duty military to support a cyber incident response effort if asked already exists. The National Cybersecurity Protection Act of 2014 (Public Law 113-282) stipulates that:

> "Federal departments and agencies, State and local governments, sector coordinating councils, information sharing and analysis organizations (as defined in section 212(5)), owners and operators of critical infrastructure, and other appropriate entities and individuals, develop, regularly update, maintain, and exercise adaptable cyber incident response plans to address cybersecurity risks (as defined in section 226) to critical infrastructure" (United States Congress 2014).

The Department of War's Role within the Cyber UCG

The Department of War's role within the Cyber UCG can be even more far-reaching. It provides cybersecurity assistance to the Defense Industrial Base, helps during civilian emergencies, and supports civil authorities. US Cyber Command, as the main cyber action arm for the DoW is directed to exercise with DoW component cyber incident response organizations, and to train their incident response teams (including assigned cyber protection teams) (DoD 2023). However, only in rare cases do active duty military provide such assistance if the impact is outside the DoWIN. An exception occurs when requested by the DoW, a federal lead agency, or the President, and provides mitigations and threat reports via the National Security Agency and the DoW Cyber Crime Center (CISA 2025).

Maj. Gen. Terin Williams emphasized this distinction, noting that the UCG model cannot be applied identically to active-duty forces because their mandates differ. Active-duty military personnel are usually asked, using DSCA authorities, to come in once for a particular industry

or utility cyber incident, whereas the National Guard maintains enduring relationships with utilities and state agencies. These longstanding partnerships, cultivated through exercises like Cyber Yankee, enable smoother coordination during an incident.

However, PPD-41 defines the UCG as "the primary method for coordinating between and among Federal agencies in response to a significant cyber incident as well as for integrating private sector partners into incident response efforts" (Executive Office of the President 2016). This means that the military, both active and Guard, should be skilled at navigating a cyber UCG during operations in which Title 10 forces are acting in a DSCA capacity.

"*Just as with any other domain or response action, participants need to understand their left and right limits, and what authority they are operating under. It's expected that if called to participate in a Cyber UCG, that the platform the personnel are responding on is off-DoWIN, where military have no authority unless requested to provide specific support,*" Brig. Gen. Rummel said.

Operating under that authority is especially important in the exercises, Lt. Col. Kurek said. "*In a realistic scenario, military members are not likely to get the direct access to a network as they do in most current exercises.… Somebody from the Guard or the military will not be allowed to touch the network in the case of an actual cybersecurity incident. To make it more realistic, you need to have more industry participation where business and utilities are at the keyboard and to transfer that knowledge from soldiers or airmen to the utilities, to industry,*" he said. "*In Operation Warp Speed, we used strategically placed sensors in the industrial networks that fed into our own monitoring tools and worked with company personnel to address detected activity.*" In this way, military responders can train, assist, and advise their industry partners.

In 2025, Army Cyber Command (ARCYBER) sent several observers from its Future Plans Directorate to examine how Cyber Yankee's methods might translate into active-duty formations. According to Col. Dave McNatt, ARCYBER's chief of plans and strategy, "*Real crisis response will almost always start off-DoWIN. [Cyber Yankee] is one of the few mature exercises that exposes Title 10 folk to the system of leaders, planners, operators, and coordinators that would deal with those incidents. Like the [ancient] Greeks taught us, you have to seek exposure to get better at your job. Without that experience, everything is theory.*" His point underscores a central benefit of Cyber Yankee: well-developed exercises provide both craft knowledge—familiarity with DSCA and UCG processes—and the practical judgment that comes only from repeated exposure to realistic, cross-sector coordination. This experiential learning is especially critical as ARCYBER expands its operational technology (OT) defense capabilities, an area that increasingly defines national-level cyber response. Col. McNatt also emphasized the broader implications for force readiness: "*There is value in [active duty] participation, but there would be even greater value if the rest of the regions in this Union did something at the same level of sophistication (and ideally, calibrated to the [Cyber Yankee] standard).*" His comments highlight Cyber Yankee's role not only as a regional exercise, but as a benchmark for the level of complexity, realism, and interagency integration needed across the country.

LOOKING AHEAD: THE FUTURE OF CYBER YANKEE

As cyber threats evolve, so will Cyber Yankee. According to Col. (Ret.) Woody Groton, who led Cyber Yankee 25's UCG training and exercising, there are three future areas within the exercise that could be war-gamed more specifically: (1) the usability of technology systems during a cyber crisis, (2) communications and operations between different agencies, and (3) state-specific cyber response plans and exercises.

In Cyber Yankee 2025, the Army Cyber Institute provided two workshops to address a whole-of-government response that is central to the UCG. The first workshop used threatcasting (Johnson and Vanatta 2017)—strategic foresight methodology used to envision and systematically plan for potential threats (typically 10 years in the future)— to imagine future scenarios in which the UCG might need to respond. These science-fact–based fictional scenarios emphasized how human factors shape incident communication. The second workshop demonstrated an experimental cyber tabletop (CTT), inspired by role-playing game mechanics, developed at the University of Indiana. This CTT used a simplified scenario involving a fictitious military installation affected by cyber disruptions in a nearby city's traffic and emergency systems, assigning participants unfamiliar roles to highlight interdependencies and the complexity of coordinated response.

Future Cyber Yankee exercises are expected to include AI-driven cyberattacks, quantum computing vulnerabilities, supply chain compromises, and deepfake-enabled social engineering. The exercise is also likely to expand its focus on resilience and recovery, ensuring that systems can not only withstand attacks but also bounce back quickly.

Technologies such as Hive IQ-a software that automates malware analysis, manages collaboration across teams of the cyber response, and keeps decision makers informed-could be tested to see how well they work during specific scenarios. In 2025, an experimental AI-enabled network sensor virtual machine was installed on the Cyber Yankee network to mirror traffic and conduct further analysis. The red team was able to test cyber effects before presenting them to blue teams (Cashman et al. 2025). These examples could include how Operational Technology operators respond to crisis and demonstrate how Cyber Yankee can serve as a testbed for AI technologies.

Communication and response across USCYBERCOM, the military, critical infrastructure entities, state governments, and the National Guard during a cyber incident could also be practiced in a more detailed manner, ensuring incident response occurs smoothly and quickly. This is a general challenge for cyber incident response. "*We need a platform for both communication and operational coordination between all parties involved in cyber incident response and right now we do not have it,*" Maj. Gen. Williams said.

Finally, specialized state-specific tabletop exercises supported by academics and legal and policy experts could help improve the training so that an actual incident response runs

more smoothly. Brig. Gen. Rummel recommended that states that do not currently have Cyber Protection Teams (CPTs), such as Alaska, would benefit from starting them. Formally established CPTs, such as those assigned to the 91st Cyber Brigade (Virginia), or Guardsmen assigned to work with state CIO/CISOs are at the frontlines of state cybersecurity protection. Every state is varied in its cybersecurity risk profile, but all states have experienced, and will continue to experience, cyber-enabled attacks and disruptions to normal operations that could be partially mitigated through prior exercising of the incident response process.

LESSONS FROM PRACTICE: CYBER YANKEE'S IMPACT ON REAL-WORLD INCIDENT RESPONSE

The Guard's Response to the UVM Medical Center Attack

The response of the National Guard to the 2020 UVM Medical Center ransomware attack illustrates how Cyber Yankee's practices translate into real-world incident response. It was based directly on the skills, relationships, and coordination patterns strengthened through the exercise. The Cyber Yankee's structure—bringing together National Guard cyber teams, state agencies, federal partners, and operators of critical infrastructure—mirrors the multi-stakeholder environment that emerged during the UVM response. Through repeated exposure to complex, multi-vector attacks and sustained coordination with private-sector operators, Guard personnel had already rehearsed the types of decisions required in large-scale recovery efforts. These included restoring compromised endpoints, reestablishing trust across hybrid IT–OT systems, and integrating with external cybersecurity contractors. During the UVM Medical Center incident, these capabilities translated into effective support as Guard teams helped review and rebuild affected systems, restore functionality in phases, and assist the hospital in reestablishing critical clinical and administrative services during the following weeks. The exercise's emphasis on UCG-style coordination also meant that Guard teams were familiar with rapid information-sharing protocols, escalation pathways, and cross-organizational communication, all of which proved essential during the hospital's prolonged recovery. In this way, the operational readiness built through Cyber Yankee materially supported the Guard's ability to assist effectively in Vermont's real-world crisis.

After the hospital networks were restored, the Vermont National Guard conducted several after-action reviews to capture lessons. The most important finding was that pre-existing relationships with UVM leadership significantly sped up response time and allowed National Guard volunteers to be available to the hospital system within 24 hours. However, not everything was as straightforward and quick as an incident response rehearsed in exercises. According to Col. (ret.) Chris Evans, who was then the unit's CIO, and dual-hatted as the state J6, the way the UVM IT staff used the Guardsmen was not the way they trained during Cyber Shield and Cyber Yankee. Instead, the team was assigned tasks according to individual skills,

rather than operating as a unified group. As a result, the Vermont Guard refined their state emergency response procedures to create different "packages" of assistance, formalizing the process to provide a tailored team or individual skill sets. They also updated their mobilization procedures to allow for flexible response packages.

Two other key lessons from the UVM incident have shaped the design of the UCG portion of Cyber Yankee. Col. Evans led the UCG training for Cyber Yankee 21, the year following UVM and noted that his experiences reinforced the move towards a civilian-led UCG model. This emphasized his observations that the military was not (and should not be) in the lead for a cyber incident response on state infrastructure, which was "*challenging for type-A people in the military,*" Evans said. "*It was in Cyber Yankee 22 when they actually started getting more civilian agencies and federal agencies... it's really hard. You do these exercises and it's so hard to have the military in the background... We're supposed to be there in a support role and you know, that's really, really hard.*" In Cyber Yankee 25, over half of the UCG attendees were civilians from federal and state agencies and regional utilities.

Scaling Cyber Yankee Insights: Recommendations for States and Regions

Cyber Yankee's evolution and successes offer several practical recommendations for other regions and for active-duty organizations seeking to enhance their cyber incident response capabilities. These recommendations translate Cyber Yankee's regionally tested practices into actionable guidance for other states, regions, and active-duty partners.

Proactively build relationships with critical infrastructure operators. Seek out, meet, and invite the leadership and cyber technicians who provide critical infrastructure services (especially power, water, gas/oil, and medical) to military installations to join conversations and exercises. Often, these have local or county offices with the responsibility to service bases. These partners can be incorporated into short, scenario-based cyber tabletop exercises (from one hour to half a day) or invited as full participants in large-scale training events. Military teams should also train utilities on the federal Request for Support (RFS) process.

Use National Guard exercises to practice real-world coordination mechanisms. Exercises should explicitly rehearse the initiation and processing of utility RFSs and the use of the Cyber 9-Line to communicate with U.S. Cyber Command. States should refine timelines for standing up a cyber UCG and share their best practices with sector-based Information Sharing and Analysis Centers (ISACs). Even small utilities—such as a one-person municipal water IT team—should understand how to initiate an RFS and who their state UCG coordinator is.

Adopt and adapt the Blue Team–Orange Team construct. When designing regional, state, or city-wide cyber exercises, replicate the Blue team / Orange team structure that pairs defensive cyber teams with utility and industry operators on their own networks. This construct teaches

cyber protection teams and incident responders about the unique operational constraints that private utilities face within their own networks.

Develop scenarios that stress Operational Technology (OT) environments. Create scenarios that force incident responders to protect OT systems. Provide training and education opportunities to Guardsmen prior to or as part of an annual exercise, such as industrial control systems and OT courses from SANS. Other scenarios might involve exercising plans for a state's defensive continuity of operations plan (COOP) or how a statewide cybersecurity service provider might integrate multi-sector challenges with OT systems.

Integrate OT Knowledge, Skills, and Abilities (KSAs) into the Joint Qualification Records (JQRs). Include OT-specific knowledge, skills, and abilities (KSAs) in appropriate Joint Qualification Records (JQRs) for cyber protection teams assigned to the National Guard. This ensures that the KSAs are aligned with the legal authorities and mission expectations to respond to a domestic cyber incident.

Build flexible mobilization and response structures. Create procedures that allow flexible mobilization and response options. If a state normally trains only as a single defensive element, or in collaboration with another state during exercises, consider how to also exercise individual mobilization requests for specialized security skills.

CONCLUSION

Despite the efforts of the National Guard, state cybersecurity teams, and even the FBI and U.S. Cyber Command, adversaries of the U.S. will still find targets to hack and exploit. This makes it all the more important for all regional National Guard entities, and the government agencies and the utilities they work with, to continue to practice close cooperation and train to defend against cyber threats to critical infrastructure. The mandate for a UCG to protect the nation's safety and security, and the regional National Guard response groups such as Cyber Yankee, has never been more urgent.

The evidence of Cyber Yankee's long-term impact will be in its replicability beyond New England and in its continued use to prepare industry, utilities, and government and state entities to respond quickly and effectively to cyber emergencies and future threats. The expertise gained through deliberate and repeated coordination, especially Cyber Yankee's unique use of the Orange Team and the exercise goals for the UCG, is achievable by active duty and the National Guard alike. Simulating real-world threats and fostering collaboration across sectors, it ensures that the nation is prepared to defend its most vital systems.

ABOUT THE AUTHORS

Dr. Sarah Lohmann teaches cybersecurity policy and emerging technology ethics at the University of Washington. She is a coauthor of the books The Weaponization of AI: The Next Stage of Terrorism and Warfare (2025), Emerging Technologies and Terrorism: An American Perspective (2024), and the editor and coauthor of the books What Ukraine Taught NATO about Hybrid Warfare (2022) and Countering Terrorism on Tomorrow's Battlefield (2022).

Lt. Col. Jason C. Brown is a research scientist and assistant professor at the Army Cyber Institute at West Point. He teaches risk management, organizational security, and systems-based decision making. As a futurist, he studies emerging threats, technological and social trends, and responses to those threats. He also leads a research team investigating critical infrastructure resilience on behalf of Army and other defense stakeholders. LTC Brown has worked within the intelligence, information operations, and cyber career fields. He has authored technical reports on the future of extremism, information warfare, cyber enabled financial crimes, microtargeting, and Chinese soft power.

ACKNOWLEDGMENTS

The authors thank the National Guard leaders, cyber operators, and emergency management professionals who shared their time and insights, as well as the Cyber Yankee organizers and participants whose collaboration and expertise made this analysis possible. The authors also extend their sincere appreciation to Prof. Carine Lallemand for the expertise and thoughtful feedback that greatly enriched the quality of this work.

REFERENCES

ACI (Army Cyber Institute). 2025. *Jack Voltaic Research Reports Series.* https://cyber.army.mil/Our-Work/Jack-Voltaic/Research-Reports/.

Air Land Sea Application Center. 2021. *Multi-Service Tactics, Techniques, and Procedures for Defense Support of Civil Authorities (DSCA).* Technical report. February 2021. https://www.alssa.mil/Portals/9/Documents/mttps/dsca_2021.pdf.

Barry, Ellen, and Nicole Perlroth. 2020. "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack." *The New York Times* (November 26, 2020). https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

Bedard, David. 2025. *Alaska National Guard Exercises Disaster Response During Vigilant Guard.* National Guard News, April 4, 2025. https://www.nationalguard.mil/News/Article-View/Article/4145804/alaska-national-guard-exercises-disaster-response-during-vigilant-guard/.

Bodker, Erica. 2025. "Locked Shields 2025: West Virginia National Guard Hosts NATO's Largest Live-Fire Cyber Resilience Exercises in the World," May 23, 2025. https://www.wv.ng.mil/News/Article/4195018/locked-shields-2025-wva-guard-hosts-natos-largest-live-fire-cyber-resilience-ex/.

Brajdić, Ivona, Ivan Kovačević, and Stjepan Groš. 2021. "Review of National and International Cybersecurity Exercises Conducted in 2019." In *International Conference on Cyber Warfare and Security,* 28–36. Reading, UK: Academic Conferences International Limited. https://doi.org/10.34190/IWS.21.034.

Cashman, William, Chasen Milner, Michael Houle, Michael Jones, Hayden Jananthan, Jeremy Kepner, Peter Michaleas, and Alex Pentland. 2025. *Accelerating AI Development with Cyber Arenas.* arXiv preprint. https://doi.org/10.48550/arXiv.2509.08200.

CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence). *Locked Shields.* https://ccdcoe.org/exercises/locked-shields/.

CISA (Cybersecurity and Infrastructure Security Agency). 2025. *The National Cyber Incident Response Plan (NCIRP).* https://www.cisa.gov/national-cyber-incident-response-plan-ncirp.

CISA (Cybersecurity and Infrastructure Security Agency). n.d. *Emergency Services Sector.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructuresectors/emergency-services-sector.

Dewar, Robert S. 2018. *Cyber Security and Cyber Defense Exercises.* Cyber Defense Report. Center for Security Studies (CSS), ETH Zürich, September.

DoD (Department of Defense). 2023. *DoD Instruction 8530.03, Cyber Incident Response,* August 9, 2023. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/853003p.PDF?ver=XPp9bgbmddCqR7gokbskWg%3d%3d.

Edinger, Julia. 2025. *Idaho Takes a Hands-On Approach to State Cybersecurity,* August 7, 2025. https://www.govtech.com/security/idaho-takes-a-hands-on-approach-to-state-cybersecurity.

Eisenbrandt, Jadyn. 2025. *Guard Soldiers Train with Civilian Experts in Cyber Discovery Exercise.* National Guard News, June 23, 2025. https://www.nationalguard.mil/News/Article-View/Article/4223483/guard-soldiers-train-with-civilian-experts-in-cyber-discovery-exercise/.

Estrada, Clarissa. 2022. *VNG's 91st Cyber Brigade Makes History at Cyber Shield.* Virginia National Guard News, June 29, 2022. https://va.ng.mil/News/Article/3078575/vngs-91st-cyber-brigade-makes-history-at-cyber-shield/.

Executive Office of the President. 2013. *Presidential Policy Directive 21: Critical Infrastructure Security and Resilience,* February 12, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Executive Office of the President. 2016. *Presidential Policy Directive 41 – United States Cyber Incident Coordination,* July 26, 2016. https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-unitedstates-cyber-incident.

Granåsen, Magdalena, and Dennis Andersson. 2016. "Measuring team effectiveness in cyber-defense exercises: a cross-disciplinary case study." *Cognition, Technology and Work* 18 (1): 121–143. https://doi.org/10.1007/s10111-015-0350-2.

Hynes, Kevin. 2025. *Cyber Tatanka Gives Network Defense Specialists Opportunity to Refine Their Skills in Safe yet Realistic Virtual Environment,* July 7, 2025. https://www.dvidshub.net/news/542196/cyber-tatanka-gives-network-defense-specialists-opportunity-refine-their-skills-safe-yet-realistic-virtual-environment.

Ihme, Kelly R. M., Patrick O'Brien Boling, Michael Zimmerman, and Timothy G. McCormick. 2025. "Who Is in Charge of Cyber Incidence Response in the Homeland?" *Parameters* 55 (3). https://press.armywarcollege.edu/cgi/viewcontent.cgi?article=3359&context=parameters.

Jeney, Carson. 2025. "Balikatan 25: Strengthening Cyber Security Ties with the Philippines," May 8, 2025. https://www.pacom.mil/Media/NEWS/News-Article-View/Article/4179489/balikatan-25-strengthening-cyber-security-ties-with-the-philippines/.

Johnson, Amanda H. 2022. "Joint Task Force Cyber Hosts Cyber Dawn 2022," July 27, 2022. https://grizzly.shorthandstories.com/california-national-guard-hosts-cybersecurity-exercise/.

Johnson, Brian David, and Natalie Vanatta. 2017. "What the Heck Is Threatcasting?" *Future Tense,* https://threatcasting.asu.edu/sites/g/files/litvpz1036/files/2019-11/what-the-heck-is-threatcasting.pdf.

Johnson, Rivers. 2012. "Cyber Guard Exercise Focuses on Defensive Cyberspace Operations," August 17, 2012. https://www.army.mil/article/85786/cyber_guard_exercise_focuses_on_defensive_cyberspace_operations.

Leffler, Stephen. 2023. *Written testimony to the Subcommittee on Cybersecurity, Information Technology, and Government Innovation, and the Subcommittee on Economic Growth, Energy Policy, and Regulatory Affairs,* September 27, 2023. https://oversight.house.gov/wp-content/uploads/2023/09/Steve-Leffler-written-testimony.pdf.

Loeffler, David. 2025. *Cyber Dawn 2025.* https://grizzly.shorthandstories.com/cyber-dawn-2025/.

Maennel, Karin, Rain Ottis, and Oliver Maennel. 2017. "Improving and Measuring Learning Effectiveness at Cyber Defense Exercises." In *Secure IT Systems,* edited by Helger Lipmaa, Aikaterini Mitrokotsa, and Raimundas Matulevičius, vol. 10674. Lecture Notes in Computer Science. Cham: Springer. https://doi.org/10.1007/978-3-319-70290-2_8.

Mag, Stephen. 2025. *What Is the Cybersecurity Color Wheel? Roles & Teams Explained.* Cybersics, July 24, 2025. https://www.cybersics.com/blog/cybersecurity-color-wheel/.

Martin, Will. 2025. "Cyber Shield 2025 Trains Guardsmen for Borderless Threats," July 22, 2025. https://reservenationalguard.com/unit-training/cyber-shield-2025-trains-guardsmen-for-borderless-threats/.

Pomerleau, Mark. 2022. "Cyber Yankee Exercise Helps National Guard Mature Partnership with Cyber Command," June 30, 2022. https://defensescoop.com/2022/06/30/cyber-yankee-exercise-helps-national-guard-mature-partnership-with-cyber-command/.

Puryear, Cotton. 2023. "Cyber Fortress 2.0 Tests Virginia's Cyber Response Plan," August 10, 2023. https://va.ng.mil/News/Article/3501226/cyber-fortress-20-tests-virginias-cyber-response-plan/.

Roudabush, Joe. 2025. "Cyber Shield 2025: A Joint Force Exercise," June 10, 2025. https://www.dvidshub.net/news/501314/cyber-shield-2025-joint-force-exercise.

Scott, Mark. 2025. *Guam Guard Participates in Balikatan 2025 Cyber Defense Exercise.* National Guard News, May 28, 2025. https://www.nationalguard.mil/News/Article-View/Article/4198937/guam-guard-participates-in-balikatan-2025-cyber-defense-exercise/.

Smeets, Max. 2022. "The Role of Military Cyber Exercises: A Case Study of Locked Shields." In *2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon),* 700:9–25. https://doi.org/10.23919/CyCon55549.2022.9811018.

StateDefenseForce.com. 2025. *Cyber Fortress 25 Unites Virginia Defense Force, National Guard, Marines, and NATO Partners Against Cyber Threats.* StateDefenseForce.com, August 18, 2025. https://statedefenseforce.com/2025/08/18/cyber-fortress-25-unites-virginia-defense-force-national-guard-marines-and-nato-partners-against-cyber-threats/.

Tarkelly, Hannah. 2025. *Cyber Shield 2025 – Coding Collaboration on a Global Scale.* DVIDS, June 12, 2025. https://www.dvidshub.net/news/500415/cyber-shield-2025-coding-collaboration-global-scale.

U.S. Code Title 10: Armed Forces. 1956a. https://uscode.house.gov/view.xhtml?path=/prelim@title10&edition=prelim.

U.S. Code Title 32: National Guard. 1956b. https://uscode.house.gov/view.xhtml?path=/prelim@title32&edition=prelim.

U.S. Department of War. 2017. *Allies, Partners Observe Cyber Guard Exercise.* U.S. Department of War News, July 5, 2017. https://www.war.gov/News/News-Stories/Article/Article/1238082/allies-partners-observe-cyber-guard-exercise/.

United States Congress. 2014. *National Cybersecurity Protection Act of 2014,* Public Law 113-282. https://www.congress.gov/bill/113th-congress/senate-bill/2519/text.

Received 7 August 2025; Revised 27 September 2025; Accepted 19 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 159-180
https://doi.org/10.55682/cdr/2ft5-1k2a

RESEARCH ARTICLE

Access Denied and *Sector Down*: Introducing Resilience Games for Critical Infrastructure Preparedness

Christopher Schwartz*[1], Jessica D. Bayliss[1], David I. Schwartz[1], A. David Abitbol[2], Brian Tomaszewski[1]

[1]Rochester Institute of Technology, Rochester, NY, USA
[2]U.S. Army Transformation and Training Command, Austin, TX, USA

Critical infrastructure (CI) organizations increasingly face disruptions that cascade across interdependent systems. Preparing for this fact requires thorough training, yet many existing training methods, especially tabletop exercises, are too resource-intensive, classified, or narrowly scoped to prepare diverse civilian and military stakeholders effectively. To address this gap, we introduce resilience games, a form of serious gaming with wargaming elements. First, we present the JV4.0 technical framework, the latest iteration of the U.S. Army Cyber Institute's Jack Voltaic series, an open-source, modular architecture for creating, running, and adapting such games. Second, we demonstrate Access Denied and Sector Down as two implementations of the framework. Access Denied is an entry-level, non-technical card game focused on incident recognition and communication. Sector Down is a cross-sector game that trains CI decision-makers to sustain essential functions under cascading attrition. We describe gameplay mechanics, alignment with practitioner taxonomies (e.g., CISA lifelines, MITRE ATT&CK/ICS, D3FEND), and insights from formative playtesting across military, academic and public venues. We conclude by outlining next steps for empirical evaluation and policy integration. The aim is to provide a scalable, accessible tool to help Department of War installations and civilian communities prepare for disruptions ranging from cyberattacks to extreme weather events.

Keywords: Critical infrastructure, cybersecurity, resilience, resilience games, wargame theory

* Corresponding author: ccsics@rit.edu

1 INTRODUCTION

In an era of increasing complexity and interconnectedness, the resilience of critical infrastructure (CI)—interdependent systems sustaining both civilian communities and U.S. Department of War (DoW) installations—has become a pressing concern for national and global security. Both civilian and military readiness, as well as overall societal stability, depend on these infrastructures. Their vast scope makes comprehensive defense infeasible, while their criticality makes inaction untenable. Policymakers and decision-makers must navigate expansive problems of scope, interdependency, and effectiveness, particularly in ensuring that installations remain operational even when surrounding infrastructures fail. Because wargaming can effectively model uncertainty, disruption, and decision-making under pressure, it serves as a valuable tool for testing resilience strategies, exploring resource allocation trade-offs, and improving preparedness.

This paper introduces resilience games, a form of serious gaming with wargaming elements (depending on the purpose and design of the game). As a form of serious game, their purpose is educational and practical: training decision-makers to sustain system functionality under continuous stress rather than to achieve battlefield victory (Abt 1970; McGonigal 2011; Huizinga 1955). Yet, like a wargame, a resilience game can employ structured opposition, role differentiation, and scenario-based play (Caffrey 2019).

Traditional approaches to preparedness training, such as tabletop exercises (TTXs), have been valuable for engaging cyber CI stakeholders. However, they are often resource-intensive, highly classified, and/or narrowly focused on individual sectors. These issues make them difficult to scale and inaccessible to many civilian and military leaders who need practical preparation the most, especially those lacking technical expertise or security clearances. As Demchak (2011) has argued, such fragmented approaches leave leaders ill-prepared for crises that manifest as whole-of-system disruptions, cascading across interdependent infrastructures and undermining national resilience. Resilience games are designed to address these limitations by providing accessible, adaptable, and reusable tools that surface systemic vulnerabilities and foster cross-sector collaboration in environments where traditional TTXs would be impractical.

Our conception of resilience gaming arose from DoW-sponsored wargaming research, specifically within the U.S. Army Cyber Institute (ACI)'s Jack Voltaic (JV) series (ACI, n.d.[a]). The Rochester Institute of Technology (RIT)'s implementation of JV4.0—the latest iteration—serves as this paper's primary case study. The JV4.0 initiative produced both a technical framework and two resilience games,*Access Denied* and *Sector Down* (Bayliss 2025b, 2025a). Both games have been designed to engage stakeholders across sectors identified by the U.S. Cybersecurity and Infrastructure Security Agency (CISA), including those that directly support

DoW installations. Importantly, while *Sector Down* is a cross-sector game for CI professionals, *Access Denied* is an entry-level, nontechnical card game for non-experts.

This paper first provides background on critical infrastructure, resilience, and the concept and role of resilience games. We then introduce the JV4.0 framework and describe the design of *Access Denied* and *Sector Down*, illustrating their mechanics and briefly summarizing insights from formative playtesting. Finally, we outline future directions for resilience gaming, including a broader conceptual scope, more sophisticated resilience measurement approaches, and opportunities for integration into national resilience strategies.

2 TOWARD A DYNAMIC UNDERSTANDING OF CRITICAL INFRASTRUCTURE

Critical infrastructure (CI) is commonly defined as the interconnected and interdependent systems that provide essential services to society (Rinaldi, Peerenboom, and Kelly 2001; Lewis 2014; DHS 2013).In current U.S. practice, the Cybersecurity and Infrastructure Security Agency (CISA) designates sixteen CI sectors (CISA, n.d.[a]), with Energy, Communications, Water, and Transportation identified as cross-cutting "lifeline" sectors because they underpin the functioning of nearly all others. Complementing this sector-based view, CISA's National Critical Functions (NCF) framework groups 55 essential functions into four areas—Supply, Distribute, Manage, and Connect— to support cross-sector risk analysis and prioritization (CISA 2019, n.d.[b], n.d.[a]; FEMA 2024).

For our two games, we adopted a provisionally more dynamic approach. For context, CI has traditionally been conceptualized in static terms: specific sectors are designated as "critical" because their disruption would critically affect national security, economic stability, and/or public health (CISA, n.d.[b]). Within this framing, resilience refers to the capacity of these systems to anticipate, withstand, adapt to, and recover from disruption (Boin, Ekengren, and Rhinard 2021). However, static definitions do not fully capture how crises can alter priorities in real time. A dynamic view recognizes that specific infrastructures can become more or less critical depending on evolving circumstances, cascading failures, and shifting decision-making priorities (Lewis and Petit 2023). For example, a recreational facility may not be critical under ordinary conditions, but could become critical during a natural disaster if repurposed as an emergency staging site. This dynamic perspective is central to resilience games, which are designed to surface such evolving interdependencies, compelling players to confront changing priorities under stress.

The chief consequence of a dynamic perspective is that criticality—and by extension, resilience—becomes viewed not as fixed attributes but instead as indicators that reflect changing states of affairs (Petersen, Lange, and Theocharidou 2020). Infrastructure becomes critical when its degradation threatens to cause societal disruption (Thayaparan et al. 2016). Resilience, in turn, can be assessed by how effectively systems resist degradation pressures.

In essence, resilience becomes a measure of how well something slows down attritional pressures acting on it (Petit et al. 2013; NIST, n.d.), whether those pressures stem from human actions (e.g., cyberattacks), non-human forces (e.g., material decay), or uncertain causes (e.g., failures in automated systems) (NIST, n.d. Eke 2024).

For resilience gaming, we adopted a simplified, gameplay-oriented approach in which all infrastructure is treated as epistemologically equal. It is up to players—acting as decision-makers—to determine which elements are "critical" within a given scenario. This approach enables games to reveal how values, priorities, and policies shape perceptions of criticality, while giving participants space to practice strategies for sustaining operations under conditions of uncertainty (Soroudi et al. 2023).

3 GAMIFYING RESILIENCE

The concept of using play for a wide range of learning and training activities is deeply embedded in culture and has been studied for many years (Huizinga 1955). Serious games, which are expressly designed for educational, training, or analytical purposes rather than entertainment (Abt 1970; McGonigal 2011; Huizinga 1955), seem particularly well-suited to address resilience. Intuitively, there is also an adversarial quality to thinking about resilience that aligns with wargaming, as though the CI system is in an active struggle against "something" that is attempting to "defeat" it. Consequently, gamifying resilience can and should draw on both domains.

We explore the gamification of resilience from both perspectives, namely, wargaming and serious gaming. Then we will discuss how resilience games concretely converge these two traditions, as well as the gaps they address by doing so.

3.1 Resilience and Wargaming

From a wargaming perspective, resilience games employ structured opposition, scenario-based play, and role differentiation (e.g., red vs. blue teams). However, unlike conventional wargames, resilience games do not prioritize conflict outcomes. Their focus is on sustaining system functionality under stress rather than achieving battlefield victory. Resilience games also do not assume a clearly defined human adversary. Instead of limiting adversarial red teams to overt, intentional human attackers, resilience games can model attritional threats such as natural disasters, systemic degradation, or ambiguous disruptions that may appear indistinguishable from random error. For example, a red action might represent a targeted cyberattack, a cascading technical malfunction, or a stochastic disruption such as a flood or power outage. Blue teams, in turn, represent infrastructure managers, operators, or community stakeholders tasked with sustaining operations despite resource constraints and uncertainty (Williams 1978; Thomas et al. 2019; Pan, Schwartz, and Mishra 2015).

This design enables resilience games to reflect the dynamic nature of crises. Success is measured not by defeating an opponent but by adapting, coordinating, and maintaining essential functions over time. In this way, resilience games build on traditions of educational and policy gaming—including crisis simulation exercises—but expand into the realm of cross-sectoral resilience, where interdependencies and cascading failures become key gameplay mechanics (Williams 1978; Tomaszewski et al. 2020; Laere et al. 2018).

Within broader wargaming theory, this intention-agnostic treatment of the adversary, along with the implicit redefinition of victory as the continued functioning of a complex system under sustained stress, positions resilience gaming in an intriguing conceptual space. Following Caffrey's (2019) generational taxonomy, wargaming has evolved from abstract competitions (first generation), to combat-focused simulations (second), to political-military games addressing national power (third). It is now entering a fourth generation of "peace games", where stability and cooperation may constitute victory conditions. Resilience gaming appears to bridge the third and fourth generations: it retains the systemic, whole-of-nation scope of third-generation games while shifting toward fourth-generation peace games by redefining success as continuity, resilience, and the prevention of systemic collapse, rather than the defeat of an adversary (Caffrey 2019).

3.2 Resilience and Serious Gaming

Serious games span a wide range of mechanics and purposes, but they share a common goal: using play to reveal hidden dynamics, change perspectives, support education and training, or make abstract challenges more tangible. Resilience games align naturally with this tradition, as they help players understand evolving risks, interdependencies, and decision-making pressures under uncertainty.

Many serious games focus specifically on education and preparedness for cybersecurity and natural disasters. Resilience may be an implicit theme or the explicit focus of play (Laere et al. 2018; DHS 2023; Schwartz et al. 2023; Thomas et al. 2019; Tomaszewski et al. 2020). These games demonstrate how interactive systems can model system stressors, reveal points of fragility, and illustrate the consequences of delayed or inadequate action. Other efforts, such as *Backdoors & Breaches*, show how simple, repeatable mechanics can train practitioners to recognize and respond to cybersecurity incidents, reinforcing procedural knowledge through structured play (Black Hills Information Security, n.d. Schwartz et al. 2023). Similarly, van Riel et al.'s (2017) work on gaming for networked infrastructure management illustrates how games can provide an experimental testbed for analyzing system interdependencies and decision-making trade-offs in complex environments (van Riel et al. 2017; Laere et al. 2018). Related efforts such as *Black Start*, a grid-restoration exercise focused on restarting generation and re-energizing the network after a blackout, underscore how preparedness activities translate into accessible, drillable practice for public and practitioner audiences (National

Renewable Energy Laboratory (NREL) 2025; EIS Council 2025; Foy 2025). *Neustart*, a board game developed for German civil protection agencies, likewise explores how communities can recover and adapt following major disruptions, highlighting how resilience itself can be gamified as both a process and an outcome (BBK, n.d. Tomaszewski et al. 2020).

3.3 Convergence and Gaps Addressed

Positioning resilience games at the intersection of wargaming and serious gaming helps clarify the practical gap they are meant to fill. Traditional tabletop exercises are resource-intensive, and the domains they cover are often limited. Resilience games, in contrast, offer accessible, replayable formats that scale across sectors and contexts. They operationalize resilience by transforming what would otherwise be an abstract and contested concept into a set of playable mechanics that stakeholders can interact with, test, and learn from. In doing so, they not only make resilience more tangible but also bridge the gap between theoretical discourse and the practical demands of applied training (Callaghan 2024; Barletta et al. 2023; Wray et al. 2020).

From a broader perspective, resilience games serve three key purposes. First, they provide an educational platform that familiarizes stakeholders with systemic vulnerabilities and interdependencies. Second, they offer a training environment for rehearsing adaptive decision-making, coordination, and continuity-of-operations strategies. Third, they function as an analytical testbed in which resilience can be operationalized, measured, and explored through repeatable scenarios and controlled variations in mechanics.

4 THE JACK VOLTAIC 4.0 TECHNICAL FRAMEWORK

In this section, we will discuss the Jack Voltaic 4.0 Technical Framework. We will briefly go over the history of the JV series; the design elements of both the overall series and 4.0; and finally 4.0's architecture.

4.1 Jack Voltaic

The Army Cyber Institute (ACI)'s JV series represents one of the earliest and most comprehensive applications of the resilience gaming concept (ACI, n.d.[a]). When the JV series first launched in 2016, the concept of a "resilience game" as described had not yet fully emerged. The JV series has consistently adopted a cross-sectoral approach to cyberinfrastructure, encompassing a range of critical infrastructure types rather than focusing on specific ones (ACI 2019a). Importantly, each subsequent iteration of JV expanded the scope of resilience scenarios, from hurricanes coupled with cyberattacks in Houston to multi-sector cyber disruptions in port cities critical to military force projection (ACI 2019b). Collectively, these exercises successfully identified critical interdependencies among infrastructure sectors, exposed gaps

in incident response, and reinforced the importance and value of whole-community partnerships. The current portfolio (JV4.0) united the efforts of five organizations (ACI, n.d.[b]). As part of this effort, RIT developed an open-source, extensible framework (the JV4.0 technical framework) for running multiplayer and quick-to-tackle tabletop and digital games tailored to the challenges faced by CI stakeholders (Schwartz et al. 2023).

Importantly, the JV series has implications that extend beyond training value alone. Exercises like JV 4.0 also function as signals of institutional capability and collective readiness—what may be termed "resilience-based power". When utilities, ports, municipal agencies, and other local actors rehearse disruption response, their preparedness inevitably confers tangible benefits to defense installations that depend on local infrastructure. The public visibility of such coordination projects credibility into cyberspace, demonstrating not only technical competence but also whole-community cohesion in the face of complex disruptions.

4.2 Design

The JV series, including JV4.0, is designed to operate in the same educational and training space as tabletop exercises (TTXs). Government agencies frequently conduct TTXs with CI stakeholders, including managers, operators, and security personnel, to prepare for disaster scenarios. Yet many of these exercises must quickly adapt to the realities of a modern workforce with limited time, resources, and technical expertise, making the construction and reconstruction of a TTX burdensome. An additional challenge is that practical educational and training exercises must overcome stakeholder reluctance toward cybersecurity topics while fostering collaboration and encouraging learning.

The JV4.0 technical framework addresses these challenges through three key design principles: modularity, scalability, and replayability. By encoding game components such as vulnerabilities, mitigation strategies, and consequences into configurable structured digital files (in .csv format), the framework enables seamless translation between tabletop and digital formats. This approach lowers barriers to adoption: games can be used in classrooms, professional training sessions, or operational planning contexts without incurring heavy resource demands. The technical framework deliberately incorporates the adversarial structure of traditional wargaming while expanding upon how adversaries are conceptualized. Blue teams represent infrastructure operators or managers responsible for sustaining operations with limited resources. Red teams, however, may take the form of intentional human attackers, stochastic disruptions, or ambiguous forces whose effects appear indistinguishable from error or chance. This design choice reflects the reality of CI crises, where disruptions often arise from overlapping causes and are not easily attributable to a single actor.

Access Denied is the most entry-level application of the framework (Bayliss 2025a). While technical CI professionals and experts can engage with it, the game is primarily designed to introduce entry-level players, students, and non-technical CI stakeholders to the core

dynamics of systemic interdependency and cascading failure. Its mechanics emphasize accessibility: players draw cards representing vulnerabilities, mitigations, and events, then allocate limited resources to maintain functionality. Lightweight and modular, *Access Denied* can be tailored to sector-specific contexts and replayed in short sessions, making it an ideal tool for familiarizing participants with resilience concepts and building comfort with cybersecurity terminology—potentially serving as a precursor to more formal TTXs.

Sector Down, by contrast, is a more advanced implementation of the framework intended for more advanced players. Whereas *Access Denied* focuses on conceptual understanding, *Sector Down* models large-scale interdependencies across multiple CI sectors. Its mechanics force players to make trade-offs under escalating disruption, balancing defense and recovery strategies with limited resources. By introducing cascading failures, turn limits, and system-wide collapse conditions (such as the "Doom Clock"), *Sector Down* challenges participants to think strategically about resilience at scale, bridging individual sector management with whole-of-system dynamics.

Together, these games demonstrate how the JV4.0 framework can support multiple resilience games with varying levels of complexity. This layered design enables resilience gaming to meet both educational and professional training needs, while remaining adaptable for future extensions. Table 1 summarizes the differences between *Access Denied* and *Sector Down*, highlighting how each game targets distinct audiences, objectives, and levels of complexity. During 2024-2025, we conducted formative playtesting at West Point, RIT, and DEF CON 33 (Village B, n.d.). Playtesters generally found the games to be intuitive and effective at surfacing interdependencies, although feedback remained anecdotal, and future work will require more rigorous empirical grounding to validate these preliminary observations.

4.3 Architecture

The JV4.0 technical framework is built to maximize flexibility across platforms and contexts. At its core, the architecture separates game logic from game content, with all information about facilities, vulnerabilities, mitigation options, and outcomes stored in structured digital files in simple .csv format. This decoupling enables the creation of new scenarios and the modification of existing ones without altering the underlying software and logic. As a result, the framework supports rapid prototyping, sector-specific customization, and replayability – qualities essential for both training and analytical applications.

The framework also supports both tabletop and digital implementations. The tabletop format facilitates face-to-face interaction through physical cards and markers, emphasizing deliberation and discussion among participants. The digital implementation, built in Unity, automates key mechanics such as random event draws, cascading failures, and adversary actions. This dual-mode architecture ensures that resilience games remain accessible in settings

where digital infrastructure may not be available while also scaling to larger, distributed, or remote exercises.

Access Denied is implemented as both a tabletop and digital card game. Its architecture emphasizes speed, simplicity and ease of deployment. Cards representing vulnerabilities, defenses, and events are drawn from decks and displayed to players. The design makes *Access Denied* easy to deploy in short training sessions or classroom settings while remaining extensible for more advanced use cases.

Sector Down is more complex structurally. Each sector (e.g., energy, water, transportation) has three facilities, each dependent on distinct resource points (e.g., physical, financial, network). These interdependencies are encoded directly in the game logic, which enforces cascading failures when critical facilities go down. The architecture also incorporates the "Doom Clock," a turn-based mechanism that accelerates system-wide collapse if critical sectors (such as power) remain offline for an extended period. In the digital version, Unity automates these cascading effects and random white-card events, simulating hazards and unexpected opportunities in real time.

Taken together, these architectural choices demonstrate how the JV4.0 framework supports both introductory and advanced resilience games. *Access Denied* provides a lightweight, accessible entry point, while *Sector Down* leverages the same underlying architecture to deliver deeper, system-level challenges. This layered design highlights the framework's versatility and its potential to support a broader family of resilience games in future development.

Table 1. Comparison of *Access Denied* and *Sector Down*

Feature	Access Denied	Sector Down
Primary audience	Entry-level players, students, and non-technical CI stakeholders	Advanced players, CI professionals/experts, and mixed civilian–military teams
Objectives	Learn terms, identify vulnerabilities, implement mitigations, balance limited resources, and understand lateral movement	Manage cascading interdependencies and prioritize resilience strategies across multiple sectors
Complexity	Low–Medium (focused on cyber pathways and direct impacts)	High (integrates cyber + physical threats, cross-sectoral interdependencies, and cascading risk)
Mechanics	Tabletop or digital card-based gameplay, resource allocation, basic MITRE ATT&CK and ICS integration	Digital card-based gameplay, Doom Clock timer, layered defenses, complex ATT&CK mapping
Duration	~30–45 minutes	~60–90 minutes
Educational value	Introduces cyber resilience concepts; highlights systemic vulnerabilities	Models systemic crises; trains decision-making under uncertainty; emphasizes collaboration
Relation to JV4.0	Accessible entry point to learn key concepts	Advanced, strategy-oriented implementation of the JV4.0 framework, aligned with CISA's lifelines

5 GAME PLAY AND MECHANICS

In this section, we discuss *Access Denied* and *Sector Down*, the two resilience games we implemented within the JV 4.0 Technical Framework.

5.1 *Access Denied*

Resilience in *Access Denied* models the need to preserve and reinforce existing infrastructure while managing vulnerabilities under resource constraints. Designed as an introductory resilience game, it emphasizes how cascading dependencies and limited resources complicate decision-making. One of the game's educational goals is to incorporate information from real cyberattacks into the cards. The 2000 Maroochy Water Services incident in Australia and the 2016 Kyiv power grid attack in Ukraine both inform the content of the card. The team designed the cards to highlight the differences between Industrial Control System (ICS) attacks and network-based cyberattacks. Mitre's ICS ATT&CK framework was used to create the cards, along with information from Joseph Weiss's work on protecting ICS. Figure 2 shows examples cards. The design goal is to rehearse recognizing threats, choosing mitigations under constraints, and building network robustness—not just "winning" a duel.

Access Denied is designed for two players (1-vs-1), but can support additional ones. Each player is both a defender of their own critical infrastructure network and an attacker of another player's network, represented by various power and water facilities. Players set up a sector play area and shuffle two decks (Table 2): a main deck (mixed action cards) and a facility deck. Each player draws an initial hand of five cards from their main deck. No facilities in play at the start; one facility enters the player's network each turn during the facility phase.

Table 2. Overview of card types in the main deck of *Access Denied*

Category	Description
Vulnerabilities (Red)	Threats or adverse conditions placed on the opponent (e.g., credential exposure, single-point-of-failure). Many require spending facility points to play.
Mitigations (Yellow)	Controls or responses that counter specific vulnerabilities (e.g., patching, segmentation, backup procedures).
Instants (Purple)	One-shot effects that modify play (e.g., trigger or alter a roll, enable lateral effects, force or disallow an action) and then go to discard.
Defenses	Sector hardening or continuity measures placed only during the defense phase on your own board to reduce risk or consequences across later turns.
Facility Points (FP)	Each facility has an FP value. Players spend FP from their own facilities to play some Vulnerabilities; successful attacks reduce the opponent's FP on targeted facilities; facilities at 0 FP are removed from play.
Hand Economy	Players manage a maximum hand of five cards. Draws, discards, and the use of Instants shape tactical tempo.
Connections Requirement	Larger facilities should be supported by more connections. Meeting minimum connection targets awards end-game bonuses and reinforces interdependency planning.

As for turn structure, play proceeds in rounds. Within each round both players move through the same phases in order (Figure 1). The game ends when a player runs out of cards or loses all facilities. Scoring is calculated by subtracting losses from remaining facility points and adding bonuses for facilities that meet minimum connection targets.

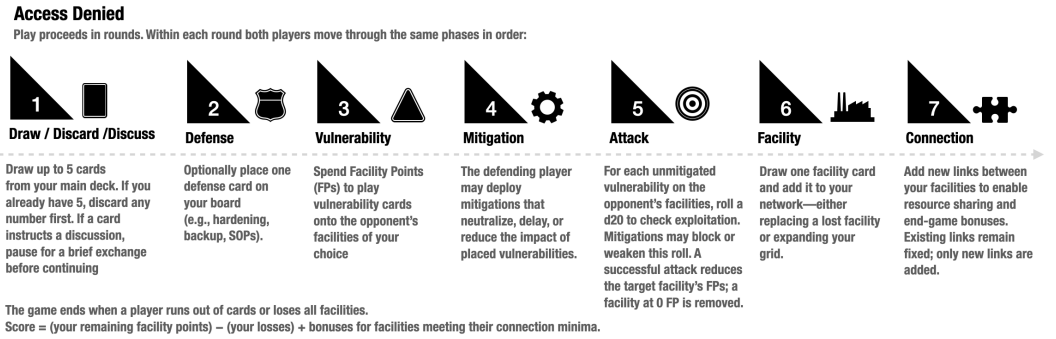


Figure 1. Turn structure of *Access Denied*

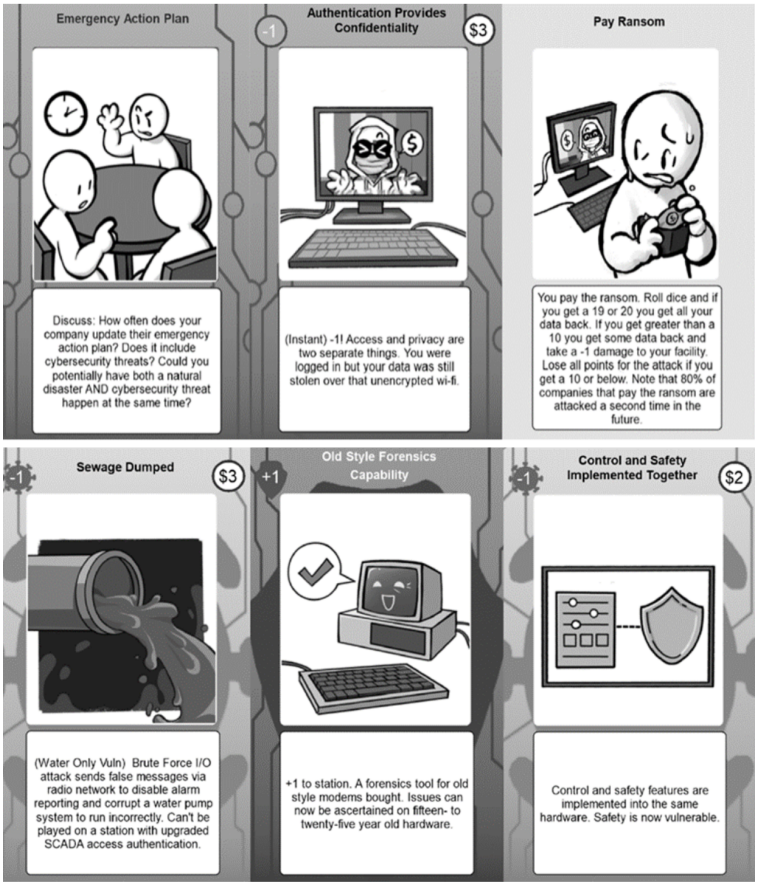


Figure 2. Examples of *Access Denied* cards. Top: cards representing information that may surprise players new to cybersecurity. Bottom: cards representing characteristics of industrial control systems (ICS)

The first phase of play—Draw/Discard/Discuss— reflects real-world constraints in resilience planning: players may recognize a critical vulnerability yet lack the immediate resources to address it, forcing difficult prioritization decisions. Throughout the game, vulnerabilities emerge dynamically, underscoring the ongoing challenge of identifying, prioritizing, and mitigating risks before they escalate. For example, the *Lateral Movement* card spreads weaknesses across connected facilities, mirroring real-world infrastructure interdependencies. Long-term survival depends not only on managing immediate crises but also on sustaining adaptive capacity over time. In this way, the game mechanics offer a practical model for understanding and testing resilience strategies in uncertain environments by requiring players to anticipate risks, allocate resources wisely, and maintain infrastructure interconnectivity.

5.2 *Sector Down*

Sector Down models CI resilience by simulating sector interdependencies, cascading failures, and the resource trade-offs between mitigating risk and supporting other sectors. Its aim is to help stakeholders understand the complexity of cross-sector dependencies and the challenges of sustaining operations when multiple infrastructures face simultaneous disruption. Red players act as adversaries—representing both intentional and non-intentional disrupting forces— seeking to bring sectors down, while Blue players represent sector managers working to preserve functionality under stress.

Sector Down is an asymmetric game: one Red attacker plays against up to four Blue defenders. Each Blue player controls a sector composed of three facilities, modeled on CISA's lifeline sectors (e.g., Energy, Communications, Water, and IT). Red plays against all Blues collectively. During setup, each Blue lays out a sector board with three facility slots, and Red prepares

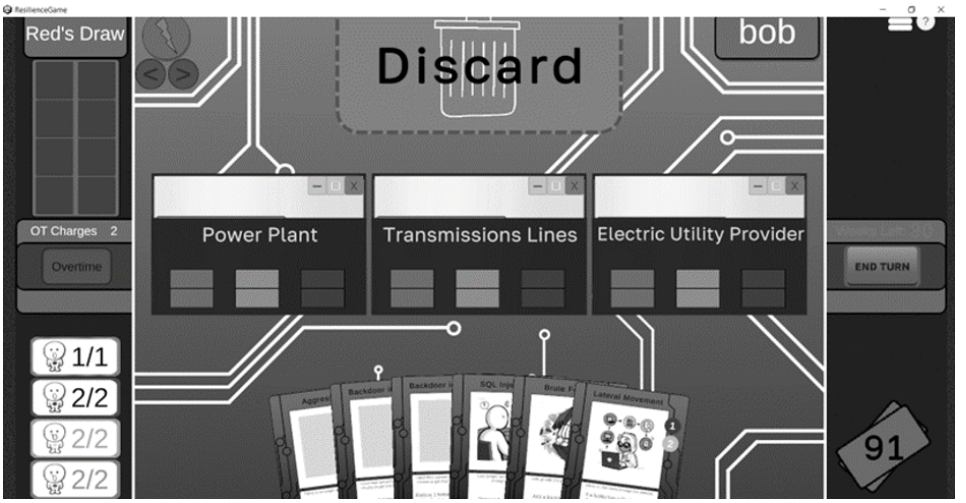


Figure 3. Digital game board for *Sector Down* as seen from the Red player's viewpoint

the attacker board (Figure 3). All players draw and maintain a hand of five cards (Table 3). Each player also receives worker tokens—the resources that power card actions. Blue players receive two colored workers tied to their sector, while Red players receive their own workers plus an additional colorless worker that can be used flexibly.

Table 3. Card types and core resources in *Sector Down*

Category	Description
Attacks (Red)	Techniques or effects Red uses to degrade or disable facilities, often stronger when a backdoor is present.
Defenses / Mitigations (Blue)	Controls that Blue deploys to block, remove, or reduce the impact of attacks, including segmentation, hardening, and recovery actions.
Operations / Support (Both)	Cards enabling worker movement, cross-sector coordination, or temporary state changes.
White cards (Global events)	Not in hand. Revealed every third turn to introduce shocks or benefits that affect all players.
Workers (Resource)	Workers are the primary resource for most actions. Certain cards allow workers to be shared across Blue sectors, forcing trade-offs between local defense and mutual aid.
Facility state (Status)	Each facility is tracked by up/down condition and ongoing effects (e.g., backdoored, fortified). Blue aims to sustain functionality (keep facilities up across sectors long enough to ride out the scenario); Red aims to push and hold facilities in a down state.

During gameplay, the Red player views Blue players one at a time and can rotate among them, with each Blue controlling three facilities that Red may target. Rounds follow a fixed cycle. Each turn starts with the Red player. For example, Red may launch a brute-force attack against an authentication point to gain initial access (Figure 5). If successful, Red can then install a backdoor to maintain persistence and escalate control of the facility. Each Blue player takes a turn, during which they can attempt to remove backdoors or restore and reinforce their facilities. Every third turn begins with a White Card phase, which injects a global event drawn alternately from positive and negative decks.

On any turn, players spend workers to play cards, trigger abilities, and operate facilities. Workers may push “overtime” for a temporary boost, but doing so risks “exhaustion” (temporary limits) on subsequent turns.

Play continues up to Turn 30 or until an earlier win condition is met:

- Deck exhaustion: if one side’s deck empties, the opponent wins.
- Turn limit: if the game reaches Turn 30, Blue wins by surviving the scenario.
- Total collapse: if all Blue facilities are down simultaneously, Red wins.
- Doom Clock: if half or more Blue sectors are down, or if any Core Sector (Energy, Communications, Water, IT) has two or more facilities down, the Doom Clock starts. Blue has three turns to recover above the threshold or Red wins.

Certain Blue cards can extend the timeline to allow recovery. Red, in response, can counter by shortening it to force permanent shutdowns. Blue players may also share their workers with one another, enabling coordinated support across sectors.

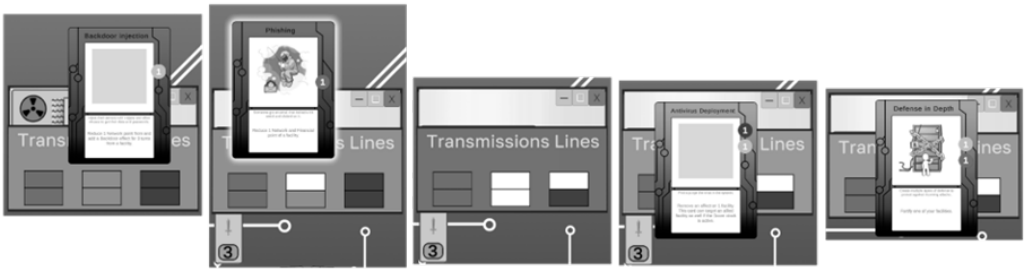


Figure 4. An example play set for *Sector Down* starts with the red player bringing down a transmission line facility controlled by a blue power player. Blue has no resources to restore the facility immediately, but can remove the backdoor that caused the issues, and then play a card to help defend against future attacks.

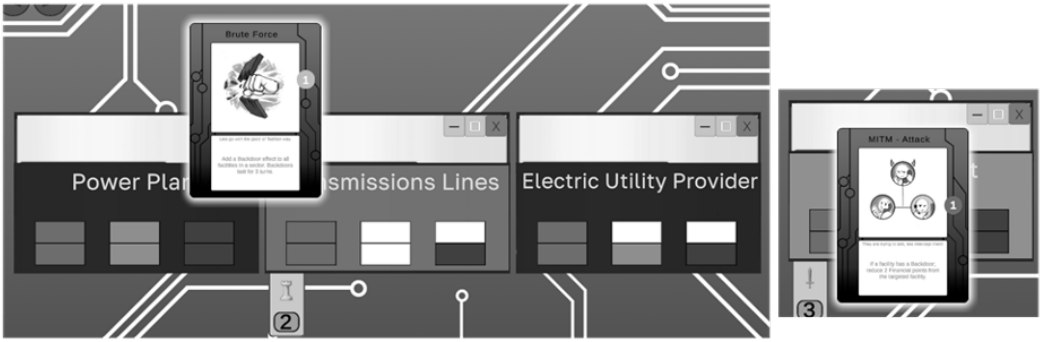


Figure 5. Red attempts to brute-force credentials at Blue's facility; if successful, Red may later install a backdoor to maintain persistence.

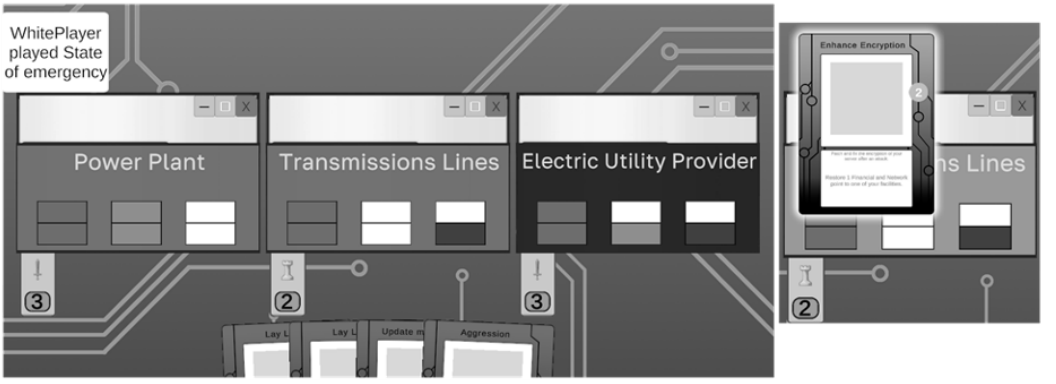


Figure 6. Two power facilities are down, activating the Doom Clock. Blue perhaps would have preferred to do something else with their turn, but instead, they must bring their transmission lines back online.

The gameplay emphasizes resource scarcity. Every action costs resources (represented by the worker tokens). Facilities, attacks, and defenses each require specific tokens, forcing Blue

Table 4. Examples of sector facility types and dependencies

CISA Sector	Facility type	Facility name	Dependency 1	Dependency 2	Dependency 3
Chemical	Production Transmission Distribution	Manufacturing plant Warehouse Transportation infrastructure	Energy Transportation Government	Water Water Defense	Agricultural Manufacturing Transportation
Energy	Production Transmission Distribution	Power plant Transmission lines Electric utility provider	Manufacturing Nuclear Information tech.	Transportation Dams Government	Water Manufacturing Transportation
Water and wastewater	Production Transmission Distribution	Water treatment facility Water pumping station Water utility	Government Government Information tech.	Emergency services Emergency services Government	Dams Manufacturing Energy

players to constantly weigh whether to defend their own sectors or divert resources to assist others, reinforcing the game's emphasis on interdependence and trade-offs.

Table 4 illustrates simplified interdependencies based on CISA's lifeline sectors. Each sector includes three types of facilities—production, transmission, and distribution—linked by three categories of points: physical, network, and financial. These mechanics abstract real-world complexity while still surfacing systemic risks, such as the reliance of Water on Power or Transportation.

A central mechanic is the Doom Clock, which activates if a CISA lifeline sector (Energy, Communications, Transportation, or Water) remains down for an excessive number of turns (Figure 6), signaling cascading impacts on dependent sectors (MITRE Corporation, n.d.[b], n.d.[a]). The clock functions as an "ultimate red team," introducing a systemic time-based pressure that can overwhelm even well-coordinated blue players. Conceptually, this mechanism illustrates to the blue player the compounding nature of system fragility.

Here is an example sequence that highlights both the fragility of sector interdependencies and the constant trade-offs Blue must make between immediate mitigation and long-term resilience (Slowik 2019; Abrams and Weiss 2008; Weiss 2010). In one playtest, Red launched a "Man-in-the-Middle" attack against Blue's power plant facility, intercepting and altering control messages to inject malicious commands—the disruption followed from those injected actions, not from interception alone. When the power plant went down, Blue's communications facility also lost capacity, thereby limiting its ability to coordinate defenses. This delay meant that their water facility could not deploy its "technician" card in time to stop a mechanical failure, compounding the disruption. Within three turns, multiple sectors were degraded, triggering the Doom Clock and forcing Blue to divert scarce resources into emergency recovery.

Stochastic events can also occur outside direct player control. This introduces a level of uncertainty that mirrors real-world crises in which both hazards and opportunities may arise unexpectedly. While some white cards introduce natural disasters or systemic shocks that exacerbate vulnerabilities, others offer temporary advantages, reflecting emergency

policy measures or ad hoc community support. For example, the "State of Emergency" card enables Blue players to mobilize additional workers for overtime, providing greater short-term defensive capacity. This mechanic highlights how unplanned external factors—whether disruptive or beneficial—shape resilience and force players to adapt strategies in response to events beyond their control.

6 PLAYTESTING AND FORMATIVE EVALUATION

We conducted a series of formative playtests during 2024–2025 to refine the games prior to formal evaluation. The primary goal was to finalize rules, interfaces, and software stability before conducting a formal evaluation of learning outcomes. We used convenience samples across five venues, collected facilitator field notes and brief exit prompts, and iterated the games between sessions. Feedback was qualitative and focused on engagement, clarity, and design improvements, rather than instructional efficacy. Table 5 summarizes the playtests, populations, and session foci.

Table 5. Summary of playtests, populations, and session foci

Location / Event	Participants	Session Focus / Outcomes
West Point (U.S.)	~10 participants; mixed military/civilian cyber researchers; median age ~40+; mixed gender	Stress-tested interface concepts; scoped problems for *Access Denied* and *Sector Down*; produced first iteration of card language and UI affordances.
MORS Global Critical Infrastructure Workshop (Germany)	20 attendees; military officers and researchers; ages ~40–60; mixed gender	Design review (presentation only); feedback refined design goals, scenario scale, and win conditions.
RIT Game-Design Students (U.S.)	~25 students; ages 18–22; ~85% men	Focused on networking/pacing for *Sector Down* and card balance for *Access Denied*.
RIT Beta Cohort (U.S.)	12 participants; mixed non-professionals and professionals	Led to rule-sheet rewrite, instructional video, and table playmat; one player recommended classroom use.
RIT Cyber Range (U.S.)	~10 participants; faculty, staff, students; ages 18–60; predominantly men	Live *Sector Down* runs surfaced stability issues and rule ambiguities; prompted redesign of persistence/backdoor timing and worker exhaustion.
DEF CON Biohacking Village (U.S.)	~100 players; preteen–40s; mixed gender; ~20% international; mostly professional/expert players	Public validation of *Access Denied*; gathered player observations and exit feedback.

Following formative testing, we implemented several refinements across both games. Card wording was tightened to clarify attack and mitigation triggers, and turn structures were revised—adding explicit phases in *Access Denied* and sharpening Red/Blue tempo in Sector Down. We also adjusted persistence and backdoor timing, improved cues for worker overtime and exhaustion, strengthened networking stability for multi-client *Sector Down* sessions, and enhanced onboarding materials for *Access Denied*, including a revised rulesheet, playmat, and instructional video.

Expert testers recommended adding facility-specific vulnerabilities and defenses, as well as expanding mitigation options. Novice players suggested a quick-play variant, such as

increasing discard throughput to shorten sessions. We also piloted a justification mechanic in *Access Denied*, in which players may propose a defensible off-label mitigation. If all agree that it is plausible, the card may be used, encouraging reasoned argumentation rather than simple card matching. These enhancements remain exploratory and have not yet been formally implemented.

Across playtest sites, *Sector Down* successfully prompted discussions about interdependencies, trade-offs, and systemic risk under time pressure. *Access Denied* consistently supported minutes-to-learn onboarding and recognition-mitigation reasoning. Again, these observations are preliminary but point to the need for more systematic evaluation.

7 FUTURE PERSPECTIVES

This section focuses on the question: *What next?* First, we will address how resilience gaming can be more rigorously evaluated. Second, we will discuss the need to expand the meaning of criticality in CI. Third, we will strategize how resilience gaming can be integrated into national resilience strategies.

7.1 Empirical Grounding and Evaluation

The games presented here demonstrate the potential of resilience gaming to model systemic vulnerabilities and train adaptive responses. However, as noted above, current evidence remains limited to formative playtests and qualitative feedback from relatively small samples. These early sessions were valuable for refining mechanics, improving usability, and revealing early indications of learning, but they do not constitute rigorous validation.

We will therefore conduct a structured evaluation using pre/post instruments aligned with practitioner taxonomies (CISA Lifelines, MITRE ATT&CK for ICS, and MITRE D3FEND). The target sample size has yet to be determined, but both practitioner and student cohorts will be included. Core outcome measures will include: (a) incident-recognition accuracy (mapping threats to controls), (b) mitigation selection and timing under resource constraints, (c) interdependency reasoning across sectors, (d) and gameplay-embedded metrics for operational continuity and adaptive coordination. We will also collect participant demographics and professional roles to identify which stakeholder groups benefit most and under what gameplay conditions (e.g., prior CI literacy, technical vs. non-technical roles). Ideally, we would also assess the durability of learning via longitudinal follow-ups—through repeated play or delayed post-tests—across both civilian organizations and DoW users.

7.2 Expanding the Meaning of "Critical" Infrastructure

Resilience games provide an opportunity to understand the role non-critical infrastructure plays within different scenarios. Not all infrastructure is considered critical, at least not at

an immediately intuitive level. Examples include recreational facilities, tourism infrastructure, and schools—sectors that, while important, do not traditionally fall under the CISA CI designation (CISA, n.d.[a]). Yet, their presence—or absence—may meaningfully influence gameplay. A key question is whether including non-critical infrastructure changes player engagement, alters perceived stakes, or enhances the realism of scenarios. Further research on using resilience games as a method could help determine how the less urgent non-critical infrastructure influences player engagement, decision-making, or scenario realism.

More broadly, resilience gaming provides a means to explore the nature of criticality itself. Traditional approaches treat critical infrastructures as predefined categories essential to national security, public health, or economic stability. Yet, criticality is context-dependent. Consider again a recreational facility. Although non-critical under normal circumstances, it may become critical during a weather catastrophe by serving as a staging platform for emergency services or as a shelter for displaced populations. Similarly, consider what would happen if a cyberattack on a city's power grid occurred at the same time as an active shooter incident at a school. Simultaneous crises force decision-makers to navigate competing priorities. Law enforcement, emergency medical services, and crisis response teams must divide their attention and resources. While the cyberattack might ordinarily take priority, as power grid failures affect hospitals, emergency communications, and CI operations, the school incident creates an immediate, visible crisis requiring urgent intervention, thus competing for criticality. Scenarios such as these introduce new layers of strategic complexity, challenging players to manage resource allocation dynamically rather than relying on predefined infrastructure hierarchies. They highlight dynamic criticality: an evolving hierarchy of what matters most under cascading stress. Future resilience games could explicitly model these shifting priorities, further enriching their strategic complexity.

7.3 Integration with National Resilience Strategies

Establishing resilience gaming as both a research methodology and a practical training tool will require broader engagement across stakeholder communities. To do this, future efforts should focus on:

- Deepening collaboration with CI professionals, policymakers, and cybersecurity experts to refine mechanics based on real-world needs.
- Clarifying the role of JV4.0 within the broader Jack Voltaic ecosystem by enhancing other JV initiatives while reinforcing its role as a resilience training platform.
- Encouraging open-source contributions to enable academics, practitioners, and developers to expand the game framework with new scenarios and mechanics.

Additionally, to solidify resilience gaming as a valuable tool in national security and infrastructure protection, further research should:

- Continue exploring developing the concept of *dynamic criticality*, where infrastructure shifts from non-critical to critical status in response to cascading failures—an avenue for future resilience game development.
- Position resilience games as decision-support tools for governments and private-sector organizations, aiding in risk assessment and resilience planning.

Finally, resilience gaming carries strategic implications beyond pedagogy. Positioned at the civic–defense seam, these games function not only as learning tools but also as forms of strategic signaling. By making collective preparedness visible to partners and adversaries, resilience gaming complements traditional notions of power projection in cyber defense.

8 CONCLUSION

Resilience games represent a conceptual evolution in gaming for national security, integrating the strengths of both serious games and wargames. As serious games, they prepare decision-makers to sustain CI and mitigate cascading failures under systemic stress. As wargames, they shift the focus from winning on the battlefield to ensuring ongoing operational continuity, providing a scalable and accessible tool to enhance national security and CI resilience. The JV4.0 technical framework, demonstrated through *Access Denied* and *Sector Down*, shows how such games can operationalize resilience via structured play, adaptive decision-making, and cross-sector collaboration.

Resilience gaming remains an emerging field. Future work must establish empirical grounding through systematic evaluations, refine mechanics for measuring resilience outcomes, and explore the implications of dynamic criticality—including how non-critical infrastructure influences scenario realism and decision-making. Broader community engagement—from military installations and utilities to municipal planners—will be key to ensuring relevance and impact. Pursued with rigor and creativity, resilience games have the potential to become a valuable instrument for preparedness, risk assessment, policy development, and strategic coordination. In an era defined by complex, interconnected crises, they offer a compelling pathway for enhancing collective resilience and, ultimately, safeguarding lives.

ABOUT THE AUTHORS

Christopher Schwartz, Ph.D. is a research scientist with the Department of Cybersecurity and the School of Interactive Games and Media at the Rochester Institute of Technology. He earned his doctorate from the Institute of Philosophy at KU Leuven, and previously worked as a journalist in Kyrgyzstan, including research editor for the Organization for Security and Cooperation in Europe (OSCE) Academy.

Jessica D. Bayliss, Ph.D. is a joint professor in the School for Interactive Games and Media and Department of Computer Science in the Golisano Computing College at the Rochester Institute of Technology (RIT). Her research interests include data-oriented design, game design, and game development and she co-created both the B.S. and M.S. degrees in game design and development at RIT. Bayliss received a Ph.D. in computer science from the University of Rochester.

David I. Schwartz, Ph.D. has worked in the academic field of game design and development since 2001, when he founded the Game Design Initiative at Cornell University. In 2007, Schwartz moved to the Rochester Institute of Technology as a game design and development faculty member who formed the School of Interactive Games and Media (IGM) in 2011. After receiving tenure in 2011, he became IGM's Director in 2015. His current research focuses on cybersecurity gamification, critical infrastructure, geogames, digital twins, and physically-based animation.

A. David Abitbol, Ph.D. is currently a career civil servant with the Department of the Army. Over the last ten years, he's worked as an Operations Research Systems Analyst (ORSA), where he develops and designs studies and mathematical models to optimize resource allocation and inform the development of policy. Prior to his time in the civil service, David was a doctoral research fellow with the RAND Corporation within the Army Arroyo Institute. When David isn't thinking about research designs and experiments, he spends his time playing with his newborn son and finding new ways to annoy his wife with interesting facts about the world.

Brian Tomaszewski, Ph.D. is a distinguished Geographic Information Scientist with research interests in the domains of Geographic Information Science and Technology, Spatial Data Science, Disaster Management, and Forced Displacement. He has published over 60 peer reviewed publications. His book Geographic Information Systems (GIS) for Disaster Management (2nd edition) was published through Routledge Press. Driven by a commitment to global betterment, he has collaborated with prestigious internationally-focused organizations such as the United Nations High Commissioner for Refugees (UNHCR) with research projects in Germany, Jordan, and Rwanda. He has received over $2,000,000 in research funding as Principal Investigator from sources such as the US National Science Foundation. He was also awarded a prestigious Fulbright Scholarship from the Polish-U.S. Fulbright Commission. Through his public scholarship, Dr. Tomaszewski has cultivated a vast educational platform, amassing over 16K subscribers on his Geographic Information Science and Technology YouTube Channel. He holds a Ph.D. in Geography from Pennsylvania State University.

ACKNOWLEDGMENTS

A large team created this work and related products: students (Liam Andres, Diego Barilla, Sam Beckman, Lizhao Cao, Jye Crocker, Michael Eaton, Elad Flaison, Ben Garvey, Emmett McEvoy, Kevin LaPorte, Mukund Suresh, Emily Nack, Henry Orsagh, Dariel Ravelo-Ramos, Lee Smith, Heena Thadani, Huadong Zhang, James Zilberman), faculty (Jessica Bayliss, Chao Peng, David I. Schwartz, Brian Tomaszewski), a research scientist (Chris Schwartz), and DoD representatives (David Abitbol, Karen Guttieri, Mark McElwain, Steve Whitham, Chris Wilkinson).

DISCLAIMER. This data was produced by the Rochester Institute of Technology under the United States Military Academy (USMA) Award Number W911NF-23-2-0036. USMA, as the Federal awarding agency, reserves a royalty-free, nonexclusive and irrevocable right to reproduce, publish, or otherwise use this data for Federal purposes, and to authorize others to do so in accordance with 2 CFR 200.315(b).

FUNDING AND SUPPORT. The authors express their gratitude to the following funding sources that supported this work at different stages of development: the Army Cyber Institute at West Point and the Army Educational Outreach Program. Esri, Unity Technologies, and RIT's ESL Global Cybersecurity Institute provided additional support that significantly contributed to this work.

REFERENCES

Abrams, Marshall, and Joe Weiss. 2008. *Malicious Control System Cyber Security Attack Case Study—Maroochy Water Services, Australia.* MITRE Corporation. https://www.mitre.org/sites/default/files/pdf/08_1145.pdf.

Abt, Clark C. 1970. *Serious Games.* New York: Viking Press.

ACI (Army Cyber Institute). 2019a. *Jack Voltaic 1.0 Executive Summary.* https://cyber.army.mil/Portals/3/Documents/JackVoltaic/JV1_Exsum_FINAL.PDF?ver=2019-08-20-153840-900.

ACI (Army Cyber Institute). 2019b. *Jack Voltaic 2.0 Executive Summary.* https://cyber.army.mil/Portals/3/Documents/JackVoltaic/JV2_Exsum_FINAL.pdf?ver=2019-08-20-153841-040.

ACI (Army Cyber Institute). n.d.(a). *Jack Voltaic.* https://cyber.army.mil/Research/Jack-Voltaic/.
ACI (Army Cyber Institute). n.d.(b). *Jack Voltaic Research Reports.* https://cyber.army.mil/Research/Jack-Voltaic/Research-Reports/.
Barletta, V., M. Calvano, F. Caruso, A. Curci, and A. Piccinno. 2023. "Serious Games for Cybersecurity: How to Improve Perception and Human Factors." In *2023 IEEE International Conference on Metrology for eXtended Reality, Artificial Intelligence and Neural Engineering (MetroXRAINE),* 1110–1115. IEEE. https://doi.org/10.1109/MetroXRAINE58569.2023.10405607.
Bayliss, Jessica. 2025a. *accessDenied Game Repository.* GitHub repository. https://github.com/profjdbayliss/accessDenied.
Bayliss, Jessica. 2025b. *RIT Resilience Game.* GitHub repository. https://github.com/profjdbayliss/RIT-Resilience-Game.
BBK (Federal Office of Civil Protection and Disaster Assistance). n.d. *Neustart: Planspiel zur Krisenvorsorge [Restart: A Simulation Game for Crisis Preparedness].* https://www.bbk.bund.de/EN/neustart-game.html.
Black Hills Information Security. n.d. *Backdoors & Breaches.* https://www.blackhillsinfosec.com/tools/backdoorsandbreaches/.
Boin, Arjen, Magnus Ekengren, and Mark Rhinard. 2021. *Resilience: The Governance of Complexity.* Oxford: Oxford University Press. https://doi.org/10.1093/oso/9780192856296.001.0001.
Caffrey, Jr., Matthew B. 2019. *On Wargaming: How Wargames Have Shaped History and How They May Shape the Future.* Newport, RI: Naval War College Press.
Callaghan, Paul. 2024. "The Ludo-Learning Matrix: A Framework for Understanding Learning in Games." In *European Conference on Games-Based Learning.* https://doi.org/10.34190/ecgbl.18.1.2650.
CISA (U.S. Cybersecurity and Infrastructure Security Agency). 2019. *National Critical Functions: An Evolved Lens for Critical Infrastructure Security and Resilience.* https://www.cisa.gov/sites/default/files/publications/national-critical-functions-overview-508.pdf.
CISA (U.S. Cybersecurity and Infrastructure Security Agency). n.d.(a). *Critical Infrastructure Sectors.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.
CISA (U.S. Cybersecurity and Infrastructure Security Agency). n.d.(b). *Critical Infrastructure Systems. Infrastructure Dependency Primer—Learn.* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/resilience-services/infrastructure-dependency-primer/learn/critical-infrastructure-systems.
Demchak, Chris C. 2011. *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security.* Athens, GA: University of Georgia Press.
DHS (U.S. Department of Homeland Security). 2013. *National Infrastructure Protection Plan (NIPP): Partnering for Critical Infrastructure Security and Resilience.* Washington, DC. https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf.
DHS (U.S. Department of Homeland Security). 2023. *Ready 2 Help,* August. https://www.ready.gov/kids/ready-2-help.
EIS Council. 2025. *Why the World's Leading Organizations Run Black Start Exercises.* https://eiscouncil.org/why-the-worlds-leading-organizations-run-black-start-exercises/.
Eke, Paul. 2024. *Securing Critical Infrastructure in the Age of AI.* Center for Security and Emerging Technology, Washington, DC. https://cset.georgetown.edu/wp-content/uploads/CSET-Securing-Critical-Infrastructure-in-the-Age-of-AI.pdf.
FEMA (U.S. Federal Emergency Management Agency). 2024. *Community Lifelines.* Last updated March 8, 2024. https://www.fema.gov/emergency-managers/practitioners/lifelines.
Foy, Kylie. 2025. "Power-Outage Exercises Strengthen the Resilience of US Bases," September 22, 2025. https://news.mit.edu/2025/power-outage-exercises-strengthen-resilience-us-bases-0922.
Huizinga, Johan. 1955. *Homo Ludens: A Study of the Play-Element in Culture.* Boston: Beacon Press.
Laere, Joeri van, Peter Berggren, Osama Ibrahim, Aron Larsson, and Susanne Kallin. 2018. "A Simulation-Game to Explore Collective Critical Infrastructure Resilience." In *Safety and Reliability – Safe Societies in a Changing World,* 1305–1312. CRC Press/Taylor & Francis. https://doi.org/10.1201/9781351174664-164.
Lewis, Lawrence Paul, and Frédéric Petit. 2023. *Critical Infrastructure Interdependency Analysis: Operationalizing Resilience Strategies.* Argonne National Laboratory. https://www.preventionweb.net/files/66506_f415finallewisandpetitcriticalinfra.pdf.
Lewis, Ted G. 2014. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* Hoboken, NJ: John Wiley & Sons. https://doi.org/10.1002/0471789542.

McGonigal, Jane. 2011. *Reality Is Broken: Why Games Make Us Better and How They Can Change the World.* New York: Penguin Press.

MITRE Corporation. n.d.(a). *ATT&CK for Industrial Control Systems (ICS).* https://attack.mitre.org/matrices/ics/.

MITRE Corporation. n.d.(b). *D3FEND Framework.* https://d3fend.mitre.org.

National Renewable Energy Laboratory (NREL). 2025. *Black Start.* https://www.nrel.gov/grid/black-start.

NIST (National Institute of Standards and Technology). n.d. *Resilience.* Computer Security Resource Center Glossary. https://csrc.nist.gov/glossary/term/resilience.

Pan, Yin, David Schwartz, and Sumita Mishra. 2015. "Gamified Digital Forensics Course Modules for Undergraduates." In *2015 IEEE Integrated STEM Education Conference (ISEC),* 100–105. IEEE. https://doi.org/10.1109/ISECon.2015.7119899.

Petersen, Laura, David Lange, and M. Theocharidou. 2020. "Who Cares What It Means? Practical Reasons for Using the Word Resilience with Critical Infrastructure Operators." *Reliability Engineering & System Safety* 199. https://doi.org/10.1016/j.ress.2020.106872.

Petit, F. D. P., D. Verner, J. R. Buehring, M. A. Phillips, R. G. Haffey, and K. G. Bassett. 2013. *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience.* Argonne National Laboratory. https://doi.org/10.2172/1087819.

Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. 2001. "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies." *IEEE Control Systems Magazine* 21 (6): 11–25. https://doi.org/10.1109/37.969131.

Schwartz, David, David Abitbol, Emily Nack, C. M. Wilkinson, Steven Whitham, Brian Tomaszewski, Jessica D. Bayliss, and Chao Peng. 2023. "Game Design for Critical Infrastructure Resilience: Game Engine Integration with Geospatial Technology." In *91st Symposium of the Military Operations Research Society (MORS).* U.S. Military Academy, West Point, NY, June. https://www.mors.org/Events/Symposium/91st-Symposium.

Slowik, Joe. 2019. *CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack.* Dragos. https://www.dragos.com/wp-content/uploads/CRASHOVERRIDE.pdf.

Soroudi, Mona, Meisam Gordan, Ili Ko, Páraic Carroll, Daniel McCrum, Sandra König, Stefan Schauer, and Lorcan Connolly. 2023. "A Serious Game Conceptual Approach to Protect Critical Infrastructure Resilience in Smart Cities." In *14th International Conference on Applications of Statistics and Probability in Civil Engineering.* Dublin, Ireland. https://www.precinct.info/storage/minisites/a-serious-game-conceptual-approach-to-protect-critical-infrastructure-resilience-in-smart-cities.pdf.

Thayaparan, M., B. Ingirige, C. Pathirage, U. Kulatunga, and T. Fernando. 2016. *A Resilience Framework for Critical Infrastructure.* https://openresearch.lsbu.ac.uk/item/872xq.

Thomas, Michael K., Andria Shyjka, Skip Kumm, and Rigel Gjomemo. 2019. "Educational Design Research for the Development of a Collectible Card Game for Cybersecurity Learning." *Journal of Formative Design in Learning* 3 (1): 27–38. https://doi.org/10.1007/s41686-019-00027-0.

Tomaszewski, Brian, Amy Walker, Emily Gawlik, Casey Lane, Scott Williams, Deborah Orieta, Claudia McDaniel, et al. 2020. "Supporting Disaster Resilience Spatial Thinking with Serious GeoGames: Project Lily Pad." *ISPRS International Journal of Geo-Information* 9 (6): 405. https://doi.org/10.3390/ijgi9060405.

van Riel, Wouter, J. Post, J. Langeveld, P. Herder, and F. Clemens. 2017. "A Gaming Approach to Networked Infrastructure Management." *Structure and Infrastructure Engineering* 13 (7): 855–868. https://doi.org/10.1080/15732479.2016.1212905.

Village B. n.d. *DEF CON 33 Biohacking Village.* https://www.villageb.io/def-con-33.

Weiss, Joseph. 2010. *Protecting Industrial Control Systems.* New York: Momentum Press.

Williams, John Allen. 1978. "Crisis Management Simulation: A Survey of Exercises and Programs." *Simulation & Gaming* 9 (4): 389–403. https://doi.org/10.1177/104687817800900404.

Wray, R., L. Massey, J. Medina, and A. Bolton. 2020. "Increasing Engagement in a Cyber-Awareness Training Game." In *Advances in Human Factors in Cybersecurity,* 147–158. https://doi.org/10.1007/978-3-030-50439-7_10.

Received 16 March 2025; Revised 18 November 2025; Accepted 21 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 181-198
https://doi.org/10.55682/cdr/qgz7-pqvc

RESEARCH ARTICLE

Preparedness Wargaming for Critical Infrastructure Resilience: Taiwan Digital Blockade Wargame

Jason Vogt*, Nina Kollars, Michael Poznansky

US Naval War College, Newport, RI, USA

For any developed country, the stable conduct of life for citizens, economies, and militaries—and the capacity to govern—depends on regular access to data and communications. This reliance makes communications and data flows a strategic target, not only for criminals but also for adversaries seeking geopolitical advantage. Defending against such threats is difficult because communication infrastructures are complex, interdependent systems with no single point of control. Addressing this challenge requires militaries, governments, and the private sector to coordinate and plan for attacks and conflict in the cyber domain. This article presents the Taiwan Digital Blockade Wargame, a scenario-based exercise designed to explore ways to improve the resilience of Taiwan's information and communications technology (ICT) infrastructure in the event of a conflict with the People's Republic of China (PRC). The wargame intends to identify overlapping opportunities that militaries, industry, and policymakers could jointly implement to enhance cyber defense and societal resilience during conflict. Methodologically, the paper contributes to the emerging practice of "preparedness wargaming," a form of critical infrastructure game that moves beyond diagnosing weaknesses to generating actionable solutions for resilience and defense. By framing wargaming as a generative research method, we show how structured gameplay and facilitated dialogue can surface novel, cross-sectoral strategies not apparent to any single actor. The article reports on the game design, process, and key recommendations, and argues that such generative wargames offer a promising tool for anticipating and mitigating complex, interdependent cyber disruptions in an era of increasing geopolitical tension.

Keywords: Taiwan, cybersecurity, People's Republic of China, cyber defense strategy, wargaming, cyber resilience

* Corresponding author: jason.vogt@usnwc.edu

INTRODUCTION

In the event of a conflict between the People's Republic of China (PRC) and Taiwan, it is reasonable to expect that Taiwan's information and communications technology (ICT) infrastructure would experience severe disruptions. These disruptions could significantly limit Taiwan's ability to communicate internally with its population and externally with the international community. The Department of War (DoW) needs to better understand the critical vulnerabilities of Taiwan's ICT infrastructure, along with the key capabilities and technologies that could be used to mitigate threats and restore functionality during conflict. A gap exists in our knowledge about how to enhance defense and resilience, whether through policy or technology.

This problem is not unique to Taiwan. Data and internet access are integral to any developed society. Yet the landscape of stakeholders, managers, and maintainers of what constitutes data and internet connectivity for nations is by no means simple. Complex interdependencies leave nations vulnerable to disruption across all aspects of national security, affecting citizens' daily lives, economic stability, military coordination, and even the ability to govern effectively (Jansen et al. 2023). Effective defense therefore requires militaries, national governments, and the private sector to coordinate and plan jointly for attacks on the internet and its enabling infrastructures. In prior work, we offered early theoretical insights into the concept of "digital denial", which we define as an adversary's actions to isolate a population from connectivity to data and communications for operational or strategic gain. In that study, we examined lessons on cyber resilience drawn from Ukraine's efforts to maintain communications amid the 2022 Russian invasion (Vogt, Kollars, and Poznansky 2024). However, the value of the so-called "Zelensky Playbook" did not translate well to Taiwan's vastly different communications architecture and geopolitical situation.

As we concluded that Taiwan was much more vulnerable to digital denial operations, we turned to wargaming to better understand what could be done to better prepare Taiwan for potential conflict with China. Why a wargame? Wargamers widely agree that wargames are useful tools for exploring and understanding complex decisions in complex environments (Haggman 2019). The wargaming community of practice designs games for multiple purposes but often distinguishes between experiential/educational and analytical approaches —though this division is contested, with many authors arguing that both objectives can coexist within a single game construct (Elg 2018). Since our goal was to generate forward-looking solutions, we turned to critical infrastructure games, a growing subset of wargames focused on problems related to critical infrastructure defense (Badea et al. 2018). We refer to these types of games as "preparedness wargaming". Typically, preparedness games are focused on improving internal coordination and response processes, which can strengthen the cyber-defense posture of governments or private entities.

The difference between these types of games and our own lies in purpose. In most cases, critical infrastructure games aim to expose where stakeholders fall short of established standard. Cyberattack games serve a diagnostic function, identifying weak or incomplete security practices that already exist. For the Taiwan Digital Blockade Wargame, we modified this model by shifting the focus from diagnosing internal defense processes to generating investment solutions.

The purpose of this article is twofold. First, it provides an overview of the Taiwan Digital Blockade wargame and the recommendations it produced, with the aim of informing policy-makers, cyber defenders, and other stakeholders preparing for potential conflict. Second, it offers a contribution to the scholarly understanding of wargaming by demonstrating how such exercises can function as generative tools—capable of eliciting insights from participants beyond the typical stakeholder set. While traditional wargames often include outside experts to inspire new ideas, it is uncommon for this generative intent to serve as the primary driver of game design.

BACKGROUND

Game Setting: The Complexity of the Problem

Taiwan is one of the most digitally connected countries in Asia, with more than 90% of its population online (CIA World Fact Book 2025). This access is underpinned by a robust ICT infrastructure supported by multiple on-island telecommunications providers, an international network of undersea communications cables, and Taiwan's power industry, which is modernizing parts of its legacy energy grid with renewable and smart micro-grid technologies. Taiwan's government actively promotes these efforts through the Ministry of Digital Affairs (MODA), which is responsible for communications and cybersecurity policy, and the Ministry of Economic Affair's Energy Administration. However, ongoing disagreements between the ruling Democratic Progressive Party (DPP) and the Kuomintang (KMT)-controlled legislature on funding threaten the viability of several government-funded resilience programs.

Taiwan's domestic ICT infrastructure is supported by three major on-island telecoms providers offering mobile and fiber access (TaiwaneSim 2025). Chunghwa Telecom, the largest provider, manages several on-island data centers that support both government communications and digital civilian economy. Taiwan remains at the forefront of mobile technology deployment. Chunghwa Telcom has partnered with several multinational corporations to establish a Centralized Radio Access Network (C-RAN) architecture that enables 5G services for private users and businesses. Unlike legacy mobile networks that depend on robust base-station infrastructure, C-RAN consolidates data processing through centralized towers and facilities, improving efficiency and reducing energy costs (Ericsson 2025). These systems are underpinned by a dense network of fiber-optic cabling. Reducing energy consumption is a

major driver of Taiwan's ICT modernization, as the island's legacy energy infrastructure has struggled to meet the nation's growing power demands.

Taiwan currently relies on fifteen undersea fiber-optic cables to connect to the global internet (Mok and Huang 2024). These cables have been inadvertently or deliberately severed at least 27 times, demonstrating their vulnerability during conflict (Wu and Lai 2023). Several cables route directly through China, increasing exposure to exploitation (TeleGeography 2025). Learning from the war in Ukraine, Taiwan's leaders recognize the need to harden the island's digital infrastructure and have launched initiatives to defend against communications isolation. Taiwan's largest telecom company has signed an agreement with EutelSat OneWeb, which operates a satellite constellation similar to Starlink, to make its mobile network more resilient (EUTELSAT/ONEWEB 2025). These satellite systems are being integrated into current and planned communications architecture to help maintain connectivity to the global internet. Although they have proven resilient to signal jamming (i.e. intentional interference designed to block or degrade wireless communications), they provide only a fraction of the bandwidth available through undersea cables.

Established in 2022, the Ministry of Digital Affairs oversees national communications and cybersecurity policy. It promotes Taiwan's digital development, enhances government efficiency, develops plans for communications resilience and improves Taiwan's cybersecurity posture. In response to repeated undersea cable-cutting incidents, MODA approved the expansion of microwave relays to connect islands isolated by cable disruption (MODA 2025b). The Ministry also developed and tested a high-altitude communications balloon for use in emergency situations (MODA 2025c). MODA has also sought to improve the nation's cybersecurity posture, reduce online fraud and counter PRC disinformation campaigns (MODA 2025a).

Power generation and distribution are managed by the Taiwan Power Company (Taipower), under the Ministry of Economic Affair's Energy Administration. Roughly 80% of Taiwan's power comes from coal, oil, and liquified natural gas, nearly all imported via maritime routes, leaving supply chains vulnerable to disruption (International Energy Agency 2025). Major power outages have occurred regularly over the past decade, with some blackouts affecting over five million customers, approximately one-quarter of the population (BBC 2025). These outages have had serious implications for Taiwan's industries, especially the power-intensive semiconductor sector, which has lost hundreds of millions of dollars due to power outages. To address these challenges, Taipower and government authorities plan to invest $29 billion in smart-grid and renewable energy infrastructure upgrades by 2030 (U.S. Department of State 2025). These efforts are focused on solar and wind generation and are supported by major investments in smart-meters and on-island cloud infrastructure.

Taiwan's political landscape is dominated by the Democratic Progressive Party (DPP) and the Kuomintang (KMT), which have alternated control of the national government over the

last 25 years, leading to substantial shifts in security and defense policies towards the PRC. As of early 2025, the DPP controlled the executive branch, while the legislature was led by a KMT led coalition with the Taiwan People's Party (TPP) (The Economist 2025). To curb DPP initiatives, the KMT and TPP have sought to cut funding to government agencies, including MODA, by more than 40% (Hioe 2025). Consequently, Taiwan's communication- resilience programs face reduced budgets and delays in implementing already-funded equipment.

Despite these challenges, Taiwan is maintaining its efforts to prepare its civilian population for potential conflict. In 2024, Taiwan established a Whole-of-Society Defense Resilience Committee to strengthen civilian defense capacity in several areas, including critical infrastructure protection (Kepe and Harold 2025). The updated National Cybersecurity Strategy acknowledges that government resources alone will likely be insufficient during crisis and seeks to augment that capacity with civilian expertise. It calls for expanding domestic technology and cybersecurity industries to cultivate skilled professionals on-island who could serve in a cyber-reserve force (Waligora 2025). A more mature and diverse tech sector is viewed as an enabler to strengthen digital resilience across society.

Although the Taiwan Digital Blockade Wargame did not explicitly examine the implications of Taiwan's current political dynamics, it remains critical for U.S. policymakers to understand that Taiwan's government and population are not unified in their approach to the PRC. This means that funding for security initiatives is potentially prone to volatility, which may necessitate future shifts in infrastructure investment priorities and strategies over the coming years. External funding sources, therefore, may provide the stability required to enhance Taiwan's ICT infrastructure resilience.

Wargaming to Generate New Solutions

Wargames have long been used by the military to train officers, evaluate war plans and examine new operational approaches (Curry 2012). According to wargaming expert Peter Perla, a wargame is defined as a "model involving people making decisions in a synthetic environment of competition or conflict, in which they see the effects of their decisions on that environment and then get to react to those changes" (Perla 2022, 200). Although wargames include inputs from operations research and other quantitative methods, it is the focus on human decision-making and their ability to provide an immersive experience, which make them distinct from other forms of analysis.

Over the past decades, wargames have been adapted to simulate organizational responses to real-world problems, including cyber-attacks, natural disasters and public health emergencies. These "preparedness" games frequently bring together stakeholders across government and industry to test strategies and coordination mechanics, while simultaneously building trust among the people and organizations that must work together to effectively respond to a crisis (Fedina and Lucas 2025). For example, the North American Electric Reliability

Corporation (NERC) and its Electricity Information Sharing and Analysis Center (E-ISAC) developed a wargame called *GRIDEX*, which enables utility providers and government agencies to practice their response and recovery actions in response to cyberattacks (Duncan 2023). There are numerous examples, but a key feature of these preparedness games is that they are typically focused on internal stakeholders and organizational processes required to respond to incidents.

As the threats to Taiwan have intensified in recent years, researchers have increasingly used wargames to help them understand different aspects of the conflict. Researchers at the Center for Strategic and International Studies have conducted two wargames examining Taiwan, one of which is focused on military responses to a major attack and another which examines economic factors that would likely result from a prolonged blockade of key resources, which can affect electrical power and other infrastructure (Cancian, Cancian, and Heginbotham 2023, 2025). Earlier this year, researchers at Syracuse placed players in the role of the PRC's government and military to study whether the role reversal would generate valuable insights for U.S planning (Michaels and Williams 2025).

The difference between conventional, cyber and critical infrastructure games lies in purpose. In most cases, critical infrastructure games aim to expose where stakeholders fall short of established standard. Cyberattack games serve a diagnostic function, identifying weak or incomplete security practices that already exist. More conventional wargames look for opportunities or weaknesses in military approaches to a problem. For the Taiwan Digital Blockade Wargame, we used a blended approach to the scenario, which included elements of conventional warfare, cyberattacks, electromagnetic warfare and covert sabotage of critical infrastructure. Instead of focusing on internal defense processes, we used the game to generate investment solutions.

The practical value of wargaming as a mechanism to interrogate complex contexts and discover potential solutions is well-established (Hirst 2020). Wargaming as a solution generation tool is not unique, but it is seldom explicitly articulated as such in the literature. As in much of the wargaming community, the generative function tends to be embedded in tacitly applied techniques [1]. In this sense, playing the game allows players (while they may also be learning) and facilitators (while they may be collecting data for sentiment analysis) to move through an abstraction of reality that stimulates the creation of solutions not previously known to any individual party prior to game play. In so doing, wargames can produce new insights and strategies that provide clarity under conditions of complexity and uncertainty (Perla 2022).

1. While we do not elaborate here on the structure and function of communities of practice (COPs), there is a robust literature on the nature of practice and the knowledge they produce. See for example: (Wenger-Trayner and Wenger-Trayner 2015)

TAIWAN DIGITAL BLOCKADE WARGAME: GAME DESIGN, SCENARIO AND PLAY

The Taiwan Digital Blockade Wargame's overarching objective is to improve the defense of Taiwan's critical infrastructure, by bringing in outside perspectives who could potentially help generate novel solutions to the problems facing Taiwan. This section provides an overview of the game design. Further details are available in the full game report (Vogt and Kollars 2024).

Participants

In August 2024, we organized game sessions at DEFCON (https://defcon.org) and Blackhat (www.blackhat.com), two of world's largest multi-day cybersecurity conventions, which took place in Las Vegas, Nevada (USA). We recruited 27 players with backgrounds in cybersecurity, industrial control systems, data center operations, threat intelligence, subsea cabling systems and other areas. Players were identified and selected in the months preceding the game via outreach through trusted networks and some social media outreach. Players were invited to apply for a slot in the game, and the research team selected the participants based on their technical skill set. Two teams of players were selected and notified prior to the event.

The first iteration of the game was executed in a private conference suite during Blackhat and included 12 players, whereas the second was executed on the open DEFCON conference floor and involved 15 players. Each session lasted about 3 hours in total. In each game, players were placed on three teams, with the goal of having a mix of skills and backgrounds on each team. For example, there were many players with backgrounds in cyber threat intelligence, but fewer with direct experience with Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, so the game team ensured that at least one person with that expertise was assigned to each team.

Game Overview

The game placed players into the role of advisors to the government of Taiwan. Players were divided into advisory councils and presented with two conflict vignettes depicting a PRC invasion of Taiwan in 2030. In the first vignette, the PRC refrained from conventional military attacks, relying instead on cyber operations, electronic warfare, and sabotage to disrupt civilian communications and power infrastructure. In the second vignette, the PRC launched a full-scale kinetic attack, including against critical infrastructure. The PRC's overarching goal in both cases was to isolate the Taiwanese government in Taipei from its domestic population and the international community.

At the start of each round, advisory councils were briefed on the degraded state of Taiwan's infrastructure. Teams then discussed what investments Taiwan should make in the coming

years to mitigate the damage anticipated in 2030. Players then voted for the team whose recommendations they believe were most effective.

Players' recommendations were categorized into three investment domains: infrastructure, cybersecurity, and recovery. Infrastructure investments referred to the purchase of physical equipment that forms part of the ICT or energy infrastructure. Cybersecurity investments encompassed software-based solutions or industry best practices aimed at enhancing cyber resilience. Recovery investments focused on post-attack measures to restore damaged or inoperable infrastructure. Players were not provided with budgetary constraints and were encouraged to propose ideas freely.

Game Schedule

The full game session, including the introduction and two gameplay moves, lasted approximately three hours (Table 1).

Table 1. Overview of Game Activities and Scenario Play Structure

Activity	Duration	Description
Introduction	30 min	Players were divided into advisory councils (teams). The game team and participants introduced themselves, highlighting their expertise. A briefing followed, outlining the game's purpose, Taiwan's ICT and power context, gameplay mechanics, desired outcomes, and logistics. Players had time for questions before starting.
Move 1 – Scenario Play	1 h 15 min	The first vignette was presented, describing the initial phase of conflict. The move was structured as follows: • **Red Action (10 min):** Facilitators presented hostile actions and situational changes. • **Team Planning (30 min):** Teams discussed mitigation and investment options in infrastructure, cybersecurity, and recovery. • **Team Presentations – Infrastructure (10 min)** followed by Voting (5 min). • **Team Presentations – Cybersecurity (10 min)** followed by Voting (5 min). • **Team Presentations – Recovery (10 min)** followed by Voting (5 min). Facilitators recorded discussion points and outcomes.
Move 2 – Scenario Play	1 h 15 min	The second vignette introduced a full-scale kinetic attack. The same cycle was followed: brief overview (*Red Action*, 10 min), 30 min team planning, presentations of recommendations across the three investment categories (10 min each), and individual voting after each round (5 min each).

Scenario Overview

The scenario presented to players was set on August 6, 2030. Relations between the PRC and Taiwan had deteriorated to the breaking point due to the re-election of a liberal, pro-independence party. Rhetoric towards independence was at an all-time high, and several government representatives had openly called for UN recognition of Taiwan as an independent state. The Central Committee of the Communist Party (CCCP) deemed the risk of Taiwan declaring independence high enough to warrant military intervention and began preparations for invasion.

With little chance of surprise, the PRC sought to disrupt Taiwan's military and civilian communications prior to the assault. To avoid a direct intervention by the U.S., the PRC initially decided to limit kinetic attacks on the island prior to the launching of amphibious forces. However, they were willing to conduct operations using cyber, electronic warfare and clandestine sabotage prior to the invasion. The Taiwanese government, aware of the impending attack, had decided to prioritize maintaining government and civilian communications at peak levels to enable military coordination with allies and show resolve in the face of PRC aggression.

Vignette 1: Non-Kinetic Attacks. The first vignette presented to players depicted a non-kinetic campaign preceding conventional military strikes on the island. To justify their actions with the goal of disrupting civilian infrastructure to support the war effort, PRC accused Taiwan of illegally using high bandwidth communications to import and export proprietary (Chinese) materials. Multiple submarine fiber-optic cables connecting Taiwan to the global internet were physically severed; while cyberattacks targeted cable landing stations, further disrupting the flow of international internet traffic to the island. The remaining undersea cables running directly to the PRC mainland remained operational but were monitored by PRC authorities.

In this scenario, the PRC also employed airborne electronic warfare platforms to disrupt GPS signals and commercial satellite ground stations integrated with civilian ICT infrastructure. These disruptions were described as episodic, varying according to platform location. Additionally, data centers hosting email servers for several major internet providers were targeted with ransomware. While commercial mobile networks remained largely functional, service degradation occurred in areas suffering electrical power outages.

For each game, players were briefed on the first vignette and shown a map of degraded ICT infrastructure across Taiwan. Teams then discussed mitigation strategies. Once discussions were complete, each team presented their recommendations to the other teams and voted. The winning teams often proposed lower cost, easily distributed systems that could be rapidly deployed across multiple regions.

Vignette 2: Kinetic Attacks. The second vignette presented to players simulated the opening phase of a conventional attack on Taiwan's infrastructure prior to the invasion. The PRC conducted missile strikes to suppress Taiwan's air power, close airfields, and ensure that no aircraft could operate within Taiwanese airspace. Missile strikes also targeted Taiwan's power transmission infrastructure but spared power production facilities. Taiwan's national command-and-control systems and data centers, including associated power systems, were hit directly.

Data centers supporting microgrid electrical power distribution were infected with malware that encrypted data related to customer smart-meter identification and usage. Engineering

workstations managing industrial control systems responsible for microgrid operations lost visibility of routers and sensors monitoring power fluctuations. As a safety measure, all renewable power generation systems connected to microgrids were shut down, reducing Taiwan's energy capacity by 20%. Power outages rippled across manufacturing sectors, forcing most semiconductor manufacturing facilities offline. Malicious cyber actors also targeted security and traffic control systems taking some offline and causing malfunction in others, which led to confusion and traffic jams in several urban areas. Meanwhile, PRC forces also engaged in jamming all remaining microwave and satellite backbone.

Despite the escalation to large-scale conventional attacks in the second vignette, most teams did not fundamentally alter their strategies or recommendations. Stockpiling communications equipment and spare electrical-grid components have utility across multiple scenarios, including those unrelated to inter-state conflict, such as earthquakes or other natural disasters. This dual-use framing suggests a politically viable pathway for governments to justify certain expenditures as part of general disaster preparedness rather than explicit war planning.

WARGAME OUTCOMES: PLAYER-DERIVED SOLUTIONS FOR CRITICAL INFRASTRUCTURE RESILIENCE

Overview of Player Recommendations

Across the two wargames, players generated 65 recommendations aimed at improving Taiwan's critical infrastructure resilience. Approximately 70% focused on infrastructure investments, including communications systems, power generation and storage, and data backup and distribution capabilities. Another 20% of recommendations addressed recovery, emphasizing the stockpiling of critical spare parts and the development of technical skills among civilians. The remaining 10% centered on cybersecurity, primarily through cryptography and related methods to enhance communications security.

Players were not provided with budgetary constraints and were instructed not to constrain their recommendations based on finances.

In post-game analysis, all recommendations were evaluated and categorized by estimated cost (high, moderate, low) and implementation timeline (short-term, 1-2 years; medium-term, 2-4 years; long-term, 4+ years). Taken individually, two-thirds of the recommendations were judged to be low- to moderate cost and executable within one to four years —feasible under a 2030 conflict scenario. The remaining third were deemed high-cost, long-term or both, making it unlikely they would be available in a 2030 invasion scenario. Included in the high-cost group were several recommendations related to the use of modular nuclear reactors, which were also deemed to be politically unfeasible at this time. These high-cost/long-term recommendations were excluded from subsequent analysis due to limited practicality.

Thematic Areas of Recommendation

Communications infrastructure and cybersecurity. Recommendations related to communications infrastructure and cybersecurity were generally the least expensive and had the shortest implementation timelines. Many involved adapting or expanding existing technologies, including HAM radios, microwave relays, P-LEO satellite communications, long-range radio mesh networks, and drone- or balloon-based relays to maintain connectivity during disruption. Players also generated several novel concepts for enabling communications, such as using Bluetooth-based secure messaging services that function without mobile towers and implementing cryptographic protocols—including blockchain techniques— to verify message authenticity and ensure communications originated from trusted sources.

Power generation, data storage, and recovery. Recommendations involving power generation and storage, data backup and distribution, and stockpiling critical spares were judged to be more costly and potentially more difficult to implement. Players called for the expanded use of renewable power generation (wind, solar, and hydro), the establishment of distributed containerized data centers to provide reliable data backups, and options for stockpiling critical spares for power generation and network operations. The costs associated with stockpiling critical spares could vary greatly depending on type, quantity and means of storage implemented.

Civilian preparedness and skills development. Preparing the civilian population for conflict was another area discussed extensively by the participants. The amount of training and resources dedicated to these efforts could range from basic cybersecurity training programs to the creation of an elite civilian cyber corps. The costs could vary significantly depending on scale, scope, and depth of programs implemented.

EMERGENT STRATEGIC APPROACHES

Three overarching strategic approaches to enhancing Taiwan's ICT resilience strategies emerged during gameplay (Table 2):

(1) **the decentralized strategy** would distribute lower cost assets across the population centers, saturating the environment and complicating the PRC's ability to target critical nodes
(2) **the centralized strategy** would concentrate critical infrastructure near targets the PRC is unwilling to strike
(3) **the interior strategy** would focus on building infrastructure and stockpiling critical spares in mountainous areas and the eastern side of the island to enable communications during a protracted conflict.

Each strategy requires prioritizing different types of investments to achieve optimal results.

Table 2. Strategic Approaches: Technologies, Benefits, and Drawbacks

Strategic Approach	Critical Technologies	Benefits	Drawbacks
Decentralized - distribute infrastructure throughout neighborhoods and towns	Solar power, P-LEO SATCOM, HAM, LoRa, distributed data, battery and repair parts	Maximizes civilian connectivity and self-sufficiency	High cost; requires civilian training and willingness to fight
Centralized - concentrate infrastructure around key manufacturing sites	Larger scale wind/solar power plants paired with data centers, large-scale battery back-ups	Requires smaller workforce to operate or maintain	Limited number of locations, population must relocate to sites
Interior - stockpile equipment in mountainous regions and the Eastern side	Solar power, microwave relays, ariel comms balloons/drones, P-LEO SATCOM, HAM, LoRa	Maximizes protection from attacks	Requires the infrastructure to be operated in difficult terrain

Decentralized Systems: Too Many Targets

A decentralized strategy favors the distribution of infrastructure to avoid the pitfalls of concentrating too many critical assets in one location. This approach can rely on many types of technologies, including many low-cost off-the-shelf technologies such as HAM radios and Long Range Radio Access (LoRa) systems. These solutions were among the most frequently suggested by players and most favorably received during voting sessions.

To be successful, the government would need to prioritize solar power generation, which can be widely dispersed, and connect it to existing mobile infrastructure. This would enable communications if large power stations and transformers go offline. The mobile infrastructure would also need to be locally connected to P-LEO satellite base stations to enable off-island internet communications. Low-cost communications devices, such as HAM and LoRa radio systems, could serve as backups if mobile infrastructure is rendered inoperable.

The government would need to invest significant time and resources to train civilians to operate and repair these systems, as well as stockpiling batteries, repair parts and replacement systems throughout the country. Well-executed, a decentralized strategy could maximize the number of civilians able to maintain communications during conflict.

High cost and the willingness of the population to participate in a decentralized strategy are the primary barriers to its execution. The government could potentially incentivize the expanded use of solar power through subsidies, but it is likely that much of the equipment would need to be purchased and distributed with government funds. Training the population would also require significant resources, without which much of the equipment would be useless. Taiwan's military or government could establish civilian training programs or even establish a civilian cyber corps to help operate the systems, but unless participation was made compulsory there is a risk that the numbers that receive training would be insufficient.

Centralized Systems: Targeting May Be Unappealing to Adversaries

A centralized strategy assumes that the PRC may be reluctant to target key manufacturing sites and certain cultural artifacts, creating safe zones where civilian power and communications infrastructure could be concentrated. The sites identified by the players included areas dedicated to the production of semiconductors, along with museums and institutions housing important Chinese cultural artifacts. The idea builds on the "silicon shield" concept, which suggests that China would avoid destroying or disrupting industries vital to its own economy, such as semiconductor imports, which could entice a response from the U.S. who is also dependent on them (Institute for Security and Development Policy 2025). In this case, China is still willing to invade Taiwan, but would be unwilling to target key manufacturing areas with conventional attacks, thereby limiting damage to critical infrastructure located in these areas. Players advocating for this strategy recommended building up renewable power infrastructure, data centers, and communications nodes within these zones. This would create safe zones where civilian refugees could maintain communication and shelter during conflict.

A centralized strategy has several advantages, not least the fact that Taiwan's government is already prioritizing renewable power investments, particularly wind and solar projects located near key manufacturing sites. This approach aligns well with existing national energy initiatives and could be further strengthened by integrating data centers into these zones, along with the capability to connect to one or more P-LEO satellite constellations. Such an integration would allow segments of the population to maintain communications with the outside world at a relatively low cost. Because the number of locations would be limited, the infrastructure could be managed by the government or trained private-sector professionals, reducing the need for large-scale civilian training.

The drawbacks of a centralized strategy include the restricted number of sites available, meaning that large portions of the population are unlikely to benefit from their existence. Located primarily along urban coastal areas, these sites would also remain especially vulnerable to electronic warfare, potentially leading to temporary disruptions to services. Moreover, because these locations are already deemed to be of high value to the PRC, the development of additional infrastructure could incentivize the PRC to seize these areas earlier in the conflict than it would otherwise. Lastly, in the event of a protracted conflict, there is no guarantee the PRC will limit its conventional strikes on these areas, particularly if it decides to prioritize the destruction of civilian infrastructure as a key objective of its military campaign.

Interior Shelters: Using Geography as a Strength

The interior strategy leverages Taiwan's geography by positioning power and communications infrastructure within its mountainous eastern regions, away from its vulnerable western coastline. This strategy prioritizes building and stockpiling equipment in forests, mountainous regions, and coastal areas on the eastern side of the island. Stockpiling and pre-positioning

are central to this strategy, and players who advocated for it often described using mountain caves and other natural formations to shield systems from attack. These systems could be positioned in such a way that it maximizes their protection against conventional attacks and disruptions from electronic warfare systems.

The development of solar power infrastructure would need to be prioritized, complemented by hydroelectrical systems already operating in some mountainous areas. Mobile networks could be established using balloons or aerial drones, while microwave relays spanning across the mountain ranges could transmit data over long distances. Satellite ground stations could be hidden throughout the mountains to enable off-island communications, and HAM radios could serve as an additional backup layer.

The interior strategy could pair well with the establishment of a small cadre of technically trained civilians, capable of operating and maintaining the systems throughout the conflict. Should the conflict become protracted, this strategy would likely sustain communications for a longer period than either the decentralized or centralized strategies, as most infrastructure would be located in areas difficult for the PRC to reach. The principal drawback to the interior strategy, however, lies in the logistical and financial challenges of building and operating systems in rugged terrain. Although fewer installations would be required than in a decentralized strategy, the approach remains costly. Civilians would also have to relocate away from coastal areas to take advantage of the services, which may not be possible for much of the population.

IMPLICATIONS FOR FUTURE PLANNING

The full implementation of civilian training programs, energy resilience measures, and communications systems hardening is beyond the current capacity of Taiwan's government. In this context, strategic planning, and targeted international cooperation will be key. Future planning should carefully consider three key factors: the cost of each system, the technical expertise required to operate and maintain it, and its utility within an overarching national resilience strategy. Further research in these areas is highly recommended.

Many of the technologies and initiatives recommended by the players involve significant start-up and sustainment costs, which must be weighed against their operational value in a conflict scenario. Some technologies, such as P-LEO satellite terminals, are versatile enough to be useful in multiple scenarios, but planners still need to avoid overinvesting in any single platform, particularly if their chosen strategy is not overly dependent on it. Other systems - particularly those that come with higher costs - need to be considered carefully before committing to them. For example, establishing a network of containerized data centers may be an effective way to ensure the integrity of the government information systems on-island, but may prove more expensive than offshoring data to a friendly nation. Conversely, if those

data centers are also used to sustain the island's internal internet connectivity, then prioritizing investments in those systems may be of greater importance. Opportunities for private sector subsidization by U.S. federal grant funding could significantly reduce the costs to speed up the implementation of either of these solutions.

The success of many of these programs will also heavily depend on the population's willingness and capacity to participate in training and operational support. In general, the broader and more distributed the systems are, the larger the number of trained participants required. If a technology is already familiar to the population and easy to use, such as mobile phone applications, then the burden of training the population to use the system is relatively low. However, if the technology requires specialized hands-on training, like HAM radios, the burden can be substantially higher and limit scalability. Tying these investments to non-military goals, such as natural disaster preparedness, may improve the population's willingness to participate in the programs. Ultimately, the government's ability to entice or compel the population to dedicate time to learning how to operate and repair certain systems will be critical to the success of any resilience plan.

The results of the game should be considered within the construct of Taiwan's National Cybersecurity Strategy. The strategy outlines plans for whole-of-society resilience programs and critical infrastructure defense that match well with game findings pointing to the importance of civilian training and preparedness for keeping Taiwan connected during a sustained conflict. The strategy places significant emphasis on building up Taiwan's domestic cybersecurity industry to help maintain internet connectivity during a crisis (Taiwan National Security Council 2025). While budget shortfalls may stymie the progress of some of these initiatives in the short-term, the game findings suggest that anything the government can do to train and educate civilians on cybersecurity practices and basic communications technology could yield substantial benefits during a conflict.

While this game was focused on the resilience of civilian communications infrastructure, we should not overlook the direct military applications of these approaches, which is the focus of most other literature on this topic. Robust, distributed civilian communications, will likely enhance the Taiwanese military's capacity to coordinate actions against a PRC invasion and provide alternatives if military communications are disrupted or destroyed. Furthermore, the investment strategies referenced above can also be paired with different military approaches, such as those that call for decentralized command & control or asymmetric tactics should the PRC gain a foothold on the island (Rodriguez 2025).

Finally, while the solutions and insights generated by the wargame offer valuable guidance for cyber resilience planning, the process of conducting the game itself also produced important outcomes. Bringing together experts from across ICT security firms helped solidify the professional networks through which responders can communicate and plan. In several instances, former players attended post-game briefings to hear feedback from others. Notably,

members of Taiwan's Ministry of Digital Affairs observed one of the game sessions, and invited the game team to conduct a follow-on exercise in Taiwan in 2025, demonstrating how playing the game has itself helped strengthen the network.

CONCLUSION

The Taiwan Digital Blockade Wargame was designed to elicit ideas from the private sector on how Taiwan's government could invest to strengthen its ICT infrastructure. The significant variation in recommendations and strategies generated by the players underscores that there is no single approach to the challenge of enduring digital resilience. This diversity of perspectives highlights the need for Taiwan's government to adopt a comprehensive and flexible strategy, one that integrates selected ideas such as those presented here, to guide future investment and preparedness decisions.

Taiwan must ultimately balance its financial capacity with the level of civil-military preparedness its population is willing to embrace. Both factors are likely to evolve over time, requiring policymakers engaged in preparedness planning to capitalize on favorable moments for investments while being ready to defend expenditures when budget is under greater scrutiny. In the end, the willingness of the civilian population to take an active role in safeguarding their nation's ICT infrastructure may prove to be the most critical determinant of its overall resilience.

ABOUT THE AUTHORS

Jason Vogt is an assistant professor and a core faculty member of the Cyber & Innovation Policy Institute at the U.S. Naval War College. Vogt previously worked for the Defense Intelligence Agency and served on active duty as an Army officer. He specializes in cyber and wargaming.

Dr. Nina Kollars is an associate professor and a core faculty member of the Cyber & Innovation Policy Institute at the U.S. Naval War College. Kollars advises on issues of military modernization and emerging technology. In her free time, she manages a community of White hat, hackers who focus on maritime vulnerabilities. Her primary areas of research are in emerging technologies, cybersecurity, and military innovation.

Dr. Michael Poznansky is an associate professor and a core faculty member of the Cyber & Innovation Policy Institute at the U.S. Naval War College. He is the author of *Great Power, Great Responsibility: How the Liberal International Order Shapes US Foreign Policy* (Oxford University Press, 2025) and *In the Shadow of International Law: Secrecy and Regime Change in the Postwar World* (Oxford University Press, 2020).

ACKNOWLEDGMENTS

The authors thank Dan Grobarcik, Ed McGrady, and Frank Smith for their assistance in game development and feedback. The authors also thank participants at Blackhat and DEFCON for contributing their time and insights, as well as the ICS Hacking Village for hosting us at DEFCON. This project underwent IRB review (NWC.2024.0008-DD-N).

REFERENCES

Badea, Dorel, Marin Marian Coman, Dumitru Iancu, and Olga Bucovețchi. 2018. "Critical Infrastructure Protection in the Knowledge Society: Increasing the Safety Level by Use of Learning Based on Wargaming Expertise." *BRAIN. Broad Research in Artificial Intelligence and Neuroscience* 9 (4): 38–48.

BBC. 2025. *Taiwan: Massive Power Outage Affects Five Million Households.* March 2, 2025. https://www.bbc.com/news/world-asia-60598234.

Cancian, Mark F., Matthew Cancian, and Eric Heginbotham. 2023. *The First Battle of the Next War: Wargaming a Chinese Invasion of Taiwan.* Center for Strategic / International Studies. https://www.csis.org/analysis/first-battle-next-war-wargaming-chinese-invasion-taiwan.

Cancian, Mark F., Matthew Cancian, and Eric Heginbotham. 2025. *Lights Out: Wargaming a Chinese Blockade of Taiwan.* Center for Strategic / International Studies. https://www.csis.org/analysis/lights-out-wargaming-chinese-blockade-taiwan.

CIA World Fact Book. 2025. *Field Listing – Internet Users.* https://www.cia.gov/the-world-factbook/field/internet-users/.

Curry, John. 2012. *Peter Perla's The Art of Wargaming: A Guide for Professionals and Hobbyists.* History of Wargaming Project.

Duncan, Matthew. 2023. "The Evolution of the North American Electrical Reliability Corporation's Grid Security Exercise." In *Cyber Wargaming,* edited by F. Smith, N. Kollars, and B. Schechter, 137–138. Washington, DC: Georgetown University Press.

Elg, Johan. 2018. "Wargaming in Military Education for Army Officers and Officer Cadets." PhD diss., King's College London. https://kclpure.kcl.ac.uk/portal/en/studentTheses/wargaming-in-military-education-for-army-officers-and-officer-cad/.

Ericsson. 2025. *Chunghwa Telecom Shows the Way Forward.* https://www.ericsson.com/en/cases/2022/chunghwa-telecom-and-ericsson.

EUTELSAT/ONEWEB. 2025. *Chunghwa Telecom Selects Eutelsat OneWeb for Low Earth Orbit (LEO) Satellite Services.* November 15, 2025. https://oneweb.net/resources/chunghwa-telecom-selects-eutelsat-oneweb-low-earth-orbit-leo-satellite-services.

Fedina, Katja, and Rebecca Lucas. 2025. *Building Societal Resilience Through Wargaming.* RAND Corporation (April 2025). https://www.rand.org/pubs/commentary/2025/04/building-societal-resilience-through-wargaming.html.

Haggman, Andreas. 2019. "Cyber Wargaming: Finding, Designing, and Playing Wargames for Cyber Security Education." PhD diss., Royal Holloway, University of London.

Hioe, Brian. 2025. *Amid KMT Budget Cuts, Taiwan's DPP Proposes Raising Defense Spending.* The Diplomat (February 18, 2025). https://thediplomat.com/2025/02/amid-kmt-budget-cuts-taiwans-dpp-proposes-raising-defense-spending.

Hirst, Aggie. 2020. "States of Play: Evaluating the Renaissance in US Military Wargaming." *Critical Military Studies* 8 (1): 1–21. https://doi.org/10.1080/23337486.2019.1707497.

Institute for Security and Development Policy. 2025. *The Silicon Shield Erosion: Fortifying Taiwan Against Geopolitical Shocks.* https://www.isdp.eu/the-silicon-shield-erosion-fortifying-taiwan-against-geopolitical-shocks/.

International Energy Agency. 2025. *Chinese Taipei.* https://www.iea.org/countries/chinese-taipei.

Jansen, Bernardus, Natalia Kadenko, Dennis Broeders, Michel van Eeten, Kevin Borgolte, and Tobias Fiebig. 2023. "Pushing Boundaries: An Empirical View on the Digital Sovereignty of Six Governments in the Midst of Geopolitical Tensions." *Government Information Quarterly* 40 (4): 101862.

Kepe, Marta, and Scott W. Harold. 2025. *Building Taiwan's Resilience: Insights into Taiwan's Civilian Resilience Against Acts of War.* Santa Monica, CA: RAND Corporation. https://www.rand.org/pubs/research_reports/RRA3388-1.html.

Michaels, Jeffery, and Michael Williams. 2025. *A Wargame to Take Taiwan, from China's Perspective.* War on the Rocks (October 7, 2025). https://warontherocks.com/2025/10/a-wargame-to-take-taiwan-from-chinas-perspective/.

MODA (Ministry of Digital Affairs). 2025a. *Deputy Minister Herming Chiueh Attends International Cybersecurity Conference, Sharing Taiwan's Experience in Cybersecurity and Communication Resilience.* https://moda.gov.tw/en/press/press-releases/13324.

MODA (Ministry of Digital Affairs). 2025b. *Response of Ministry of Digital Affairs to Chunghwa Telecom's Subsea Cable Disruption on January 3, 2025.* January 3, 2025. https://moda.gov.tw/en/press/press-releases/14990.

MODA (Ministry of Digital Affairs). 2025c. *The Ministry of Digital Affairs Demonstrates High-Altitude Communication Platform to Strengthen Taiwan's Communication Resilience.* https://moda.gov.tw/en/press/press-releases/14322.

Mok, Charles, and Kenny Huang. 2024. *The Most Critical Resilience Questions of Them All: Taiwan's Undersea Cables.* University of Nottingham Taiwan Research Hub (October 2, 2024). https://taiwaninsight.org/2024/10/02/the-most-critical-resilience-questions-of-them-all-taiwans-undersea-cables/.

Perla, Peter. 2022. "Wargaming and the Cycle of Research and Learning." *Scandinavian Journal of Military Studies* 5 (1): 197–208. https://doi.org/10.31374/sjms.124.

Rodriguez, Tyler. 2025. "The Inevitable Invasion is Over, Now What? Resistance in a Post-Invasion Taiwan." *Small Wars Journal* (August 18, 2025). https://smallwarsjournal.com/2025/08/18/the-inevitable-invasion-is-over-now-what-resistance-in-a-post-invasion-taiwan/.

Taiwan National Security Council. 2025. *National Cybersecurity Strategy 2025.* National Information and Security Office.

TaiwaneSim. 2025. *Taiwan Mobile Operators: Which One Is the Best?* https://taiwanesim.com/mobile-operators/.

TeleGeography. 2025. *Submarine Cable Map.* https://www.submarinecablemap.com/submarine-cable/flag-north-asia-loopreach-north-asia-loop.

The Economist. 2025. *Taiwan's Political Drama Is Paralysing Its Government.* January 23, 2025. https://www.economist.com/asia/2025/01/23/taiwans-political-drama-is-paralysing-its-government.

U.S. Department of State. 2025. *2024 Investment Climate Statements: Taiwan.* Technical report. https://www.state.gov/reports/2024-investment-climate-statements/taiwan/.

Vogt, Jason, and Nina Kollars. 2024. *Taiwan Digital Blockade Wargame Report.* U.S. Naval War College. https://usnwc.edu/_images/portals/0/NWCDepartments/Cyber--Innovation-Policy-Institute/CIPI-Taiwan-Digital-Blockade-Distro-A2900.pdf.

Vogt, Jason, Nina Kollars, and Michael Poznansky. 2024. "Should Taiwan Attempt to Replicate the Zelensky Playbook." War on the Rocks, May 15, 2024. https://warontherocks.com/2024/05/should-taiwan-attempt-to-replicate-the-zelensky-playbook/.

Waligora, Erik. 2025. *Advancing Cyber Resilience: Taiwan's Strategic Shift in the Seventh Phase of Its National Cybersecurity Program.* Global Taiwan Brief 10, no. 14 (July 2025). https://globaltaiwan.org/2025/07/advancing-cyber-resilience-taiwans-strategic-shift/.

Wenger-Trayner, Etienne, and Beverly Wenger-Trayner. 2015. *Introduction to Communities of Practice: A Brief Overview of the Concept and Its Uses.* https://wenger-trayner.com/introduction-to-communities-of-practice/.

Wu, Huizhong, and Johnson Lai. 2023. *Taiwan Suspects Chinese Ships Cut Islands' Internet Cables.* Associated Press (April 18, 2023). https://apnews.com/article/matsu-taiwan-internet-cables-cut-china-65f10f5f73a346fa788436366.

Received 8 March 2025; Revised 20 October 2025; Accepted 5 November 2025

✧ Educating and Empowering the Workforce ✧

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 201-223
https://doi.org/10.55682/cdr/ys0t-9tc9

PROFESSIONAL COMMENTARY

Strengthening Cyber Resilience by Building Critical Infrastructure Communities: the C-CIC Pilot Study

Anne M. Chance*[1], Volker Franke[12], Timo A. Zwarg[2]

[1]TRENDS Global, Marietta, GA, USA
[2]Kennesaw State University, Kennesaw, GA, USA

Community resilience is crucial in addressing cyber threats to critical infrastructure, as these threats are often complex and require a multi-layered approach. In this paper, we explore how practices used to build trust and mutual support in face-to-face communities can be adapted to strengthen cyber resilience. Specifically, we apply the idea of community resilience as an effective response to cyber threats by examining the importance of building trust and social capital and discussing lessons learned from a pilot project designed to establish an intentional online cyber critical infrastructure community (C-CIC) in the metro Atlanta area. By analyzing the interplay of technological affordances, social norms, and individual behaviors, this research offers a deeper understanding of how trust shapes the structure and function of resilient cyber community ecosystems. Based on lessons learned from the Atlanta C-CIC pilot, the paper concludes with recommendations for building effective intentional online cyber critical infrastructure communities.

Keywords: cybersecurity, critical infrastructure, community-building, resilience, trust, online community, social capital

* Corresponding author: anne@trendsglobal.org

1 INTRODUCTION

> Our nation's critical infrastructure—the services Americans rely on every day—is under continuous threat by nation-state cyber adversaries and cybercriminal organizations around the globe. Over the last several years, we've witnessed increasingly frequent and complex attacks against small and medium-sized businesses, K-12 schools, water utilities, and healthcare organizations, including hospitals, which were in the past considered "off-limits." - Nitin Natarajan, Deputy Director Cybersecurity and Infrastructure Security Agency (CISA), January 7, 2025

Critical infrastructure provides services essential for the functioning of a productive modern society; it encompasses utilities, finance, healthcare, telecommunication, and emergency services, among others. In recent years, critical infrastructure has increasingly been the target of cyberattacks around the globe. In the spring of 2018, cybercriminals launched a ransomware attack against the city of Atlanta that restricted access to a wide range of online platforms, municipal operations, and databases. Although the city did not pay the ransom, the attack resulted in millions of dollars in damage, and it took several months for services to be fully restored (Young 2021). Beginning in 2019, the Russian Foreign Intelligence Service (SVR) attacked the computing networks of the Texas-based SolarWinds network management software company. SVR inserted malicious code into a routine software update, which allowed them to gain widespread access to government agencies and Fortune 500 companies (Government Accountability Office 2021). In May 2021, hackers disrupted operations of the Colonial Pipeline, causing fuel shortages and panic buying across the Eastern Seaboard (Wood 2023). These examples illustrate the different ways threat actors exploit the vulnerabilities of both public and private sector critical infrastructure organizations.

To test and improve critical infrastructure resilience against cyberattacks, the Army Cyber Institute (ACI) developed *Jack Voltaic*, a cyber research project and exercise series. *Jack Voltaic* brings together military and civilian partners, including local/city governments and private companies. Since 2016, ACI and partners have iteratively designed and conducted these exercises to stress-test collective responses to cascading cyber incidents. The exercises repeatedly revealed the same critical gap: technical systems often fail because the humans responsible for protecting them lack the social infrastructure necessary for coordinated response at scale (ACI 2021a, 2018, 2021b, 2022). As the *Jack Voltaic 3.0 Research Report* bluntly states, "crisis management and remediation is personality driven" and municipalities "tend to lack experience with real cyber events and thus have difficulty visualizing second-, third-, and fourth-order effects." The exercises have consistently shown that cyber resilience depends on personal relationships and the need for institutionalization (ACI 2021a).

We developed the *Critical Sherpas* pilot in metro Atlanta to test a core hypothesis derived from the *Jack Voltaic* exercises: that establishing pre-incident social networks is essential for effective cyber defense. This intentional online community serves as a laboratory for

adapting face-to-face trust-building to a digital environment. The moniker *Critical Sherpas* reflects the community's vital role as expert guides who navigate the treacherous terrain of modern cyber threats on behalf of the public.

Community psychology and sociological research demonstrate that key factors strengthening resilience in physical communities are trust, social capital, and mutual aid networks (Norris et al. 2008; Tierney 2019). Starting with the assumption that the same principles apply to cyber defense (Castelfranchi, Falcone, and Marzo 2006), this paper explores how practices used to build trust and mutual support in face-to-face communities can be adapted to digital and online communities to strengthen cyber resilience. Drawing on observations from the *Critical Sherpas* pilot and beta test, we examine how an intentionally designed online cyber critical infrastructure community (C-CIC) can strengthen cyber resilience by improving cross-sector coordination, information sharing, and collective cyber defense capabilities.

Drawing on Metcalf (2004), Bohill (2010) defines an *intentional community* as a voluntary assembly of individuals from diverse backgrounds who convene to address perceived social inadequacies. These groups foster a distinct "we-consciousness" by adopting shared practices and a consciously devised culture that serves as an alternative to mainstream society. Accordingly, we define the C-CIC as an intentionally designed network of individuals from diverse professional backgrounds, who voluntarily convene online to address shared vulnerabilities and systemic challenges within cyber and critical infrastructure domains.

We first examine the theoretical importance of trust and social capital in physical and virtual communities from the literature. After introducing the key factors and considerations guiding the design of the *Critical Sherpas* C-CIC pilot, we discuss insights derived from beta testing feedback. The purpose of our research is to inform collaborative efforts between cyber professionals, critical infrastructure operators, government, and private sector leaders seeking to intentionally design C-CICs to improve cyber resilience of critical infrastructure.

2 BACKGROUND AND LITERATURE REVIEW

2.1 Cyber Resilience of Critical Infrastructure

The National Institute of Standards and Technology (NIST) defines cyber resilience as "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources. Cyber resiliency is intended to enable mission or business objectives that depend on cyber resources to be achieved in a contested cyber environment" (NIST, 2024, 2022, 2021).

We define community resilience as a community's capacity to anticipate, absorb, adapt to, and transform through disruption, whether social, economic, environmental, or political. Rather than simply bouncing back to a previous state, we see resilience as an emergent strength, a process in which communities become more equitable, inclusive, and cohesive

by navigating challenges together. This perspective is informed by established research approaches focusing on structural violence (Chance 2023; Galtung 1990; Galtung and Höivik 1971; Galtung 1969), trauma-informed practices (Erickson and Harvey 2023), and conflict transformation (Lederach 2005). This definition reinforces the importance of social capital, trauma awareness, and participatory processes that help empower historically underserved voices. In the C-CIC pilot, our objective was to improve community resilience by creating online spaces where collaboration could thrive.

Whereas cybersecurity focuses on protecting digital assets and preventing breaches, cyber resilience presumes that intrusions will occur. It emphasizes both functional continuity and system adaptation despite reduced capability (Linkov and Kott 2018). Smith (2023) argues that cyber resilience depends on system properties such as critical thresholds, recovery times, and adaptive learning. Björck et al. (2015) also focuses on operational continuity and highlights the importance of strategic planning to achieve intended outcomes. This is particularly important (and therefore challenging) because cyber resilience is a dynamic, system-wide capability that spans technical, human, and institutional domains.

Municipalities and smaller organizations are especially vulnerable to cyber threats due to limited budgets, underinvestment, inconsistent governance, outdated IT systems, and insufficient staff training. This also makes them attractive targets for ransomware. Additionally, small businesses often face risks through third-party services and supply chain compromises (Hossain et al. 2024). The consequences are real and can be severe. As the 2023 Hiscox Cyber Readiness Report shows, in 2022, 41 percent of small businesses were targets of cyberattacks, and spent an average of $16,000 in ransom. Only half recovered all their data, while the other half had to rebuild their systems (Hiscox 2023). In 2021, 61 percent of small businesses were targeted, and their employees experienced over three times as many social engineering attacks as those at larger enterprises (Rahmonbek 2025).

Mitigating these threats requires human-centered, collaborative solutions. Strategic alliances between local governments, businesses, academic institutions, and other municipalities have been shown to improve collective response by enabling the sharing of threat intelligence, best practices, and pooled resources (Hossain et al. 2024). Social connections and collective support play a critical role in helping individuals and groups withstand and recover from adversity and disruption. When people are connected to and supported by others, their ability to bounce back from challenges is significantly strengthened (Tierney 2019).

Cyber resilience is stronger when those responsible for protecting critical infrastructure know each other personally, understand local vulnerabilities and interdependencies, and can coordinate rapidly during crises. In face-to-face communities, such relationships traditionally developed organically through professional associations, shared workplaces, or community organizations. However, the realities of modern cybersecurity work make regular in-person coordination between disparate professions, areas of expertise, and jurisdictional purviews

challenging. This creates a compelling case for connecting local cyber professionals through online platforms. While hybrid approaches that also incorporate face-to-face relationship-building might be optimal, practical constraints often necessitate virtual connectivity.

To enable effective collective action, online cybersecurity communities must be intentionally designed to foster trust and social capital.

2.2 Trust

Trust is a cornerstone of cyber resilience for interdependent critical infrastructure sectors (e.g., energy, water, transportation) where a disruption in one sector can cause cascading failures. Defending essential services requires effective collaboration among diverse stakeholders from government agencies, private industry, and emergency response teams. In such communities, trust is deeply embedded in social relationships, peer interactions, and shared norms (Wu, Edwards, and Das 2022).

A collaborative online platform for stakeholders can enhance preparedness and response, but its effectiveness ultimately hinges on cultivating trust among users. This is essential because key security behaviors, like information sharing and crisis coordination, are fundamentally social processes (Wu, Edwards, and Das 2022). As is the case with consumer products and brands (Harrigan et al. 2021), community members must trust the beliefs and intentions of both their peers and the platform itself. A lack of trust in digital spaces may lead to siloed information sharing, misinformation, and hesitancy in adopting collaborative security measures (Collett 2021). Without trusted networks, stakeholders may withhold threat intelligence out of fear of reputational damage or competitive disadvantage. This can lead to fragmented crisis response, exacerbate vulnerabilities, prolong recovery, and erode public confidence in leaders' ability to protect essential services (Backman 2021).

2.3 Social Capital

Bourdieu (1986) defined social capital as the resources accessible via one's network of relationships. In their comprehensive review, Bhandari and Yasunobu (2009) define it as a collective asset centered on social relationships, characterized by shared norms, values, beliefs, trust, networks, and institutions that facilitate cooperation and collective action for mutual benefit. Social capital is characterized by the quality of community members' civic engagement and mutual obligation, which both enable sustained cross-sector collaboration, especially under conditions of uncertainty or crisis (Bhandari and Yasunobu 2009). Bourdieu's observation that social capital requires "an unceasing effort of sociability [and] a continuous series of exchanges in which recognition is endlessly affirmed and reaffirmed" highlights why cybersecurity communities cannot simply rely on static institutional relationships, and must actively cultivate trust and social capital (Bourdieu 1986, 250).

Substantial social capital fosters effective information exchange, encourages engagement, and reduces risk perception, making it easier for community members to engage with each other and coordinate their responses internally and externally during cybersecurity incidents and infrastructure crises (Alvi et al. 2024; Karačić, Marić, and Kovač 2021). In both offline and online communities, social capital may be *bonding* (fostering in-group solidarity) or *bridging* (connecting diverse groups across sectors).

Bonding social capital, as defined by Omukoba and King'ara (2024), refers to the resources and trust fostered within homogenous groups, such as professionals in the same organization or field (Alves et al. 2022). When people within an organization trust each other, they tend to share important information more openly, coordinate their actions more smoothly, and follow common rules, which in turn makes the whole system more secure. These trust-based relationships improve cybersecurity performance by supporting faster decision-making, better communication, and more consistent practices (Pigola et al. 2025). While bonding social capital is beneficial, too much of it risks reinforcing information silos and may become a barrier to external connections.

Bridging social capital, on the other hand, focuses on external cooperation among government agencies, private industry, and critical infrastructure operators (Putnam 2020; Omukoba and King'ara 2024; Karačić, Marić, and Kovač 2021). Strong external relationships can break down silos, reduce delays in threat response, and foster a more resilient and adaptive cybersecurity ecosystem.

An effective balance of bonding and bridging capital fosters networks of shared responsibility. Ultimately, social capital functions as both a trust enabler and a risk mitigator in online communities. The C-CIC was conceived as an intentional effort to cultivate bonding and bridging social capital as the foundational infrastructure for effective cyber defense.

2.4 Digital Community Design Strategies

Deliberate strategies grounded in trust and social capital are essential to ensure online platforms for coordination among government, private industry, and security professionals remain effective, cohesive, and resistant to fragmentation, misinformation, and disengagement (Collett 2021; Backman 2021).

The declining access to social capital that Putnam (2020) identifies in the digital age is a significant threat to community health, making deliberate investment in building it a necessity. Putnam argues that social networks are the "quintessential resource" for any group needing to solve complex problems or mobilize for collective action. However, Putnam also demonstrates that computer-mediated platforms are inherently poor at generating deep trust and bridging social capital that are prerequisites for effective collaboration. Similarly, Gordon and Lopez

(2019) found that, rather than enthusiasm for adoption, community-based organizations expressed ambivalence and considered technology both a help and a hindrance.

Therefore, the primary challenge for any online community platform lies in incorporating design features that intentionally "thicken community ties" and overcome the natural trust deficit of digital media. To achieve these outcomes, the following four elements served as a strategic design framework for the C-CIC pilot.

2.4.1 Guiding Objectives. *Critical Sherpas* was designed to address a fundamental paradox revealed by the *Jack Voltaic* exercises: cyber resilience depends on trust networks and social coordination, yet these networks rarely exist before they are urgently needed during a crisis. Rather than treating community formation as an ancillary benefit of technical coordination platforms, we positioned it as the primary objective: to improve cross-sector cyber response capability and effectiveness by creating a trusted network of professionals who could coordinate rapidly during incidents. However, we recognized that this operational goal could only be achieved through a secondary objective: deliberately fostering the social relationships, shared norms, and institutional connections that enable coordination at scale.

2.4.2 The Strategic Foundation: A Hybrid Ecosystem. While online communities provide robust platforms for support and continuous engagement independent of physical location, they can face challenges in achieving the depth of engagement and the strong emotional connections characteristic of in-person interactions. As numerous studies suggest, effective modern-day professional communities are not purely virtual or entirely in-person. They are intentionally designed as hybrid ecosystems with enhanced capacities to leverage the strengths of both modalities to create more resilient, engaged, and effective professional networks (Alves et al. 2022; Ghamrawi 2022; Shaw et al. 2022; Borowiec et al. 2021).

While virtual work can prevent some conflicts, in-person interactions are vital for building deeper trust, resolving complex issues, and bridging gaps between subgroups. Integrating periodic in-person workshops into a virtual framework can therefore make collaborations more robust and enhance community cohesion (Alves et al. 2022; Gläsener, Afflerbach, and Weibel 2014). Research into blended learning environments indicates that combining digital and in-person educational strategies enhances engagement and learning outcomes (Namyssova et al. 2019). These blended approaches ensure that community members develop strong interpersonal relationships and trust, which are critical for effective collaboration in high-stakes environments.

Online platforms are especially effective at maintaining and expanding "weak ties"; non-hierarchical connections that go beyond face-to-face interactions, allowing individuals to assess the needs, motives, and actions of their counterparts from different organizational backgrounds and cultures, thereby bridging social capital (Granovetter 1973; Markley and

Franke 2020). Since these online interactions often lead to face-to-face meetings, online and offline community engagement become mutually reinforcing (Bruckman 2022). Millington (2021) emphasizes the importance of keeping conversations active and creating ongoing content to sustain member interest. Hosting and facilitating both online and offline events are powerful ways to keep the community vibrant.

2.4.3 Pillars of Community Trust: Governance, Culture, and Operations. Trust in an online community is rooted in transparent governance; users must understand how decisions are made and feel confident that rules are applied fairly. Clearly defined platform policies, security measures, and participation guidelines affect how users assess the platform's credibility (Collett 2021; Tian et al. 2022). Regular, open communication from platform administrators reinforces reliability (Backman 2021).

Establishing clear ethical guidelines for engagement discourages harmful behavior, misinformation, and security breaches. Active moderation and conflict resolution mechanisms prevent distrust from spreading by addressing disputes early, fairly, and transparently (Kwasek and Kocot 2023). Public reporting on cybersecurity practices builds trust by demonstrating accountability and commitment to best practices (Alvi et al. 2024; Collett 2021). Building a culture of collective responsibility in which users report suspicious activity, follow security best practices, and mentor others creates a resilient, self-sustaining trust ecosystem (Kwasek and Kocot 2023).

Users are more likely to engage when they feel valued and respected (Kwasek and Kocot 2023). Community trust thrives in an environment where diverse voices are included, contributions are recognized, and conflicts are resolved fairly (Collett 2021). Shin et al. (2024) found that a lack of feedback loops and participants' doubts that their voice made any difference in policy decisions impacted sustained engagement with civic platforms. Rewarding positive contributions and engagement by establishing recognition systems, acknowledging key insights, and promoting trusted members increases user commitment and strengthens those weak ties that build necessary social capital (Harrigan et al. 2021; Tian et al. 2022).

In addition to rewards and recognition, well-aligned incentives are crucial. Non-financial incentives can include professional development and networking opportunities. Professional development credits can be earned through training, short courses, lectures, or other live events offered by affiliated organizations. Networking opportunities help build bridging social capital by strengthening relationships between agencies and organizations. Engagement beyond crises, such as networking events, informal discussions, and shared learning initiatives, keeps trust relationships active and sustained over time (Karačić, Marić, and Kovač 2021).

Operationally, trust is best tested and strengthened before a crisis occurs. Pre-established (and practiced) crisis communication protocols ensure that stakeholders know who to trust

and where to get accurate information during cyber incidents (Backman 2021). Fischer-Preßler, Bonaretti, and Bunker (2024) found that sustained engagement was a challenge due to the need for training and different decision hierarchies across organizations. By engaging members in simulated cybersecurity incidents and collaborative problem-solving activities like *Jack Voltaic*, communities strengthen resilience and build trust networks that can be leveraged in real emergencies (Backman 2021). Collaborative training enhances cross-sector trust and improves communication and coordination between government agencies, private entities, and infrastructure operators (Collett 2021). Scenario-based trust-building activities, such as joint threat assessments or shared red-team exercises, help stakeholders build confidence in each other's expertise and decision-making capacity (Backman 2021).

Building trust in an online C-CIC requires deliberate effort, strong governance, secure identity verification, ethical leadership, and active participation. Transparency, clear policies, and verified reputation systems create an environment where stakeholders feel confident in engaging and sharing information. Additionally, ongoing security training, pre-crisis relationship-building, and collaborative cybersecurity exercises hone trust and resilience under crisis conditions. By fostering a culture of responsibility, reliability, and shared security, online C-CICs can enhance cyber resilience, cross-sector collaboration, and coordinated cybersecurity efforts.

2.4.4 Core Platform Requirements: Functional and Security Features. Vetting new users to ensure congruence of values and fit for the community is essential for trust-building, especially in communities dealing with sensitive cybersecurity concerns. User authentication, peer validation, and platform reputation scores can help mitigate misinformation, prevent impersonation, and counter bad-faith actors (Alvi et al. 2024; Karačić, Marić, and Kovač 2021). Multi-factor authentication (MFA), social authentication, and identity verification prevent unauthorized access to sensitive discussions (Wu, Edwards, and Das 2022). Reputation-based trust models, where users build credibility through peer ratings, expert endorsements, and their history of contributions, help establish and support trusted community leaders (Wu, Edwards, and Das 2022; Tian et al. 2022).

Certification systems (Karačić, Marić, and Kovač 2021) and role-based access to information channels (where verified cybersecurity experts can be distinguished from general participants) ensure that users can assess the reliability of shared information (Wu, Edwards, and Das 2022). Trust grows when members perceive the platform as a reliable source of actionable insights and secure intelligence sharing. Implementing best practices to prevent leaks, misinformation, or exploitation by malicious actors is critical for building and maintaining high levels of trust (Collett 2021). Encouraging controlled information sharing, for example, through tiered access levels, encrypted discussions, and secure document exchange protocols, protects sensitive data while maintaining transparency (Wu, Edwards, and Das 2022). Cybersecurity training

and peer-led knowledge sharing help bridge the gap between technical experts and non-technical stakeholders, increasing confidence in shared information (Kwasek and Kocot 2023). Ultimately, these technical features act as the digital scaffolding that supports the social architecture of the C-CIC, converting abstract trust into actionable security coordination.

In summary, the literature provides valuable insights into the benefits and challenges of building trust and social capital in online communities, particularly for high-stakes professional domains like cybersecurity. Practical questions, however, remain about how these principles translate into actual community-building efforts. Guided by input and feedback from C-CIC stakeholders, we set out to test these concepts in practice by designing, implementing, and beta testing a pilot community as described in the following section.

3 METHODOLOGY AND PILOT IMPLEMENTATION

The primary focus of the *Critical Sherpas* pilot study was to explore how an intentionally designed community could improve the cyber resilience of critical infrastructure. The goal of the pilot was to create a resilient, cross-sector, trust-based online community. It was designed to strengthen professional networks and processes, and to integrate key local actors into a structured virtual community with defined engagement strategies. Through a connection with our partner SherpaWerx, we enlisted the support of the Atlanta chapter of the Armed Forces Communications & Electronics Association (AFCEA) [1] to raise awareness and recruit participants. We intend for the pilot to serve as a test case for a scalable framework that could be replicated by other municipalities, counties, and states, with the long-term vision of feeding into a resilient, national critical infrastructure protection network.

The research team engaged stakeholders and reviewed technology platforms to assess critical security needs, existing capacities, interdependencies, the potential impact of disruptions, and existing protection measures. We employed a multi-phase iterative design approach to develop and test an intentional online community platform for our pilot in metro Atlanta.

3.1 Stakeholder Needs Assessment

Interviews. We conducted eight semi-structured interviews with members of the Atlanta critical infrastructure community and participants in a Jack Voltaic round table facilitated by the Army Cyber Institute. Interviewees represented government agencies, private sector organizations, academic institutions, and nonprofit entities. Half were executive-level members of the cybersecurity community, and the remaining were senior academics in cybersecurity, cyberlaw, business law, and ethics. The purpose of the interviews was to identify common coordination challenges to inform platform requirements. The interviews were conducted online and lasted no more than one hour. The interview guide included five baseline questions

1. https://www.afcea.org/

(outlined below). Following a semi-structured approach, interviewers also asked additional follow-up questions when needed.

- What websites do you find useful for your job and your organization?
- Where do you go to get your information regarding the industry?
- What do you need that you do not find in other platforms?
- Where do you find and share best practices?
- Who else do you think should be invited into the community?

We reviewed the websites listed and the resources mentioned by our interviewees to see similarities and differences with the initial architecture of the portal. Question 3 was essential in determining gaps to be filled. Question 4 when compared across disciplines allowed us to see knowledge and sharing gaps. Question 5 aimed to broaden our understanding of who is important to have in a cyber critical infrastructure community.

The purpose of this initial needs assessment was to identify areas of overlap and siloing and to adapt the platform to meet the community's needs. We used respondents' feedback to adapt and restructure the portal's architecture and to front-load information that might be useful to those who are not aware of the available resources.

Stakeholder interviews consistently emphasized the need for stronger mechanisms to connect and engage stakeholders, noting that trust and personal relationships are foundational for rapid, coordinated response. Community engagement platforms, when paired with standardized response protocols, can ensure that key players are familiar with one another and can act decisively during incidents. A centralized information repository emerged as a priority to overcome information silos, with participants seeking a single location that aggregates threat intelligence, vendor recommendations, wargame resources, and vetted tools. Respondents viewed public education initiatives as critical for building a culture of shared responsibility, improving awareness from leadership to junior staff.

Enhanced resource connectivity and secure geographic mapping of critical infrastructure were also top needs. Interviewees highlighted that cascading impacts like power outages halting water and gas flow are poorly understood across sectors, underscoring the value of tools that visualize interdependencies and supply chains. They also recommended shared calendars and discussion forums to further support collaboration, allowing stakeholders to identify gaps, share best practices, and develop collective resilience strategies. Together, these needs point to a portal that functions not just as an information hub but as an active, trusted community for cross-sector coordination.

Online Survey. We distributed an online survey in April 2024 to Metro Atlanta critical infrastructure protection professionals about the effectiveness of existing coordination efforts and organizational policies, and respondents' willingness to participate in a C-CIC. Survey

distribution leveraged professional networks, AFCEA chapters, and stakeholder referrals to reach diverse sectoral representation. The survey instrument comprised twelve questions combining open-ended and closed-ended formats. It also collected organizational demographics including sector affiliation and information on existing critical infrastructure policies or plans. Key questions included are presented in Table 1.

Table 1. Key survey questions and response formats

Survey question	**Format**
What are the biggest threats and needs for critical infrastructure protection in metro Atlanta? (up to three responses)	Open-ended
How would you assess the effectiveness of current practices to coordinate efforts among individuals and organizations involved with the protection and security of civilian critical infrastructure in metro Atlanta?	Five-point Likert scale from *very effective* to *very ineffective*
How could coordination be improved?	Open-ended
Would you or your organization be interested in participating in a Cyber Critical Infrastructure Community for metro Atlanta?	Yes/No

In total, 25 cyber professionals from a range of sectors responded to the survey, including private industry (n=15), academia (n=3), nonprofits (n=2), and government agencies or military (n=3). Asked about existing coordination efforts, only nine respondents stated their organization maintained comprehensive critical infrastructure policies, plans, and designated points of contact. Coordination effectiveness received mixed assessments, with a slight majority (n=13) rating efforts as "somewhat or very effective" while the remainder rated coordination effectiveness as "somewhat or very ineffective" (n=6), or "neither effective nor ineffective" (n=6). These findings, along with interview insights, revealed both coordination gaps and receptivity to new coordination approaches, providing empirical grounding for the design of the C-CIC portal.

These findings from interviews and surveys informed the C-CIC pilot design. Specific needs articulated by respondents indicated a strong desire for centralized threat intelligence, secure spaces for sensitive information sharing, common event calendars, and tools for visualizing critical infrastructure interdependencies.

3.2 Technology Platform Selection

Platform Benchmarking. We conducted an exploratory benchmarking analysis of nine commonly used online engagement technologies to inform our platform selection. These included conflict resolution platforms, professional networking platforms, and virtual collaboration platforms. We analyzed platform services, customization capabilities, and engagement mechanisms to understand their functionality and identify gaps relevant to identified C-CIC needs. The exploratory benchmark revealed several patterns across platform types.

The inclusion of conflict-resolution and peacebuilding platforms (Digital Peacebuilding Community of Practice, ConnexUs, Platform 4 Dialogue) reflected our theoretical premise that cybersecurity is inherently about conflict prevention and responsiveness, and that established peacebuilding concepts and practices for building trust could inform approaches to limiting or eliminating conflict during cyber crises. However, these platforms often contained outdated or inactive content, with many sites showing no recent updates or few resources. This pattern of content stagnation highlighted the challenge of sustaining engagement in online communities of practice without active management or regularly refreshed content.

Professional platforms (LinkedIn groups, IEEE Cybersecurity Community, ISACA Engage) host numerous groups dedicated to cybersecurity professionals but they generally can not be customized and restrict access to platform members only. While LinkedIn is home to highest concentration of cybersecurity-focused groups among the platforms reviewed, the members-only access model and lack of customization options limited its utility for building locally-focused communities with controlled access tiers. IEEE Cybersecurity Community and ISACA Engage similarly prioritize global professional networking over local coordination needs.

Collaboration platforms (Slack and Discord) offered different functionality, existing primarily to facilitate discussions rather than providing additional content such as information repositories or structured resources. While these platforms excel at enabling real-time communication, they lack the integrated resource-sharing, event coordination, and professional development tools identified as priorities in our stakeholder interviews. Across all platform categories, we observed that most existing solutions prioritize global networking over local coordination and lack geographic customization capabilities. It proved difficult to assess whether these communities were effective, or the extent to which they were utilized, because visibility is restricted to members only. Critically, none of the platforms in the benchmark combined local geographic focus, customizable access controls, integrated resource repositories, event coordination, and professional development tools in a single solution.

The benchmarking analysis, informed by specific needs articulated in our stakeholder interviews and surveys, justified the selection and development of a purpose-built platform.

Platform Selection. The C-CIC portal was implemented using *Mighty Networks*, a cloud-based community platform that provides integrated discussion forums, event hosting, resource sharing, and member management capabilities (Mighty Networks 2024a). *Mighty Networks* was selected based on established evaluation criteria for community platforms, including native feature integration, mobile accessibility, customization options, and scalability potential (Mighty Networks 2024b). Out of the box, the platform offers key functionalities identified as useful in our stakeholder interviews: private organizational subgroups with controlled access, integrated event calendars, resource libraries, and member verification systems.

3.3 C-CIC Design and System Architecture

The portal design integrated theoretical principles from community building literature with empirical needs identified through stakeholder interviews and survey responses. The C-CIC portal serves a hybrid digital community featuring knowledge exchange tools, private organizational subgroups, event coordination capabilities, and resource repositories.

The cloud-based technical infrastructure of *Mighty Networks* enables both web browser access and native mobile applications for iOS and Android devices, enabling cross-platform engagement essential for busy professionals. The platform's "spaces" architecture allows for flexible community organization, with different access levels for general community discussions, sector-specific working groups, and restricted information sharing areas. Although the platform offers built-in analytics capabilities for tracking member engagement, we used it primarily for interacting with users and monitoring community growth.

The platform housing the portal had architectural limitations, including security gaps which forced us to create a two-step referral and admission process supported by user monitoring and member vigilance. Due to time constraints and the limited number of adopters we were not able to fully implement community-building best practices with the C-CIC portal.

3.4 Pilot Beta Testing

A dozen cybersecurity professionals, selected from our initial needs assessment and referrals, accepted invitations to participate in structured virtual beta testing sessions. Four sessions captured user experience data, design recommendations, and functionality assessments, informing subsequent platform modifications to enhance navigation, access controls, and user guidance systems. Beta test users provided real-time feedback via screen-sharing sessions with the testing team. Users were given rudimentary navigation instructions and an initial overview of the portal. They were then asked to navigate it on their own, with testing team members available to assist and answer questions. Feedback was analyzed to assess the portal's usability and potential utility.

In general, the feedback reflected a tension between ease of use and strong security. Test users appreciated having strong security and controlled access, but they also needed the platform to be easy to navigate and quick to use during fast-moving situations. Some test users expressed strong enthusiasm for the platform's cross-sector information-sharing capabilities and its controlled-access features for sensitive discussions. Participants from a government agency expressed a desire for a portal that would give counties a way to access information and for the agency to disseminate information to them.

Although pilot adoption fell short of established benchmarks for sustained engagement, feedback revealed two categories of potential enhancements: 1) the need for enhanced user

guidance on information sharing protocols and privacy controls, and 2) improved user experience for section accessibility, joining processes, and feature functionality.

4 DISCUSSION

The experience of the C-CIC pilot highlights a fundamental challenge in cyber resilience community-building: initial enthusiasm among stakeholders does not automatically translate into sustained engagement. This pattern suggests that simply transplanting traditional community-building strategies into cybersecurity contexts may be insufficient. Instead, the findings from our pilot point to the need for tailored approaches that address the unique barriers to ongoing participation in cyber-focused communities such as the sensitivity of information, the demands on professionals' time, and the complexities of trust and verification in digital environments. Interpreting these findings, it becomes clear that fostering lasting engagement in cyber resilience initiatives requires rethinking conventional models and developing new frameworks that are responsive to the specific needs and constraints of cybersecurity practitioners.

Our survey results revealed that nearly half of the respondents rated current efforts as only "somewhat effective," while only one respondent considered them "very effective." These results suggest room for coordination improvement, though the limited sample size and engagement levels prevent broad generalization. Have stakeholders come to accept suboptimal coordination as an acceptable baseline performance? Addressing this possibility in future research could help clarify how organizational expectations influence collaborative performance in cybersecurity contexts.

4.1 Community Engagement: The Critical Mass Problem

The most significant challenge of the *Critical Sherpas* pilot was achieving sustainable engagement. With only 25 early adopters from the target metropolitan area population, the portal fell short of Millington's (2021) critical mass benchmarks: 100 contributing members per month, 300 monthly posts, and 10 new registrations per day. Consistent with findings in the broader literature on leadership and sustainability of online communities (Kraut et al. 2012; Johnson, Safadi, and Faraj 2015), the pilot's reliance on a single community champion, AFCEA Atlanta (via a connection with our partner SherpaWerx), rather than a larger number of stakeholders, proved limiting.

Engert et al. (2023) show that sustained engagement on digital platforms depends on strengthening five antecedents: clear platform rules, a compelling value proposition, active platform agents, alignment with user needs, and visible contributions from complementors (members offering different perspectives that enhance the value of each other's participation). These enable the core behaviors of sharing information, connecting with others, and coordinating efforts. While these factors and behavioral objectives were all considered in

the design of the C-CIC pilot, engagement metrics are needed to understand how specific design choices affect changes in these behaviors and overall community engagement. Future research should test different engagement approaches and track participation longitudinally to determine which methods are most effective and sustainable.

4.2 Designing for Trust: The Usability-Security Tension

Stakeholders and participants uniformly highlighted the importance of clear information-sharing protocols and strong privacy controls, underscoring the challenge of calibrating trust in environments where transparency itself can heighten vulnerability. Prior research suggests that in professional and emergency response networks, trust calibration depends on both the perceived credibility of information sources and the robustness of governance mechanisms that protect against misuse. Backman (2021) emphasizes that pre-established trust networks enable rapid, secure information exchange during crises, while Alvi et al. (2024) and Wu, Edwards, and Das (2022) note that effective trust mechanisms must balance institutional assurance with interpersonal confidence to reduce risk and support collaboration. This means that C-CIC platform design must mirror these trust architectures—embedding clear validation systems, transparent but bounded communication channels, and flexible privacy controls that sustain confidence without compromising security.

Balancing the tension between ease of use and strong security is necessary in cybersecurity and critical infrastructure protection, where mistakes can have serious consequences (Di Nocera, Tempestini, and Orsini 2023). This highlights a central challenge: the system must protect sensitive information while still allowing people to work together smoothly and efficiently. Our platform comparison suggests that large, general-purpose systems often focus on reaching many users rather than supporting careful, high-quality coordination. In contrast, our pilot indicates that a more specialized, security-focused platform may be necessary for the kind of precise, trust-based collaboration that C-CICs depend on. The enthusiasm for features that enable private subgroups with controlled access suggests that stakeholders recognize the need for bridging social capital and building nuanced trust within the broader community.

4.3 Incentives for Sustained Engagement

The lack of formal incentives, including rewards, recognition, or professional development credits likely contributed to the limited engagement in the C-CIC pilot. Instead, we relied on intrinsic motivation, which proved insufficient against the competing time demands of cybersecurity professionals. Our findings parallel tensions documented in other security-sensitive professional networks. Like intelligence communities that must balance collective learning against "need to know" secrecy protocols (Rusho et al. 2025), and healthcare information exchanges navigating privacy constraints, cyber infrastructure communities face inherent contradictions between the openness required for effective knowledge sharing and

the competitive or confidentiality pressures that inhibit it. Research on "coopetition" networks demonstrates that formal coordination mechanisms and technology-enabled trust-building become essential when standard community assumptions of voluntary, open participation cannot apply (Tsai 2002; Randolph, Hu, and Silvernail 2020).

4.4 Implications for Theory and Practice

While *Critical Sherpas* faced expected challenges common to new online communities, the pilot surfaced valuable insights that align closely with findings of Kraut et al. (2012) on the importance of clearly defined objectives and competitive differentiation. The project was intentionally designed to foster organic growth, and while this approach yielded enthusiastic engagement from early adopters and strong initial partnerships, it also revealed the need for more structured facilitation, diversified leadership, and more precise articulation of the platform's unique value. These lessons reflect the natural evolution of a complex, multi-sector initiative and offer a strong foundation for refining future efforts. By aligning more closely with proven strategies such as establishing a clear purpose, building referral systems, and defining a competitive niche, future iterations of the C-CIC portal can be positioned for broader adoption and sustained impact.

One consideration pertaining to cyber and critical infrastructure communities is whether the inclusion and handling of highly sensitive information is appropriately accounted for, both theoretically and practically. Further research is necessary to determine if design modifications are needed for more effective connection, coordination, and collaboration between professionals and organizations who need to use and share sensitive information to fulfill their respective responsibilities. Existing community theory, particularly as applied to information sharing and analysis centers (ISACs) and computer emergency response teams (CERTs), focuses extensively on solving the information-sharing dilemma: the collective action problem of exchanging sensitive threat intelligence (Gillard et al. 2023; Stein 2023). However, this framing may be misaligned with the primary value proposition of a geographically bounded C-CIC.

The metro Atlanta-focused pilot suggests that the primary value of C-CICs lies in establishing relational infrastructure that exists independent of transactional data exchange. Members do not necessarily need to share proprietary breach data to benefit from understanding regional roles, establishing face-to-face familiarity with counterparts, and proactively building bonding and bridging social capital in the community. These relationships enable rapid, trust-based coordination when digital channels fail or time pressures prohibit formal vetting of personnel and information. This distinction aligns with emergency management literature on "swift trust" (Wong 2013), which demonstrates that crisis coordination depends less on information transparency than on pre-defined roles and prior relationship-building. Unlike virtual ISACs where value is measured by intelligence-sharing volume, the success of geographic C-CICs

is whether a utility CISO knows precisely whom to call when a regional attack occurs, and trusts that person will answer.

Standard community theory's emphasis on openness and reciprocity thus requires modification: in security-sensitive contexts, affective social capital (familiarity, affect, emotional bonds) may be cultivated without solving the cognitive social capital dilemma (informational trust, data reciprocity). The argument underlying the C-CIC model is that these can be decoupled.

Additional findings from the C-CIC pilot suggest that applying community resilience frameworks to the cyber domain requires significant adaptation. Unlike face-to-face communities, where social capital is reinforced through physical proximity and chance encounters, cyber communities operate in an environment of invisible relationships. In this context, resilience does not emerge organically; it must be engineered. Our research indicates that digital trust differs fundamentally from physical trust; it is fragile, prone to siloing, and heavily dependent upon verification. Because online bonding can easily become insular, bridging capital (the connection between diverse sectors) must be deliberately fostered through structured interventions like cross-sector forums, shared calendars, and trust-building exercises.

These theoretical distinctions have immediate practical implications. While community resilience principles offer a helpful starting point, our pilot demonstrates that grassroots volunteerism alone is insufficient for sustaining a C-CIC. The unique constraints of the cybersecurity profession, including the high sensitivity of information, reputational risk, and extreme time pressure, mean that these communities cannot function on intrinsic motivation alone. We argue that cyber community building must transition from a volunteer-driven model to an institutional infrastructure model. Sustainable C-CICs require enterprise-grade technical infrastructure, robust security protocols, and, crucially, dedicated professional facilitation. Just as physical infrastructure requires maintenance crews, digital social infrastructure requires community managers to verify identities, curate threat intelligence, and maintain the 'we-consciousness' that prevents engagement drop-off.

These needs raise important questions regarding scalability. If achieving critical mass is challenging within a single metropolitan area with dense professional networks, scaling such initiatives to regional, national, or international levels presents exponentially more barriers. Future research should investigate whether a federated model connecting local, high-trust C-CICs is more effective than a monolithic national platform. Ultimately, the beta test validated that while trust and social capital drive cyber resilience, intentionally designed communities must be carefully engineered and require institutional investment to function. Cyber community building should not be viewed as a low-cost networking experiment, but rather as a well-funded, well-resourced imperative for national security and resilient emergency preparedness infrastructure.

CONCLUSION

The C-CIC pilot advances our understanding of cyber resilience by demonstrating that adapting community-building principles from face-to-face to online contexts can improve cyber critical infrastructure coordination. However, successful implementation requires significant modification to address the unique constraints of cybersecurity environments. Our Atlanta-based *Critical Sherpas* pilot provides empirical evidence that stakeholder demand for improved cyber coordination exists and that effective coordination through an online community platform design is achievable. However, sustainable engagement demands professional-grade facilitation and institutional investment rather than volunteer-driven approaches. This finding has important implications for how we conceptualize cyber resilience as both a theoretical framework and a practical imperative.

For practitioners and policymakers, this research suggests that effective cyber critical infrastructure communities should be treated as an essential coordination infrastructure that requires dedicated funding, professional management, and enterprise-level technical coordination. Organizations and agencies investing in cyber resilience initiatives should budget for sustained community facilitation, recognizing that busy cybersecurity professionals need well-designed and easily accessible structured engagement opportunities that clearly add professional value rather than additional volunteer commitments. The success of such initiatives may depend on integrating community building into existing frameworks for professional development and emergency preparedness, and forming industry associations where participation can be formally recognized and resourced.

Based on these findings, future cyber community initiatives should implement specific design principles, including multi-sectoral stakeholder teams instead of single champions, structured referral pathways for sustained growth, and hybrid approaches that combine online platforms with in-person events and trust-building activities. Building on the theoretical framework distinguishing relational from cognitive social capital, geographically bounded cyber communities appear optimally positioned to cultivate the affective bonds, role familiarity, and face-to-face relationships that enable rapid crisis coordination, a function distinct from the information-sharing mandate of national-scale ISACs or CERTs. The integration of structured referral pathways as part of outreach, awareness-raising, and engagement activities can enhance participation and strengthen community ties beyond what can be achieved through purely digital approaches. Broad, inclusive partnerships with cyber stakeholders across sectors will be essential for achieving the scale and sustainability that voluntary approaches cannot provide, requiring institutional commitment rather than relying on individual enthusiasm alone.

The broader implications for a national cybersecurity strategy are significant. Since cyber threats increasingly require systematic and coordinated community responses, building

resilient cyber communities becomes a matter of national security, and infrastructure investment must go far beyond optional networking enhancement. Future research should examine optimal resource allocation models for cyber community initiatives, evaluate the effectiveness of different institutional partnership frameworks, and develop metrics for assessing community-level cyber resilience outcomes. The path forward requires treating cyber community building as seriously as we treat other forms of critical infrastructure protection. Sustained investment, professional expertise, and the recognition that community resilience is a public good become essential for effectively protecting national security.

ABOUT THE AUTHORS

Dr. Anne M. Chance directs Solution Labs for TRENDS Global. Her research focuses on historical identity, personal values, and ethno-territoriality. Dr. Chance has a Ph.D. in International Conflict Management, Peacebuilding, and Development, a Master's Degree in Cultural Preservation. She is currently developing vertically integrated program labs that teach resiliency practices to emerging professionals.

Dr. Volker Franke is Professor of Conflict Management at Kennesaw State University and Founder and Executive Director of TRENDS Global, a 501c3 nonprofit, dedicated to research and capacity strengthening in community-focused peacebuilding and conflict transformation (https://trendsglobal.org). Dr. Franke has extensive experience in research and capacity building in conflict management and adaptive peacebuilding.

Timo Zwarg is a PhD Candidate in International Conflict Management, Peacebuilding, and Development at Kennesaw State University. Mr. Zwarg holds a Master of Science in Peace and Security from the University of Hamburg. His research focuses on decolonial practices, participatory action, and community peacebuildling.

ACKNOWLEDGMENTS

The *Critical Sherpas* C-CIC pilot study team included researchers from Kennesaw State University, SherpaWerx, and TRENDS Global. The pilot was financially supported by the Army Cyber Institute at West Point.

REFERENCES

ACI (Army Cyber Institute). 2021a. *Jack Voltaic 3.0: Cyber Research Report - Prepare | Prevent | Respond.* Technical report. https://cyber.army.mil/Portals/3/Documents/JackVoltaic/3.0/JackVoltaic_Executive_Summary_3.0.pdf.

Alves, M., I. Dimas, P. Lourenço, T. Rebelo, V. Peñarroja, and N. Gamero. 2022. "Can Virtuality Be Protective of Team Trust? Conflict and Effectiveness in Hybrid Teams." *Behaviour & Information Technology* 42 (7): 851–68. https://doi.org/10.1080/0144929X.2022.2046163.

Alvi, Tariq Hameed, Samia Tariq, Amad Rashid, and Maryyam Qasim Khan. 2024. "Trust Mechanisms in the Sharing Economy." *Pakistan Business Review* 26 (3): 228–51. https://doi.org/10.22555/pbr.v26i3.1284.

Army Cyber Institute. 2018. *Jack Voltaic 2.0: Threats to Critical Infrastructure - Executive Summary.* Technical report. Army Cyber Institute, United States Military Academy. https://cyber.army.mil/Portals/3/Documents/JackVoltaic/JV2_Exsum_FINAL.pdf.

Army Cyber Institute. 2021b. *Jack Voltaic 3.0: Executive Summary - Increasingly Connected, Ready to Respond.* Technical report. Army Cyber Institute, United States Military Academy. https://cyber.army.mil/Portals/3/Documents/JackVoltaic/3.0/JackVoltaic_Executive_Summary_3.0.pdf.

Army Cyber Institute. 2022. *Planning Playbook: Jack Voltaic®. Version 1.1.* Technical report.

Backman, Sarah. 2021. "Conceptualizing Cyber Crises." *Journal of Contingencies and Crisis Management* 29 (4): 429–38. https://doi.org/10.1111/1468-5973.12347.

Bhandari, Humnath, and Kumi Yasunobu. 2009. "What Is Social Capital? A Comprehensive Review of the Concept." *Asian Journal of Social Science* 37 (3): 480–510. https://doi.org/10.1163/156853109X436847.

Björck, Fredrik, Henric Johnson, Johan Johnson, and Martin Löf. 2015. "Cyber Resilience: Fundamentals for a Definition." In *Availability, Reliability, and Security in Information Systems,* edited by Alvaro Rocha, Ana Maria Correia, Sandra Constanzo, and Luis Paulo Reis, vol. 315. Advances in Intelligent Systems and Computing. Springer International Publishing. https://doi.org/10.1007/978-3-319-16486-1_31.

Bohill, Ruth Rewa. 2010. "Intentional Communities: Ethics as Praxis." PhD diss., Southern Cross University. https://researchportal.scu.edu.au/esploro/outputs/doctoral/Intentional-Communities--Ethics-as-Praxis/991012821645102368.

Borowiec, Katrina, Deoksoon Kim, Lizhou Wang, Juli Kim, and S. Wortham. 2021. "Supporting Holistic Student Development Through Online Community Building." *Online Learning* 25 (4): 154–71. https://doi.org/10.24059/olj.v25i4.2882.

Bourdieu, Pierre. 1986. "The Forms of Capital." In *Handbook of Theory and Research for the Sociology of Education,* edited by John G. Richardson. Greenwood Press.

Bruckman, Amy S. 2022. *Should You Believe Wikipedia?: Online Communities and the Construction of Knowledge.* 1st. Cambridge University Press. https://doi.org/10.1017/9781108780704.

Castelfranchi, C., R. Falcone, and F. Marzo. 2006. "Being Trusted in a Social Network: Trust as Relational Capital." In *Trust Management. iTrust 2006,* edited by K. Stølen, W.H. Winsborough, F. Martinelli, and F. Massacci, vol. 3986. Lecture Notes in Computer Science. Springer, Berlin, Heidelberg. https://doi.org/10.1007/11755593_3.

Chance, Anne M. 2023. "Inscribing Violence: Quantifying the Impact of World Heritage Site Inscription on Direct and Structural Violence." PhD diss., Kennesaw State University. https://digitalcommons.kennesaw.edu/incmdoc_etd/51.

Collett, Robert. 2021. "Understanding Cybersecurity Capacity Building and Its Relationship to Norms and Confidence Building Measures." *Journal of Cyber Policy* 6 (3): 298–317. https://doi.org/10.1080/23738871.2021.1948582.

Di Nocera, Francesco, Giorgia Tempestini, and Matteo Orsini. 2023. "Usable Security: A Systematic Literature Review." *Information* 14 (12): 641. https://doi.org/10.3390/info14120641.

Engert, Martin, Julia Evers, Andreas Hein, and Helmut Krcmar. 2023. "Sustaining Complementor Engagement in Digital Platform Ecosystems: Antecedents, Behaviours and Engagement Trajectories." *Information Systems Journal* 33 (5): 1151–1185. https://doi.org/10.1111/isj.12438.

Erickson, M., and T. Harvey. 2023. "A Framework for a Structured Approach for Formulating a Trauma-Informed Environment." *Journal of Education* 203 (3): 666–677. https://doi.org/10.1177/00220574211046811.

Fischer-Preßler, Diana, Dario Bonaretti, and Deborah Bunker. 2024. "Digital Transformation in Disaster Management: A Literature Review." *The Journal of Strategic Information Systems* 33 (4): 101865. https://doi.org/10.1016/j.jsis.2024.101865.

Galtung, J. 1969. "Violence, Peace, and Peace Research." *Journal of Peace Research* 6 (3): 167–191. http://www.jstor.org/stable/422690.

Galtung, J. 1990. "Cultural Violence." *Journal of Peace Research* 27 (3): 291–305.

Galtung, J., and T. Höivik. 1971. "Structural and Direct Violence: A Note on Operationalization." *Journal of Peace Research* 8 (1): 73–76. https://doi.org/10.1177/002234337100800108.

Ghamrawi, Norma. 2022. "Teachers' Virtual Communities of Practice: A Strong Response in Times of Crisis or Just Another Fad?" *Education and Information Technologies* 27 (5): 5889–915. https://doi.org/10.1007/s10639-021-10857-w.

Gillard, S., D. Percia David, A. Mermoud, and T. Maillart. 2023. "Efficient Collective Action for Tackling Time-Critical Cybersecurity Threats." *Journal of Cybersecurity* 9 (1): tyad021. https://doi.org/10.1093/cybsec/tyad021.

Gläsener, Katharina, Thomas Afflerbach, and Antoinette Weibel. 2014. "Trust and Distrust in Hybrid Virtual Teams: Perceptions of Trustworthiness across Subgroup Boundaries." In *8TH FINT/EIASM Conference on Trust within and between Organisations.* https://www.alexandria.unisg.ch/handle/20.500.14171/86160.

Gordon, Eric, and Rogelio Alejandro Lopez. 2019. "The Practice of Civic Tech: Tensions in the Adoption and Use of New Technologies in Community Based Organizations." *Media and Communication* 7 (3): 57–68. https://doi.org/10.17645/mac.v7i3.2180.

Government Accountability Office. 2021. *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response,* April 22, 2021. https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic.

Granovetter, Mark S. 1973. "The Strength of Weak Ties." *American Journal of Sociology* 78 (6): 1360–1380. https://doi.org/10.1086/225469.

Harrigan, Maggie, Kim Feddema, Shasha Wang, Paul Harrigan, and Emmanuelle Diot. 2021. "How Trust Leads to Online Purchase Intention Founded in Perceived Usefulness and Peer Communication." *Journal of Consumer Behaviour* 20 (5): 1297–312. https://doi.org/10.1002/cb.1936.

Hiscox. 2023. *Hiscox Cyber Readiness Report 2023.* Technical report. https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2023.pdf.

Hossain, Sk Tahsin, Tan Yigitcanlar, Kien Nguyen, and Yue Xu. 2024. "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework." *Applied Sciences* 14 (13): 5501. https://doi.org/10.3390/app14135501.

Johnson, Steven L., Hani Safadi, and Samer Faraj. 2015. "The Emergence of Online Community Leadership." *Information Systems Research* 26 (1): 165–87. https://doi.org/10.1287/isre.2014.0562.

Karačić, Adriana, Ivana Marić, and Jelena Kovač. 2021. "The Importance of Service User Trust in the Collaborative Economy." In *Proceedings of the Central European Conference on Information and Intelligent Systems (Varaždin, Croatia),* 107–14.

Kraut, Robert E., Paul Resnick, Sara Kiesler, Moira Burke, and Yan Chen, eds. 2012. *Building Successful Online Communities: Evidence-Based Social Design.* MIT Press.

Kwasek, Artur, and Maria Kocot. 2023. "Organisational Agility as a Factor Determining Trust in Organisations." *Zarządzanie – Working Papers Humanitas University Management,* no. 1, 193–211. https://doi.org/10.5604/01.3001.0054.2981.

Lederach, John Paul. 2005. *The Moral Imagination: The Art and Soul of Building Peace.* New York: Oxford University Press.

Linkov, Igor, and Alexander Kott. 2018. "Fundamental Concepts of Cyber Resilience: Introduction and Overview." In *Cyber Resilience of Systems and Networks,* edited by Igor Linkov and Julia T. Richards. Springer. https://doi.org/10.1007/978-3-319-77492-3_1.

Markley, Eliza, and Volker Franke. 2020. "Snowball Networking: Making Security Cooperation more effective through Personal Communication." *Journal of Communication and Behavioural Sciences* 1 (1): 19–34.

Mighty Networks. 2024a. *Features: Community Platform for Building, Engaging & Monetizing.* https://www.mightynetworks.com/features.

Mighty Networks. 2024b. *How to Evaluate Community Platforms,* February 6, 2024. https://www.mightynetworks.com/resources/how-to-evaluate-community-platforms.

Millington, Richard. 2021. *Build Your Community: Turn Your Connections into a Powerful Online Community.* 1st. Pearson Business.

Namyssova, Gulnara, G. Tussupbekova, Janet Helmer, K. Malone, Mir Afzal, and D. Jonbekova. 2019. "Challenges and Benefits of Blended Learning in Higher Education." In *Proceedings of the 2nd International Conference on Education and Social Sciences,* 22–31.

NIST (National Institute of Standards and Technology). 2021. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* NIST Special Publication 800-160, Volume 2, Rev. 1. National Institute of Standards, Technology, and the MITRE Corporation, December. https://doi.org/10.6028/NIST.SP.800-160v2r1.

NIST (National Institute of Standards and Technology). 2022. *Assessing Enhanced Security Requirements for Controlled Unclassified Information.* NIST Special Publication 800-172A. National Institute of Standards and Technology, March. https://doi.org/10.6028/NIST.SP.800-172A.

NIST (National Institute of Standards and Technology). 2024. *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach.* NIST Special Publication 800-160, Volume 2, Rev. 2. National Institute of Standards, Technology, and the MITRE Corporation. https://doi.org/10.6028/NIST.SP.800-160v2r2.

NIST (National Institute of Standards and Technology). *Resilience.* Website. https://csrc.nist.gov/glossary/term/resilience.

Norris, Fran H., Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche, and Rose L. Pfefferbaum. 2008. "Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness." *American Journal of Community Psychology* 41 (1-2): 127–150. https://doi.org/10.1007/s10464-007-9156-6.

Omukoba, Deckillah S., and George N. King'ara. 2024. "Membership in Online Groups: A Source of Bridging and Bonding Social Capital for Kenyan Youth." *Journal of the Kenya National Commission for UNESCO* 5 (1): 1–19. https://doi.org/https://doi.org/10.62049/jkncu.v5i1.221.

Pigola, Angélica, Priscila Rezende da Costa, Leonardo Vils, and Fernando de Souza Meirelles. 2025. "Enhancing Information Security Management and Performance through Social and Relational Factors: A Structural Equation Modelling Approach." *Behaviour & Information Technology* (June): 1–23. https://doi.org/10.1080/0144929X.2025.2522206.

Putnam, Robert D. 2020. *Bowling Alone: The Collapse and Revival of American Community.* Revised and Updated. Simon & Schuster.

Rahmonbek, Komron. 2025. *35 Alarming Small Business Cybersecurity Statistics for 2025,* January. Accessed October 24, 2025. https://www.strongdm.com/blog/small-business-cyber-security-statistics.

Randolph, Ryan V., Haiyan Hu, and Kevin D. Silvernail. 2020. "Better the Devil You Know: Inter-Organizational Information Technology and Network Social Capital in Coopetition Networks." *Information & Management* 57 (6): 103344. https://doi.org/https://doi.org/10.1016/j.im.2020.103344.

Rusho, Yael, Daphne R. Raban, Daniel Simantov, and Gal Ravid. 2025. "Knowledge Sharing in Security-Sensitive Communities." *Future Internet* 17 (4): 144. https://doi.org/https://doi.org/10.3390/fi17040144.

Shaw, L., Dana Jazayeri, D. Kiegaldie, and M. Morris. 2022. "Implementation of Virtual Communities of Practice in Healthcare to Improve Capability and Capacity: A 10-Year Scoping Review." *International Journal of Environmental Research and Public Health* 19 (13): 7994. https://doi.org/10.3390/ijerph19137994.

Shin, Bokyong, Jacqueline Floch, Mikko Rask, Peter Bæck, Christopher Edgar, Aleksandra Berditchevskaia, Pierre Mesure, and Matthieu Branlat. 2024. "A Systematic Analysis of Digital Tools for Citizen Participation." *Government Information Quarterly* 41 (3): 101954. https://doi.org/10.1016/j.giq.2024.101954.

Smith, Sidney. 2023. "Towards a Scientific Definition of Cyber Resilience." In *Proceedings of the 18th International Conference on Cyber Warfare and Security,* 18:379–86. 1. https://doi.org/10.34190/iccws.18.1.960.

Stein, D. 2023. "Data Insecurity Law." *Santa Clara High Technology Law Journal* 39 (4): 445–512. https://digitalcommons.law.scu.edu/chtlj/vol39/iss4/1.

Tian, Yuan, Honglei Zhang, Yifei Jiang, and Yang Yang. 2022. "Understanding Trust and Perceived Risk in Sharing Accommodation: An Extended Elaboration Likelihood Model and Moderated by Risk Attitude." *Journal of Hospitality Marketing & Management* 31 (3): 344–68. https://doi.org/10.1080/19368623.2022.1986190.

Tierney, Kathleen. 2019. *Disasters: A Sociological Approach.* Polity Press.

Tsai, Wenpin. 2002. "Social Structure of 'Coopetition' within a Multiunit Organization: Coordination, Competition, and Intraorganizational Knowledge Sharing." *Organization Science* 13 (2): 179–90. https://www.jstor.org/stable/3085992.

Wong, L. C. 2013. *Understanding 'Swift Trust' to Improve Interagency Collaboration in New York City.* Technical report. Defense Technical Information Center.

Wood, Kimberly. 2023. *Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack.* The Georgetown Environmental Law Review, March 7, 2023. https://www.law.georgetown.edu/environmental-law-review/blog/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/.

Wu, Yuxi, W. Keith Edwards, and Sauvik Das. 2022. "SoK: Social Cybersecurity." In *2022 IEEE Symposium on Security and Privacy (SP),* 1863–1879. IEEE. https://doi.org/10.1109/SP46214.2022.9833757.

Young, Kelli. 2021. "Cyber Case Study: City of Atlanta Ransomware Incident," September 20, 2021. https://coverlink.com/case-study/city-of-atlanta-ransomware/.

Received 17 March 2025; Revised 18 November 2025; Accepted 24 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 225-240
https://doi.org/10.55682/cdr/25ae-dftk

RESEARCH ARTICLE

A Human-AI Teaming Approach to Closing the Talent Gap in Critical Infrastructure

Allyson Hauptman*

Army Cyber Institute, West Point, NY, USA

Many critical infrastructure sectors are facing significant talent gaps among their workforce. The Industrial Internet of Things revolution has introduced new technologies and requirements for workers to understand while continuing to perform the duties for which they were hired, and the introduction of these data-driven technologies has concurrently created the need for new team roles with their own sets of capabilities. One possible solution for overcoming these talent gaps is the integration of artificially intelligent teammates. Research suggests human-AI teaming could potentially offload tedious, repetitive, or dangerous human work and accomplish tasks that, while difficult for a human to complete, cater well to what computers do best. This paper proposes a simple 3-steps guiding framework for teams in critical infrastructure organizations to determine a) the gaps on their team, by distinguishing between gaps caused by insufficient personnel (capacity) and those driven by new technological demands (capability), b) which roles are well-suited for an AI teammate, based on the match between task demands and AI capabilities, and c) the human-centered design considerations, including presence, explainability, autonomy management, and ethical alignment, that are essential to its integration as an effective teammate.

Keywords: human-AI teaming, AI teammates, critical infrastructure, talent management, cyber defense workforce, human-centered design, Internet of Things, IoT

* Corresponding author: allyson.hauptman@westpoint.edu

1 INTRODUCTION

The increased use of and reliance on technology has created a more connected and efficient society than ever before; yet, these technologies simultaneously strain and challenge our critical infrastructure sectors to keep up. Many critical infrastructure sectors, such as energy (Fiume et al. 2006) and the Defense Industrial Base (DIB) (Goure 2018), face significant talent gaps among their workforce. There are multiple reasons behind this talent gap. First, some sectors are experiencing a mass wave of employee turnover and are struggling to backfill these positions (Fiume et al. 2006). Second, the Industrial Internet of Things (IIoT) revolution has introduced new technologies and requirements for workers to understand and operate while continuing to perform the duties for which they were hired (O'Heir 2017). Finally, the introduction of new data-driven technologies, such as artificial intelligence (AI), has created the need for the development of brand-new team roles with their own sets of capabilities. For industries already struggling to hire and retain enough workers to operate, these additional challenges are causes for immediate concern (Lewis 2019).

While the increased use of technology in various critical infrastructure sectors has created these problems, it may also be a solution. Human-AI teams (HATs) are a recent focus of AI research due to the possibilities they present to offload human workload and accomplish tasks that, while difficult for a human to complete, cater well to what computers do best. AI can be programmed to complete some tasks that teams do not have the manpower (O'Heir 2017) and/or capabilities to complete. An essential part of this construct's success is that the AI is not treated as just another tool that a human must manage; rather, the AI is an autonomous agent that fulfills a completely interdependent team role (O'Neill et al. 2022). In this way, the team's overall workload is reduced while its ability to tackle new challenges is enhanced.

While HATs have been explored as a performance-enhancing construct in a variety of environments, there is a significant lack of research on their role in critical infrastructure, particularly in addressing the growing workforce challenges. This paper explains the need for such a solution and presents a simple guiding framework for critical infrastructure teams to determine what gaps might be filled by an AI teammate, the scope of the AI teammate's role, and the human-centered design considerations the team needs to address in integrating the AI as an effective teammate.

The development of this framework was guided by the following research question:

How can a human-AI teaming guiding framework help critical infrastructure organizations identify, scope, and fill talent gaps essential for cyber defense?

2 BACKGROUND

2.1 The Development of a Talent Gap in Critical Infrastructure

Critical infrastructure encompasses the systems and assets vital to a nation's well-being and security, and can be divided into multiple sectors, including energy, transportation, financial services, and the Defense Industrial Base (Wagner 2021). Most critical infrastructure sectors, while overseen by various government agencies, are predominantly privately owned and operated and are highly dependent on uninterrupted operations to be successful (Durkovich 2020). This condition of uninterrupted operations creates a very high demand and workload for the professionals who operate in these sectors. Critical infrastructure sectors are interdependent, and thus when the sector is unable to provide continuous service, it affects the operations of various other sectors (Wagner 2021). For example, if a power company is unable to provide its promised output to the city it serves, that would directly affect the city's transportation services, communication services, healthcare services, and more are deeply affected.

This interdependency has increased with the emergence of cyber critical infrastructure and the vital computer services that keep all sectors running. As sectors introduce IoT devices to connect operational technologies to information technologies, both for increased efficiency and convenience, they simultaneously introduce vulnerabilities to cyber attacks (Malatji, Marnewick, and von Solms 2022). These vulnerabilities have several important implications for critical infrastructure and its workforce.

First, cybersecurity is now an essential additional layer that all critical infrastructure organizations need to build into their talent pools (Malatji, Marnewick, and von Solms 2022). While simple firewalls and scans may have been sufficient for systems that were segmented from outside threats, increased connectivity substantially increases an organization's risk of exploitation and thus requires dedicated manpower operating on dedicated equipment.

Second, organizations must be able to recognize and remediate issues caused by a cyber attack. Many critical infrastructure systems rely on operational technologies that require highly specialized expertise. Often, organizations lack these skills in-house. As a result, they frequently depend on contracted specialists, and only when they can first detect that something is wrong. A cyber attack can easily undermine this model if the organization is unable to identify that a system has been compromised or is operating abnormally (Thomas and Chothia 2021). These limitations compound an already serious challenge, leaving many organizations vulnerable to prolonged disruption and delayed response.

Research has found that a talent gap exists in critical infrastructure sectors involving both technical capabilities and sector-specific managerial skills needed to manage, secure, and implement technologies. The literature reveals a number of drivers of this gap, including an aging workforce (Ashworth 2006), diminishing vendor-locked knowledge (Sandborn and

Prabhakar 2015), and a younger generation seeking better working conditions and pay (Ayodele, Chang-Richards, and Gonzalez 2020). As it stands, many sectors are nearly stretched to the breaking point of human resources, facing urgent shortages in cybersecurity and operational technology roles.

In response, several initiatives are exploring how to rebuild the cyber talent pipeline. One promising development is the growth of cybersecurity clinics: university-based, service-learning programs that pair students with local governments, utilities, hospitals, and nonprofits to provide real cyber defense support while training the next generation of practitioners (Asare et al. 2025). These clinics provide students with hands-on experience working with real systems and threats, while offering critical infrastructure organizations a much-needed cyber capacity at a low cost. Recent national investments are expanding these clinics nationwide to address the chronic shortage of entry-level talent. Beyond clinics, sectors have experimented with a range of alternative training-focused strategies. A recent study sought to understand how tailored training could help overcome this gap and found that various sectors have experimented with simulation-based learning and virtual training environments to accelerate workforce preparation (Olonilua and Aliu 2025). In parallel, gamified training approaches have been developed to both attract new talent and enhance retention among the critical infrastructure workforce (Ashley et al. 2022). These efforts represent meaningful progress, yet they remain focused on mitigating the talent gap through human training alone. Given the scale and persistence of the problem, it is worth expanding the question: instead of training humans alone, why not explore whether AI agents can fill some of these gaps directly?

2.2 Human-AI Teaming

The emergence of AI as an everyday technology, sometimes called the Artificial Intelligence Revolution, has quickly reversed fears that AI would never succeed in applied settings (Li 2020). The ability to design AI to accomplish complex tasks with increasing levels of autonomy enables the use of a new team construct, where the AI is viewed as a teammate rather than a tool. A HAT consists of at least one human and one AI agent working interdependently in pursuit of shared goals (O'Neill et al. 2022). In other words, the AI agent must take on a fully independent team role that is integral to the team's accomplishment of overarching goals. For this to occur, the AI agent needs to operate with a minimum level of autonomy. HAT research has shown this minimum level to be that of partial autonomy, where the AI can fully execute a task once approved by a human (O'Neill et al. 2022). As such, it is essential to note that the AI referred to in this paper encompasses a wide range of technologies capable of acting as autonomous agents.

HAT constructs can provide significant advantages to teams, particularly those oriented around technical goals to which AI capabilities are naturally suited. HATs can work together to overcome challenges that all human teams struggle to overcome, such as tasks requiring

complex data operations (Nyre-Yu, Gutzwiller, and Caldwell 2019) and those spread over widespread geography (Chen 2023). Teaming is a unique type of collaboration, and experiments pitting all-human teams and all-AI teams against HATs have shown that HATs are more likely to underperform due to an inability to establish basic teaming components such as shared situational awareness and intra-team trust (McNeese et al. 2021). This means that AI teammates must incorporate human-centered design principles.

AI agents that require too much human oversight or act in an unexpected manner can actually increase the workload and stress of human workers (Hauptman et al. 2023). HAT research on situational autonomy has shown drastic increases in team performance when the team can modify an AI agent's autonomy levels (Salikutluk et al. 2024). Empirical research within the cybersecurity and medical fields have shown that too much AI autonomy can result in catastrophic failure states if the AI makes an error and a human teammate is unable to respond to correct it (Hauptman, Schelble, Flathmann, et al. 2024). This is because as AI operates with more autonomy, humans lose situational awareness of the AI's actions and their consequences (Onnasch et al. 2014). This is an important finding in the HAT community, as it slightly revises the need for an AI teammate to always operate with partial or full autonomy. This paper's position is that, in order to function as an AI teammate, the AI agent must be minimally capable of operating with partial autonomy. As humans are sometimes restricted from making independent decisions, an AI teammate could also be restricted from operating at higher autonomy levels under certain conditions.

2.3 AI Teammates in the Workforce

Much of the existing HAT research focuses on the gaming community due to the ability to customize AI agents within gaming platforms, as well as the recruitment pool of players used to partnering with virtual teammates (Zhang et al. 2021).

As researchers have sought to study the role of AI agents in applied settings, multiple recent studies have explored the promise of AI teammates in cybersecurity and cyber defense (Hauptman et al. 2023; Hauptman, Mallick, et al. 2024; Maennel and Maennel 2024; Malatji 2024). The security and defense of increasingly complex systems is an ideal space to investigate the use of AI teammates, as they would be much more capable of analyzing and adapting to emerging threats than their human counterparts (Malatji 2024). For instance, interviews with cyber incident responders suggested that AI teammates could be used to identify and operationalize indicators of compromise (IOCs) within an intrusion prevention system during incident response in real-time (Hauptman et al. 2023). This is an important consideration for critical infrastructure, where the ability to predict, detect, and respond to cyber threats is a new, essential capability that most organizations do not currently possess.

Developing an effective AI teammate for distinct purposes, such as cybersecurity, requires AI designers to consider a variety of human-AI interaction factors. Teams utilize several

mechanisms to coordinate and collaborate in pursuit of shared goals, mechanisms that need to be part of an AI teammate's design. For example, one study that incorporated an AI network infrastructure agent found that the way AI teammates communicate with human teammates should seamlessly integrate into its existing channels, as opposed to asynchronously providing humans with updates. Study participants noted that asynchronous updates would add mental load to already demanding jobs and be far more likely to be viewed as simply another tool (Hauptman, Schelble, Duan, et al. 2024).

Sometimes, these mechanisms cannot be replicated, as AI is inept at participating in behavioral communication, and failures of AI to replicate it have proven to produce worse team performance than if they tried not to replicate it at all (Demir, McNeese, and Cooke 2016). HAT research suggests that to overcome this, teams need to identify what essential information AI teammates need to communicate and develop the best ways for the AI to push that information in a manner that will be received positively by human teammates (Demir, McNeese, and Cooke 2016). Thus, an AI teammate that is effective in one environment may be ineffective if placed in a new type of team. For instance, an AI teammate designed to maintain a campus network with a small group of IT experts may be highly efficient and valued. However, if the same agent were deployed on a more secure network with focused cybersecurity professionals without modifications, it might be immediately disregarded as a liability. For this reason, it is essential that organizations determine which aspects of teaming are most crucial for an AI agent to replicate if it is to assume a full, interdependent team role.

3 PROCESS FOR DETERMINING IF/HOW TO EMPLOY AN AI TEAMMATE

Based on our research expertise in human–AI teaming, we developed a three-step process to help organizations assess whether, when, and how an AI teammate should be integrated into their workforce. The process presented in this paper is a conversation starter- it is intended to get critical infrastructure sectors thinking about the sources of their talent gaps, if AI is a probable solution, and, if so, identify the human-centered design considerations necessary for a successful human–AI collaboration.

The three steps are articulated as guiding questions that organizations should ask themselves when considering the integration of AI teammates: Is it a capacity or capability gap? What would be the role of the AI on the team? And what are some important human-centered design considerations? (Figure 1). Framing the process through these questions anchors the discussion in organizational needs, technological suitability, and human factors. The following subsections elaborate on each step in turn.

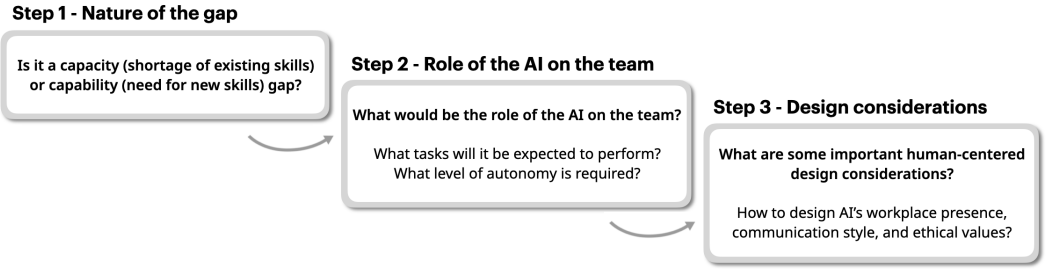


Figure 1. A 3-step process to determine if and how an AI teammate should be integrated.

3.1 Question 1: Is it a Capacity or Capability Gap?

The gaps that critical infrastructure sectors are struggling to fill can be classified by either an issue of *capacity* or an issue of *capability*. A capacity gap reflects skills that the team has organically possessed in the past but is currently struggling to maintain. This loss or shortage of skills is often due to retirement, turnover, or insufficient recruitment pipelines. In contrast, a capability gap concerns the emergence of new needs that existing human workers are ill-equipped to address. It arises when new operational demands, technologies, or threat vectors create requirements that the existing workforce is not equipped to meet. In the first case, an AI teammate is only beneficial in a small set of circumstances; whereas, in the case of a capability gap, an AI teammate is almost always value-added to the organization.

Understanding whether a workforce challenge reflects a loss of past capacity or the emergence of new capability demands is, therefore, a critical first step in determining whether, and how, an AI teammate should be integrated.

If you answered capacity gap:

What does a capacity gap mean for AI integration? Critical infrastructure sectors are encountering shallow hiring pools. Understanding the underlying causes of these shortages is essential for determining whether an organization should (a) invest in strategies to attract and retain human talent or (b) consider whether an AI agent could meaningfully supplement the team.

In some cases, the shallow pool is due to rising worker expectations around pay, benefits, and flexible work arrangements (Ashworth 2006). Over the years, sectors have utilized short-term fixes to fill critical roles. However, with sectors such as energy seeking to hire over 200,000 employees over the next three years (Hauser et al. 2025), it is increasingly clear that sustainable, long-term workforce solutions are necessary. For the most part, these positions remain inherently well-suited to human workers, and it behooves the sector to adapt to the changing demands of the workforce, as they are not going to disappear by filling one or two

team roles with AI. Instead, replacing humans in work roles that suit their capabilities and interests is more likely to breed fear of replacement and increase the rate of turnover among workers who experience negative emotional responses to the AI (Verma and Singh 2022). In such circumstances, an AI teammate is not an appropriate solution.

On the other hand, in many cases, the shallow hiring pool stems from a growing mismatch between the jobs available and the skills pursued by younger workers (Becker 2010). This poses a significant challenge for critical infrastructure organizations that require very specific skill sets that, for a variety of reasons, are considered unattractive to today's workforce. These reasons include lengthy or demanding educational pathways, lower entry-level salaries, rigid work schedules, and perceived status in the social hierarchy (Becker 2010). Because these issues typically lie beyond an individual organization's control, AI may offer a viable means of addressing persistent capacity shortages. In fact, strategically deploying AI in positions that are less attractive to the workforce may redirect human workers toward developing new skills needed to address emerging capability gaps.

If you answered capability gap:

What does a capability gap mean for AI integration? The capability gap refers to the emergence of new, largely technologically driven, needs in critical infrastructure sectors. Big data and AI-driven technologies are emerging as vital components of a sector's growth and efficient operations (Johnson et al. 2021). The incorporation of these technologies is generating new skill requirements in teams where workers must understand how to operate and leverage the technology (Johnson et al. 2021). As of 2024, the United States alone faced more than 500,000 unfilled cybersecurity-related positions (Dubov and Dubova 2025). Some of these skill gaps can, and should, be filled by humans with the right education and experience. As AI can fill repetitive, automatable job roles, humans are free to fill those that require greater degrees of creativity and reason (Daugherty and Wilson 2018).

However, some emerging roles require levels of speed, precision, pattern recognition, or computational breadth that surpass human cognitive limits to truly leverage the technology for the team. For instance, cyber incident responders report the need for AI teammates that can collect, analyze, and make sense of network data more quickly and accurately than a human analyst (Hauptman et al. 2023). This could be particularly useful for critical infrastructure sectors involving Supervisory Control and Data Acquisition (SCADA) systems, as AI solutions can overcome the challenges of having to monitor, understand, and compare various protocols and languages simultaneously (Aldossary, Ali, and Alasaadi 2021). Thus, in the case of a capability gap, an AI teammate is a promising solution to an organization's talent gap.

3.2 Question 2: What would be the Role of the AI on the Team?

Once the gaps that an organization wants to address with an AI teammate are identified, the next step is to define the scope of the AI teammate's role clearly. This scoping process mirrors how one would scope a position for a human hire. It involves two complementary decisions. First, the organization must determine which tasks the AI agent will be expected to perform. Second, it needs to understand and define how much autonomy the AI agent should be given to accomplish those tasks efficiently and safely. Together, these decisions ensure that the AI teammate is positioned to contribute meaningfully without introducing unnecessary risks or ambiguity in its role.

Scope the AI role with the necessary tasks.

The most common use of AI is as a tool or assistive technology. In contrast, an AI agent functioning as a teammate is intended to occupy a defined, independent role rather than merely augment one already filled by a human (O'Neill et al., 2020). Human-AI teaming research has extensively investigated what roles would be best suited for an AI agent, based on its unique capabilities and realistic limitations. Studies show that roles involving the collection, integration, and analysis of vast amounts of data (Enskovitch et al. 2021), as well as the strict application of predefined actions (Hauptman et al. 2023) are well suited for AI teammates.

Conversely, roles requiring nuanced judgment, frequent adaptation to novel situations, or precise physical interaction with the environment remain better matched to human workers (Hauptman, Schelble, Duan, et al. 2024). For instance, studies have highlighted the potential of AI teammates as network security analysts, responsible for collecting and analyzing vast amounts of distributed data, or as healthcare assistants capable of storing and utilizing a patient's historical data and symptom patterns to develop a diagnosis (Hauptman, Schelble, Duan, et al. 2024).

Scope the AI role with the right level(s) of autonomy.

Once a team has determined that a specific role is suited for an AI teammate, the next step is to specify the level of autonomy that AI should have in executing its assigned tasks. This decision is analogous to determining a human worker's place in the management hierarchy, clarifying not only what the agent does but also how independently it is allowed to act. Human-AI teaming research has attempted to adapt and apply the levels of automation into the levels of autonomy to design and classify autonomous agents (O'Neill et al. 2022). As noted in Section 2, to be considered a teammate, an AI agent must minimally operate with the ability to fully execute its team role.

Further considerations include that the AI possesses enough autonomy to perform its duties without unduly increasing the workload or supervisory burden on human teammates (Hauptman et al. 2023). At the same time, its autonomy should not exceed the point at which it begins making decisions for which it lacks the necessary programming, contextual understanding, or reasoning capabilities (Hauptman, Schelble, Flathmann, et al. 2024). This ladder concept is of particular importance to teams that operate in high-risk environments, as the *ironies of autonomy* show that the more autonomy that AI has, the less capable human teammates are of detecting and responding to AI failures (Ganesh 2020). This balance is essential for teams that frequently navigate ethically ambiguous situations, a topic further explored in the third question.

3.3 Question 3: What are Important Human-centered Design Considerations Necessary to Ensure Effective Teaming?

Competent AI agents are not guaranteed to be either effective or accepted by a team (Flathmann et al. 2023). Empirical studies have shown that humans are more likely to trust and positively perceive an AI teammate when they perceive more similarities between themselves and the AI (Georganta and Ulfert 2024). In fact, several human-centered design considerations have been explored for generating trust in human-AI teams in the workplace (Hauptman, Duan, and McNeese 2022). This section highlights three such considerations particularly relevant for the design of an AI teammate operating in critical infrastructure sectors: workplace presence, explainability and communication style, and ethical ideology.

Design for the AI teammate's workplace presence.

An essential part of customizing an AI teammate is designing the type of presence the AI will have in the workplace. In many instances, an AI teammate may be required to have no physical presence at all, operating purely as a software agent embedded within a system or network resource. Even so, the nature of its presence—and how that presence is communicated to the team—often requires additional design attention. A recent study has shown that AI teammates should possess a degree of presence that is on par with how human team members are used to engaging with one another. For example, teams that collaborate in a physical workplace every day would more readily trust and accept an AI teammate that exhibits some form of physical embodiment. Conversely, teams that are geographically dispersed and communicate over video conferencing would prefer an AI represented through an avatar or visual agent consistent with their communication norms (Hauptman et al. 2023). This is an important design consideration for critical infrastructure sectors, where trust, clarity, and shared situational awareness are central to safe operations. As such, AI teammates may require additional representational layers and embodiments beyond what is necessary for them to function and complete their tasks. For instance, while an AI teammate operating

as a network analyst may not require a physical presence to perform its duties, providing a dedicated interface or "presence point" within the team's workspace can substantially improve how its alerts, findings, and recommendations are perceived and acted upon.

Future research should investigate how these presence-related design choices function in real-world deployments, as empirical work in operational settings remains limited. The field could also benefit from drawing more systematically on insights from adjacent domains such as human–robot interaction (Putlitz and Roesler 2024), Computer-Supported Collaborative Work (CSCW), and digital twin research, all of which offer insightful perspectives on embodiment, co-presence, and mediated interaction. Additionally, design scholarship on data physicalization (Bae et al. 2022; Jansen et al. 2015) provides a rich repertoire of approaches for making computational agents and their outputs more legible, tangible, and meaningfully integrated into human work practices.

Design the AI teammate to communicate with the team.

An important component of an AI teammate's presence is how it communicates. Explainable AI (XAI) is an extremely active research area, and is commonly defined as "an interface between humans and a decision maker that is, at the same time, both an accurate proxy of the decision maker and comprehensible to humans" (Chatila et al. 2021). In essence, effective explanations from an AI to a human must be relevant to the decision at hand, accurate in representing the AI's reasoning, and communicated in a way that is understandable and usable by the human receiving it. While research generally supports AI explanations as increasing trust in AI systems (Schoenherr et al. 2023), human-AI teaming research has shown that overly detailed or frequent explanations can have the opposite effect (Hauptman, Mallick, et al. 2024). Evidence also suggests that the method by which an AI agent's explanations are communicated is more important to human teammates. It is essential that an AI teammate's explanations reflect how the team generally communicates. This extends to preferred communication platforms (email, messaging platforms, reports), modalities (written, verbal, imagery) and frequency (Hauptman, Mallick, et al. 2024). Aligning with these norms helps ensure that explanations feel natural, appropriately timed, and easy to integrate into existing workflows.

Design the AI teammate to reflect the team's ethical values.

AI teammates need to communicate more than just their actions. An integral component of AI teammate acceptance is how well the AI seems to understand and exhibit adherence to the team's shared ethical code. This shared code is an essential part of effective teaming (Ouakouak and Ouedraogo 2019). Shared codes of ethics are vital to professional organizations in critical infrastructure sectors that make decisions affecting the safety and welfare of workers, clients, and society on a daily basis (Nichols, Nichols, and Nichols 2007). HAT research has thus

proposed that AI teammates that are designed to incorporate and consider the shared ethical ideology of their team are more likely to be trusted and accepted as teammates (Flathmann et al. 2021).

That humans can trust an AI agent to consider and act in accordance with the team's ethical code is integral to long-term teaming in the workplace, as studies show that classic trust repair strategies are ineffective when an AI agent commits an ethical violation (Textor et al. 2022). This will be harder to design for in some sectors than others, depending on the extent to which the sector has a set of codified ethical principles on which everyone trains, such as the medical sector's Hippocratic Oath (Nicolaides 2014). In addition to guiding behavior, ethical codes can also be used to design AI teammates that adapt autonomy levels in response to ethical dilemmas, thereby preventing violations of the team's ethical code (Hauptman, Schelble, and McNeese 2022). This represents a promising human-centered design feature, as it acknowledges the inherently variable nature of ethics in complex, dynamic environments, and promotes responsible AI behavior before violations occur.

4 THE WAY FORWARD

As several critical infrastructure sectors begin to address growing talent gaps in their workforces, it is essential to recognize not only the challenges but also the opportunities presented by the increasing capabilities and adoption of AI technologies. Many of the demands faced by these sectors are due to the creation of new team roles required to collect, understand, and utilize large data sets, tasks that lend themselves well to AI agents. Consequently, human-AI teaming constructs are a promising solution to overcoming current and forthcoming talent gaps.

To do this effectively, this paper introduced a question-based framework for identifying and scoping the roles of AI agents designed to work as teammates in critical infrastructure organizations. This framework should be understood as a starting point rather than a mature model, and the public and private sectors need to take multiple next steps to test and refine it. Future work is necessary to further develop and validate the framework. While the present article provides conceptual guidance, it does not include case studies that demonstrate how the framework operates in real operational environments. To fully operationalize the "how," future research should translate these questions into concrete organizational workflows, develop maturity models or decision trees, and create actionable checklists tailored to sector needs. These steps will be crucial for transforming the framework into a practical tool for critical infrastructure cyber defense.

Critical infrastructure organizations should apply the guiding framework proposed in this paper to clarify their talent gaps, understand the sources of those gaps, and determine which roles in their organizations are most suited for AI teammates. As noted in Section 2, most

HAT research to date has been conducted in low-risk or gaming settings. Governments and industry partners will need to invest in pilot programs that allow organizations to experiment with these roles in operational environments, helping them identify the human-centered design features most critical for effective integration into sector-specific teams.

Ultimately, while AI holds enormous potential for these sectors, it is also true that their integration comes with nuances and associated risks. Research on human–AI teaming is still recent, and many questions about real-world implementation, organizational fit, and long-term impacts remain open. Poorly designed systems, incorrect autonomy levels, and vulnerability to cyber attacks could all derail the employment of AI and exacerbate, rather than alleviate, the talent gap. Accordingly, iterative evaluations and field testing are essential and researchers must continue to refine and adapt this framework to include sector-specific considerations and lessons learned. Doing so will enable the development of AI teammates that critical infrastructure organizations can adopt, accept, and utilize in the real world.

ABOUT THE AUTHOR

MAJ Allyson Hauptman is a Cyber Warfare Officer in the United States Army and a senior researcher at the Army Cyber Institute at West Point. She holds a master's degree in Cybersecurity from Tallinn Technical University and a doctorate in Human-Centered Computing from Clemson University, where her dissertation focused on adaptive autonomous teammates. Her research areas include human-AI teaming, adaptive autonomy, and cyber defense policy.

ACKNOWLEDGMENTS

Thank you to the participants at the 2025 Jack Voltaic Workshop on Cyber Resilience and National Power Projection for your insights and contributions to the framework presented in this article.

REFERENCES

Aldossary, Lina Abdulaziz, Mazen Ali, and Abdulla Alasaadi. 2021. "Securing SCADA systems against cyber-attacks using artificial intelligence." In *2021 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT),* 739–745. IEEE. https://doi.org/10.1109/3ICT53449.2021.9581394.

Asare, Isak Nti, Scott Shackelford, Jungwoo Chun, and Sarah Powazek. 2025. "Protecting Communities while Training Future Cybersecurity Professionals: Lessons from the Consortium of Cybersecurity Clinics." *The Cyber Defense Review* 10 (2). https://doi.org/10.556582/cdr/1dm8-wekj.

Ashley, Travis D., Roger Kwon, Sri Nikhil Gupta Gourisetti, Charalampos Katsis, Christopher A. Bonebrake, and Paul A. Boyd. 2022. "Gamification of cybersecurity for workforce development in critical infrastructure." *IEEE Access* 10:112487–112501. https://doi.org/10.1109/ACCESS.2022.3216711.

Ashworth, Michael J. 2006. "Preserving knowledge legacies: workforce aging, turnover and human resource issues in the US electric power industry." *The International Journal of Human Resource Management* 17 (9): 1659–1688. https://doi.org/10.1080/09585190600878600.

Ayodele, Olabode Adekunle, Alice Chang-Richards, and Vicente Gonzalez. 2020. "Factors affecting workforce turnover in the construction sector: A systematic review." *Journal of Construction Engineering and Management* 146 (2): 04019112. https://doi.org/10.1061/(ASCE)CO.1943-7862.0001725.

Bae, S. Sandra, Clement Zheng, Mary Etta West, Ellen Yi-Luen Do, Samuel Huron, and Danielle Albers Szafir. 2022. "Making Data Tangible: A Cross-disciplinary Design Space for Data Physicalization." In *Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems.* New York, NY, USA: Association for Computing Machinery. https://doi.org/10.1145/3491102.3501939.

Becker, Frank Stefan. 2010. "Why don't young people want to become engineers? Rational reasons for disappointing decisions." *European Journal of Engineering Education* 35 (4): 349–366. https://doi.org/10.1080/03043797.2010.489941.

Chatila, Raja, Virginia Dignum, Michael Fisher, Fosca Giannotti, Katharina Morik, Stuart Russell, and Karen Yeung. 2021. "Trustworthy AI." In *Reflections on Artificial Intelligence for Humanity,* edited by Bertrand Braunschweig and Malik Ghallab, 13–39. Cham: Springer International. https://doi.org/10.1007/978-3-030-69128-8_2.

Chen, Zhisheng. 2023. "Collaboration among recruiters and artificial intelligence: removing human prejudices in employment." *Cognition, Technology and Work* 25 (1): 135–149. https://doi.org/10.1007/s10111-022-00716-0.

Daugherty, Paul R., and H. James Wilson. 2018. *Human + Machine: Reimagining Work in the Age of AI.* Boston, MA: Harvard Business Review Press.

Demir, Mustafa, Nathan J. McNeese, and Nancy J. Cooke. 2016. "Team communication behaviors of the human-automation teaming." In *2016 IEEE International Multi-disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA),* 28–34. IEEE. https://doi.org/10.1109/COGSIMA.2016.7497782.

Dubov, Dmytro, and S. Dubova. 2025. "A Global Shortfall of Cyber Workforce: Evaluating the US Strategy and Approach and Ukraine's Emerging Challenges." *Actual Problems of International Relations* 1 (162): 55–62. https://doi.org/10.17721/apmv.2025.162.1.55-62.

Durkovich, Caitlin. 2020. "Protecting Critical Infrastructure." In *Beyond 9/11: Homeland Security for the Twenty-First Century,* edited by Chappell Lawson, Alan Bersin, and Juliette N. Kayyem. MIT Press. https://doi.org/10.7551/mitpress/13831.003.0012.

Enskovitch, John, Corey Fallon, Kate Miller, and Aritra Dasgupta. 2021. "Beyond visual analytics: Human-machine teaming for AI-driven data sensemaking." In *2021 IEEE Workshop on Trust and Expertise in Visual Analytics (TREX),* 40–44. IEEE. https://doi.org/10.1109/TREX53765.2021.00012.

Fiume, Leonard J., Ilya Grinberg, Mohammed Safiuddin, and Robert F. Zahm. 2006. "A partnership between the electrical power industry and academia to address the technical talent gap." In *2006 IEEE PES Power Systems Conference and Exposition,* 655–659. IEEE. https://doi.org/10.1109/PSCE.2006.296396.

Flathmann, Christopher, Beau G. Schelble, Nathan J. McNeese, Bart Knijnenburg, Anand K. Gramopadhye, and Kapil Chalil Madathil. 2023. "The purposeful presentation of AI teammates: Impacts on human acceptance and perception." *International Journal of Human-Computer Interaction* 40 (20): 6510–6527. https://doi.org/10.1080/10447318.2023.2254984.

Flathmann, Christopher, Beau G. Schelble, Rui Zhang, and Nathan J. McNeese. 2021. "Modeling and guiding the creation of ethical human-AI teams." In *Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society,* 469–479. https://doi.org/10.1145/3461702.3462573.

Ganesh, Maya Indira. 2020. "The ironies of autonomy." *Humanities and Social Sciences Communications* 7 (1): 1–10. https://doi.org/10.1057/s41599-020-00646-0.

Georganta, Eleni, and Anna-Sophie Ulfert. 2024. "Would you trust an AI team member? Team trust in human-AI teams." *Journal of Occupational and Organizational Psychology* 97 (3): 1212–1241. https://doi.org/10.1111/joop.12504.

Goure, Daniel. 2018. "Winning future wars: Modernization and a 21st century defense industrial base." *The Heritage Foundation, 2019 Essays,* no. 4, 61–92. https://www.heritage.org/military-strength-topical-essays/2019-essays/winning-future-wars-modernization-and-21st-century.

Hauptman, Allyson I., Wen Duan, and Nathan J. McNeese. 2022. "The Components of Trust for Collaborating With AI Colleagues." In *Companion Publication of the 2022 Conference on Computer Supported Cooperative Work and Social Computing,* 72–75. CSCW'22 Companion. Virtual Event, Taiwan: Association for Computing Machinery. https://doi.org/10.1145/3500868.3559450.

Hauptman, Allyson I., Rohit Mallick, Christopher Flathmann, and Nathan J. McNeese. 2024. "Human factors considerations for the context-aware design of adaptive autonomous teammates." *Ergonomics* 68 (4): 571–587. https://doi.org/10.1080/00140139.2024.2380341.

Hauptman, Allyson I., Beau G. Schelble, Wen Duan, Christopher Flathmann, and Nathan J. McNeese. 2024. "Understanding the influence of AI autonomy on AI explainability levels in human-AI teams using a mixed methods approach." *Cognition, Technology and Work* 26:435–455. https://doi.org/10.1007/s10111-024-00765-7.

Hauptman, Allyson I., Beau G. Schelble, Christopher Flathmann, and Nathan J. McNeese. 2024. "The Role of Autonomy Levels and Contextual Risk in Designing Safer AI Teammates." In *2024 IEEE 4th International Conference on Human-Machine Systems (ICHMS).* IEEE. https://doi.org/10.1109/ICHMS59971.2024.10555844.

Hauptman, Allyson I., Beau G. Schelble, and Nathan J. McNeese. 2022. "Adaptive Autonomy as a Means for Implementing Shared Ethics in Human-AI Teams." In *Proceedings of the AAAI Spring Symposium on AI Engineering.*

Hauptman, Allyson I., Beau G. Schelble, Nathan J. McNeese, and Kapil Chalil Madathil. 2023. "Adapt and overcome: Perceptions of adaptive autonomous agents for human-AI teaming." *Computers in Human Behavior* 138. https://doi.org/10.1016/j.chb.2022.107451.

Hauser, Michael, Donald Paul, Jim Crompton, and Iraj Ershaghi. 2025. "Workforce Development for the Energy Industry." Paper presented at the SPE Western Regional Meeting, Garden Grove, California, USA, April 2025. SPE. https://doi.org/10.2118/224208-MS.

Jansen, Yvonne, Pierre Dragicevic, Petra Isenberg, Jason Alexander, Abhijit Karnik, Johan Kildal, Sriram Subramanian, and Kasper Hornbæk. 2015. "Opportunities and Challenges for Data Physicalization." In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 3227–3236. CHI '15. Seoul, Republic of Korea: Association for Computing Machinery. https://doi.org/10.1145/2702123.2702180.

Johnson, Marina, Rashmi Jain, Peggy Brennan-Tonetta, Ethne Swartz, Deborah Silver, Jessica Paolini, Stanislav Mamonov, and Chelsey Hill. 2021. "Impact of big data and artificial intelligence on industry: developing a workforce roadmap for a data driven economy." *Global Journal of Flexible Systems Management* 22 (3): 197–217. https://doi.org/10.1007/s40171-021-00272-y.

Lewis, Ted G. 2019. *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation.* John Wiley & Sons.

Li, Robin. 2020. *Artificial intelligence revolution: How AI will change our society, economy, and culture.* Skyhorse Publishing.

Maennel, Kaie, and Olaf M. Maennel. 2024. "Human-AI Collaboration and Cyber Security Training: Learning Analytics Opportunities and Challenges." In *2024 17th International Conference on Security of Information and Networks (SIN),* 01–08. IEEE.

Malatji, Masike. 2024. "Human-Artificial Intelligence Teaming Model in Cybersecurity." In *2024 International Conference on Intelligent Cybernetics Technology and Applications (ICICyTA),* 216–220. IEEE. https://doi.org/10.1109/ICICYTA64807.2024.10913351.

Malatji, Masike, Annlize L. Marnewick, and Sune von Solms. 2022. "Cybersecurity capabilities for critical infrastructure resilience." *Information and Computer Security* 30 (2): 255–279. https://doi.org/10.1108/ICS-06-2021-0091.

McNeese, Nathan J., Beau G. Schelble, Lorenzo Barberis Canonico, and Mustafa Demir. 2021. "Who/what is my teammate? Team composition considerations in human-AI teaming." *IEEE Transactions on Human-Machine Systems* 51 (4): 288–299. https://doi.org/10.1109/THMS.2021.3086018.

Nichols, Nick, George V. Nichols, and Patsy A. Nichols. 2007. "Professional Ethics: The Importance of Teaching Ethics to Future Professionals." *Professional Safety* 52 (7).

Nicolaides, Angelo. 2014. "The Critical Role of Ethics Training in Medical Education." *African Journal of Hospitality, Tourism and Leisure* 3 (1): 1–12.

Nyre-Yu, Megan, Robert S. Gutzwiller, and Barrett S. Caldwell. 2019. "Observing cyber security incident response: qualitative themes from field research." In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 63:437–441. 1. SAGE Publications. https://doi.org/10.1177/1071181319631016.

O'Heir, Jeff. 2017. "Filling the talent gap." *Mechanical Engineering* 139 (1): 28–33. https://doi.org/10.1115/1.2017-JAN-1.

O'Neill, Thomas, Nathan J. McNeese, Amy Barron, and Beau Schelble. 2022. "Human-autonomy teaming: A review and analysis of the empirical literature." *Human Factors* 64 (5): 904–938. https://doi.org/10.1177/0018720820960865.

Olonilua, Oluponmile, and John Ogbeleakhu Aliu. 2025. "Assessing Workforce Training Strategies in Critical Infrastructure: Insights and Recommendations (Report No. IHS-2025-1000)." *Institute for Homeland Security,* https://hdl.handle.net/20.500.11875/5062.

Onnasch, Linda, Christopher D. Wickens, Huiyang Li, and Dietrich Manzey. 2014. "Human performance consequences of stages and levels of automation: An integrated meta-analysis." *Human Factors* 56 (3): 476–488. https://doi.org/10.1177/0018720813501549.

Ouakouak, Mohammed Laid, and Noufou Ouedraogo. 2019. "Fostering knowledge sharing and knowledge utilization: The impact of organizational commitment and trust." *Business Process Management Journal* 25 (4): 757–779. https://doi.org/10.1108/BPMJ-05-2017-0107.

Putlitz, Johanna zu, and Eileen Roesler. 2024. "Let's get physical: The influence of embodiment on industrial human-robot interaction." *Proc. Hum. Factors Ergon. Soc. Annu. Meet.* 68, no. 1 (September): 437–443.

Salikutluk, Vildan, Janik Schöpper, Franziska Herbert, Katrin Scheuermann, Eric Frodl, Dirk Balfanz, Frank Jäkel, and Dorothea Koert. 2024. "An Evaluation of Situational Autonomy for Human-AI Collaboration in a Shared Workspace Setting." In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems.* CHI '24. Honolulu, HI, USA: Association for Computing Machinery. https://doi.org/10.1145/3613904.3642564.

Sandborn, Peter A., and Varun J. Prabhakar. 2015. "The forecasting and impact of the loss of critical human skills necessary for supporting legacy systems." *IEEE Transactions on Engineering Management* 62 (3): 361–371. https://doi.org/10.1109/TEM.2015.2438820.

Schoenherr, Jordan Richard, Roba Abbas, Katina Michael, Pablo Rivas, and Theresa Dirndorfer Anderson. 2023. "Designing AI Using a Human-Centered Approach: Explainability and Accuracy Toward Trustworthiness." *IEEE Transactions on Technology and Society* 4 (1): 9–23. https://doi.org/10.1109/TTS.2023.3257627.

Textor, Claire, Rui Zhang, Jeremy Lopez, Beau G. Schelble, Nathan J. McNeese, Guo Freeman, Richard Pak, Chad Tossell, and Ewart J. de Visser. 2022. "Exploring the relationship between ethics and trust in human-artificial intelligence teaming: A mixed methods approach." *Journal of Cognitive Engineering and Decision Making* 16 (4): 252–281. https://doi.org/10.1177/15553434221113964.

Thomas, Richard J., and Tom Chothia. 2021. "Learning from vulnerabilities-categorizing, understanding and detecting weaknesses in industrial control systems." In *Computer Security: ESORICS 2020 International Workshops, CyberICPS, SECPRE, and ADIoT, Revised Selected Papers,* 100–116. Springer International Publishing. https://doi.org/10.1007/978-3-030-64330-0_7.

Verma, Surabhi, and Vibhav Singh. 2022. "Impact of artificial intelligence-enabled job characteristics and perceived substitution crisis on innovative work behavior of employees from high-tech firms." *Computers in Human Behavior* 131:107215. https://doi.org/10.1016/j.chb.2022.107215.

Wagner, Paul. 2021. *Critical Infrastructure Security.* SSRN 3762693. https://doi.org/10.2139/ssrn.3762693.

Zhang, Rui, Nathan J. McNeese, Guo Freeman, and Geoff Musick. 2021. ""An ideal human": expectations of AI teammates in human-AI teaming." *Proceedings of the ACM on Human-Computer Interaction* 4 (CSCW3): 1–25. https://doi.org/10.1145/3432945.

Received 13 March 2025; Revised 5 November 2025; Accepted 20 November 2025

THE CYBER DEFENSE REVIEW
2025, VOL. 10, NO. 2, 241-265
https://doi.org/10.55682/cdr/1dm8-wekj

RESEARCH ARTICLE

Protecting Communities while Training Future Cybersecurity Professionals: Lessons from the Consortium of Cybersecurity Clinics

Isak Nti Asare[1], Scott Shackelford*[1], Jungwoo Chun[2], Sarah Powazek[3]

[1]Indiana University, Bloomington, IN, USA
[2]MIT: Massachusetts Institute of Technology, Cambridge, MA, USA
[3]University of California, Berkeley, Berkeley, CA, USA

Communities across the United States and globally are increasingly vulnerable to cyberattacks targeting critical infrastructure, nonprofits, and other trusted institutions. In response, a national consortium of universities and community colleges has established cybersecurity clinics to address this challenge through an innovative, action-oriented approach. This article explores the role of clinical education not only in training cybersecurity professionals, but also in scaling the development of clinics to improve the security posture of critical infrastructure providers. By integrating classroom instruction, hands-on practice, direct client interaction, and close supervision, clinics can bridge the gap between theory and practice, enhancing public sector cyber resilience while having institutions of higher education meet their larger social obligations. Case studies from the consortium of cybersecurity clinics—including those at Indiana University, MIT, and UC Berkeley—illustrate the role these clinics have already played in supporting critical infrastructure and advancing national cyber resilience efforts. Furthermore, we examine the clinics' role in promoting change and improvement in cyber culture within a wide range of government and non-governmental organizations. This work provides a foundation for the continued expansion of cybersecurity clinics as a model for national cyber resilience, offering key insights into ways of strengthening cyber defenses and protecting critical infrastructure.

Keywords: Cyber resilience, critical infrastructure Protection, cybersecurity clinics, clinical education, public sector, cybersecurity training, community defense

* Corresponding author: sjshacke@iu.edu

1 INTRODUCTION

Communities across the United States are increasingly vulnerable to cyberattacks targeting critical infrastructure, nonprofits, and other trusted institutions. While national security debates often focus on federal capabilities and corporate defenses, many of the most acute risks originate at the local level, where resource-strapped governments, utilities, and service organizations remain exposed to sophisticated adversaries. These vulnerabilities are not only a local concern—they create systemic risks for national defense and power projection. Strengthening cyber resilience at the community level is therefore a strategic imperative for national security.

In recent years, a novel model has emerged to address this challenge: the university-based cybersecurity clinic. Inspired by clinical education in medicine and law, cybersecurity clinics embed students in hands-on engagements with real organizations under faculty supervision. Clinics offer pro bono or low-cost services, including security assessments, incident response planning, and staff training, to public-serving institutions that cannot otherwise afford professional cybersecurity support. At the same time, they serve as a training ground for the next generation of cybersecurity professionals, equipping students with interdisciplinary skills in technical defense, policy, law, and organizational governance.

This paper examines the impact of cybersecurity clinics on critical infrastructure resilience and national power projection, focusing on case studies from the consortium of cybersecurity clinics, including those at Indiana University, MIT, and UC Berkeley. It argues that cybersecurity clinics not only serve as incubators for interdisciplinary education but also function as essential contributors to the broader effort of fortifying cyber resilience across sectors in line with principles from Public Interest Technology (PIT). What makes this model particularly powerful is that while these clinics operate as independent units, through the consortium of clinics, they coordinate strategically, allowing them to share best practices, improve methodologies, and scale impact across different regions and sectors. By fostering collaboration among universities, these clinics create a networked approach to cybersecurity capacity-building, ensuring that solutions developed in one setting can be adapted and applied elsewhere. As such, we present the clinic model as a scalable, collaborative framework for strengthening cybersecurity capacity at the local, national, and international levels, ultimately supporting broader national security and power projection efforts.

The paper proceeds in five parts. Section 2 situates cybersecurity clinics within the broader landscape of PIT and clinical education. Section 3 examines the cybersecurity challenges facing state and local governments and nonprofits, highlighting the gaps clinics are designed to fill. Section 4 elaborates on the design and pedagogical underpinnings of the clinic model. Section 5 presents detailed case studies of MIT, UC Berkeley, and Indiana University, followed

by a comparative analysis. Section 6 concludes with policy recommendations for scaling cybersecurity clinics as a national resilience strategy.

2 BACKGROUND

2.1 Cybersecurity as a Strategic Imperative: Interdisciplinary Solutions for National Resilience and Power Projection

Cybersecurity is a fundamental pillar of national defense and economic power. The ability of a nation to protect its critical infrastructure, respond to cyberattacks, and project power in cyberspace requires interdisciplinary competencies that span public policy, public administration, law, organizational behavior, business management, education, and applied social sciences. Cybersecurity involves a vast network of stakeholders—multiple levels of government, NGOs, private-sector enterprises, and community organizations—each operating under distinct regulations, missions, and resource constraints. However, all contribute to mitigating cybersecurity risks.

Policymakers, for example, establish regulations that shape cybersecurity governance; legal experts interpret and ensure compliance; behavioral scientists study and influence user behavior to reduce vulnerabilities; and technologists develop and implement security measures. These roles do not operate in isolation—regulations influence technical design choices, legal frameworks shape organizational security policies, and human behavior determines the effectiveness of even the most advanced cybersecurity tools. As a result, an integrated and interdisciplinary approach is essential to effectively address cybersecurity risks. In the context of national security, cyber threats to critical infrastructure pose significant risks to military readiness and power projection (Clarke and Knake 2019).

As recent cyber incidents have demonstrated, adversarial state and non-state actors increasingly target essential services—such as power grids, transportation systems, and emergency response networks—to disrupt civilian life and military operations (Borghard and Lonergan 2017). The 2021 Colonial Pipeline ransomware attack underscored the vulnerability of civilian infrastructure managed by cyber threats, leading to fuel shortages that affected economic stability and public confidence (Beerman et al. 2023). Meanwhile, cyber-enabled disinformation campaigns have further demonstrated how digital vulnerabilities can be exploited to undermine social cohesion and weaken national decision-making (Nye 2019). Again, addressing these challenges requires a holistic approach that integrates technical expertise with policy, legal, and operational considerations.

Cybersecurity clinics provide a compelling model for strengthening cyber resilience at the local, national, and international levels by directly addressing critical infrastructure vulnerabilities, supporting national security priorities, and fostering the next generation of

cybersecurity professionals. A significant challenge in national cyber defense is that many critical infrastructure providers—such as small municipal governments, regional water utilities, rural healthcare networks, and nonprofit service providers—operate with severely limited cybersecurity resources (Preis and Susskind 2022; Norris et al. 2021). These organizations often lack dedicated security personnel, robust cyber hygiene practices, or the ability to defend against sophisticated cyber threats, making them attractive targets for adversarial state and non-state actors (Fox-Sowell 2024). Because military operations frequently depend on civilian-managed infrastructure, vulnerabilities in these under-resourced sectors present a direct risk to national power projection and operational readiness. By securing these essential services, cybersecurity clinics may help reduce systemic cyber risks that adversaries could exploit to disrupt national defense capabilities.

We argue that the work of clinics strengthens the broader cyber ecosystem, reducing the attack surface that foreign actors might leverage in cyber-enabled coercion or warfare. In addition, we maintain that cybersecurity clinics provide a scalable model to expand national cybersecurity capacity. By forming structured partnerships with federal and state agencies, the clinic model should be integrated into the national cybersecurity strategies.

2.2 Public Interest Technology and the Role of Cybersecurity Clinics in Community Resilience

Public Interest Technology (PIT) is an emerging field that applies technological expertise to advance the public good, ensuring that technology serves community well-being (McGuinness and Schank 2021). PIT aligns technological innovation with civic responsibility, emphasizing the development of tools, policies, and interventions that promote transparency, accessibility, and security for all communities—particularly those that are under-resourced or disproportionately affected by digital threats. Cybersecurity clinics represent a key instantiation of PIT, as they channel university resources, technical expertise, and student training and engagement toward mitigating cyber risks for public-serving institutions such as local governments, nonprofits, hospitals, and small businesses.

Cybersecurity is often framed in terms of corporate risk management and national defense, yet its impact on small businesses, local governments, nonprofits, and other public services is equally urgent (Zoghbi 2024). In fact, increased threats and attacks aimed at critical infrastructure present a risk to national defense and power projection. These organizations rely on digital systems to deliver essential services but frequently lack the resources to protect themselves from rapidly evolving cyber threats (CISA 2024). Cybersecurity clinics embody the principles of PIT by bridging the gap between academic learning and real-world public service, aligning student education with community-based cybersecurity interventions that enhance the resilience of public-serving organizations.

A key strength of cybersecurity clinics is their ability to deliver professional-grade services to organizations that cannot afford traditional consultancy fees. Many local agencies, municipalities, and nonprofits operate with minimal IT staffing and shoestring budgets, making them especially vulnerable to cyberattacks (Pattison-Gordon 2024). By offering pro bono or low-cost assessments, cyber hygiene training, and incident response planning, clinics help these organizations adopt robust security practices that would otherwise be out of reach. This direct engagement has a transformative effect: clinics don't just provide short-term fixes—they help organizations internalize cybersecurity as an ongoing responsibility, ensuring that best practices persist long after the engagement ends.

Beyond immediate technical support, cybersecurity clinics address systemic inequities in cybersecurity access. Vulnerable populations—such as rural communities, lower-income groups, tribal nations, and older generations—are often disproportionately impacted by cyber incidents (World Economic Forum 2022). Cybersecurity clinics help close the digital divide, providing culturally and contextually tailored cybersecurity education and services. Importantly, students gain critical skills in communicating cybersecurity concepts in plain language, ensuring that effective security measures are inclusive and accessible rather than exclusive to well-funded entities.

In addition to serving immediate needs, cybersecurity clinics help cultivate a pipeline of public sector cyber talent. Even when state or local governments wish to improve their security posture, they often struggle to attract qualified professionals who might prefer higher-paying private sector jobs (Norris et al. 2021). Clinic engagements bridge this gap by exposing students to real-world public sector challenges—and in doing so, enable students to pursue their growing interest in public service. This fusion of education and civic duty benefits both sides: organizations receive targeted support, while students gain experience that can shape their professional trajectories toward service-oriented roles.

Finally, cybersecurity clinics influence policy by revealing systemic gaps in local governance and resource allocation. Municipalities partnering with clinics often discover the need for clearer regulations or dedicated funding to lend aid during local cybersecurity crises. As students deliver their final reports or exit briefings, they frequently highlight policy-level changes that may strengthen an organization's long-term resilience. Over time, these interactions can spark efforts to implement broader legislative or budgetary reforms. In this way, the clinic model not only helps individual clients but may also steer decision-makers toward developing more thorough cybersecurity frameworks at the local, state, or even federal levels. Some cybersecurity clinics have gone beyond client engagements to produce policy proposals that reflect lessons learned from their work with community and local government stakeholders. Over time, these engagements may catalyze broader legislative and regulatory reforms, strengthening cybersecurity at the local, state, and even federal levels.

2.3 The State of Community and Local Government Cybersecurity

Local governments and community organizations are on the front lines of cybersecurity threats, yet they often lack the resources, expertise, and personnel to defend against increasingly sophisticated cyberattacks. These vulnerabilities do not exist in isolation—foreign adversaries and cybercriminals increasingly target municipal agencies, public schools, and healthcare providers as a means to disrupt broader national systems. Because national security depends on the resilience of local and regional infrastructure, these persistent gaps in local cybersecurity have far-reaching consequences for national cyber defense and power projection. Scholarly work has begun to show that this is not just a practical gap but a research gap: municipal cybersecurity remains comparatively underexamined relative to national or sectoral critical-infrastructure studies, limiting both descriptive baselines and the conceptual frameworks that could guide policy and practice (Norris et al. 2021; Norris and Mateczun 2022; Norris, Mateczun, and Forno 2022; Hossain et al. 2024; Preis and Susskind 2022).

Local public agencies such as schools, libraries, cities, and towns are at the epicenter of the cybersecurity crisis. Between 2013 and 2019, over 169 ransomware attacks hit local governments across 48 states and the District of Columbia (Liska 2019), and ransomware attacks generally increase in frequency year-over-year (Fox-Sowell 2024).

Cyberattacks on state and local governments cause swift and severe fallout. Ransomware attacks, in particular, can disrupt city services, expose sensitive information, and cost millions of dollars to recover from (Perlroth 2019). A ransomware attack on Atlanta in 2018 forced the city to shut down many of its online services, including billing, court documents, and airport wi-fi (McKay 2018), while an attack the same week impeded Baltimore's computer-assisted dispatch system, forcing 911 call centers to handle emergency support manually (NBC News 2018). Outside of the immediate impacts, cyber-attacks can have long tailwinds; a ransomware attack on the City of Dallas in 2024 impacted police services and exposed the social security numbers and health information of over 200,000 people (Everton 2024), raising the risk of identity theft and exposing extremely sensitive information.

Small governments may seem to be infrequent targets compared to large, wealthy cities, but many small governments face additional threats due to their limited staff and reliance on technology and contractors. In 2019, the same ransomware attack affected 23 cities in Texas through a software product they used that was managed by another company (Allyn 2019). The Mayor of Keene, TX, one affected city, emphasized: "A lot of folks in Texas use providers to [manage software] because we don't have a staff big enough to have IT in-house." According to cyber experts at Mastercard (2025), "It's easy to think that [small cities] may not be a target… but the incidents we continue to see prove otherwise." Local governments face serious cybersecurity challenges, but protecting these institutions from cyberattacks is of the utmost importance to preserve critical services for communities.

Critically, the academic literature indicates we still lack a systematic account of this threat environment at the municipal tier. Comparative reviews find only a small number of peer-reviewed studies on local-government cyber incidents since 2000, and most are descriptive case narratives rather than empirically informed or cross-jurisdictional analyses (Norris et al. 2021; Norris and Mateczun 2022; Norris, Mateczun, and Forno 2022; Hossain et al. 2024). Preis and Susskind (2022) further argue that interdependencies are poorly theorized: attacks on a single city can cascade across shared networks, vendor ecosystems, or interlocal service arrangements, yet scholarship rarely models those spillovers. The absence of standardized incident reporting at the municipal level compounds the problem by limiting the construction of longitudinal datasets and hindering policy learning (Chodakowska, Kańduła, and Przybylska 2022; Norris and Mateczun 2022; Norris, Mateczun, and Forno 2022).

Despite elevated threats, the status quo favors large, for-profit organizations that have the time, talent, and resources to follow expert best practices and secure their infrastructure, while smaller and public organizations may get left behind. This fragmented approach to cybersecurity inherently benefits adversarial state actors and cybercriminal networks, who can exploit under-resourced municipalities as a weak link in the nation's digital infrastructure.

When cities and towns can invest in cybersecurity, they face an uphill battle. Talent shortages and lower government wages can impede many cities' abilities to hire IT and cybersecurity talent; According to CyberSeek's May 2024-April 2025 data update [1], U.S. employers posted approximately 514,000 cybersecurity-related job listings suggesting that over 450,000 cybersecurity jobs remain open at that time given the supply-to-demand ratio of about 74%, and in 2022, private sector jobs paid 14% more than equivalent public sector jobs (Zengler 2022). The cybersecurity product marketplace is also flooded with tools, making it difficult for cities without in-house experts to understand what they need. Over 10,000 cybersecurity products exist [2], and the average mid-market organization uses between 76 and 100 cybersecurity tools across their organization (Oracle 2020). This combination of frequent threats and low resources makes state and local governments some of the most at-risk organizations in the U.S. for cyberattacks.

The literature deepens this picture by showing that municipal cyber risk is not only about money—it is also about institutional capacity and governance. Caruson, MacManus, and McPhee (2012) documented more than a decade ago that many local officials lacked even a basic working knowledge of cyber risk, which in turn produced over-reliance on vendors and difficulty scrutinizing proposed solutions. Subsequent studies find that generalist administrators and elected officials still face a steep learning curve, widening the gap with technical staff and complicating priority-setting (Hatcher, Meares, and Heslen 2020; Frandell and Feeney 2022). Meanwhile, fragmented authority and the lack of standardized reporting or oversight

1. https://www.cyberseek.org/heatmap.html
2. https://dashboard.it-harvest.com/

at the municipal level entrench variation and hinder coordinated response (Chodakowska, Kańduła, and Przybylska 2022; Norris and Mateczun 2022). Preis and Susskind (2022) add an equity dimension: underinvestment multiplies risk because communities with the thinnest administrative and fiscal capacity are also those whose services e.g. water, EMS, schools—are most critical to daily life, and most exposed to cascading harms when compromised. Put differently, the "capacity gap" and the "governance gap" interact—resource scarcity, organizational design, and policy fragmentation jointly produce vulnerability at the local tier.

This paper extends this discussion by emphasizing the role of clinics as public-interest service providers for municipalities, nonprofits, and other under-resourced organizations. By demonstrating how clinics deliver essential capacity to actors otherwise excluded from the cybersecurity marketplace, we argue that clinics should be understood not only as workforce pipelines but also as governance mechanisms that strengthen local resilience and, by extension, national security. In this sense, clinics address both the service gaps highlighted by municipal governance literature (Preis and Susskind 2022; Norris and Mateczun 2022) and the workforce challenges identified in cybersecurity education research. Their promise lies in bridging these domains—linking education, governance, and resilience in ways that no other intervention currently does.

3 EXPANDING ON THE CYBERSECURITY CLINIC MODEL AND DESIGN

The growing cybersecurity vulnerabilities faced by local governments, nonprofits, and small businesses require scalable solutions that can rapidly expand cybersecurity capacity while training the next generation of professionals. Cybersecurity clinics address this need by providing structured, hands-on training for students while delivering real cybersecurity support to under-resourced organizations. Unlike traditional coursework, clinics immerse students in live cybersecurity environments, where they assess risks, implement security measures, and develop cyber policies that have tangible and sometimes immediate impact. Cybersecurity clinics offer a structured approach to skill-building that is both scalable and sustainable.

This section examines the pedagogical foundations of the cybersecurity clinic model. While Section 2 describes the policy and governance context, here the focus shifts to education and workforce development. Drawing on experiential learning theory and traditions of clinical education in medicine, law, social work, and engineering, we outline how cybersecurity clinics are designed to prepare students for high-stakes professional practice. The section proceeds in three parts: first, it situates clinics within experiential learning traditions; second, it identifies the distinctive features of the clinical approach; and third, it highlights how these features scale into workforce development and national resilience.

3.1 Experiential Learning and the Clinical Education Model

Clinical education is rooted in experiential learning theory, which emphasizes learning through direct engagement, reflection, and iterative practice (Kolb 1984). According to Kolb's model, students cycle through four stages: concrete experience, reflective observation, abstract conceptualization, and active experimentation (Kolb, Boyatzis, and Mainemelis 2001). This process ensures, Kolb would argue, that learning is not passive but an evolving, participatory experience where students apply theoretical knowledge to practical situations, analyze outcomes, and refine their approach (Kolb and Kolb 2005).

Cybersecurity clinics extend this framework into professional environments where decisions can carry immediate consequences. Unlike controlled classroom exercises, cybersecurity threats are evolving, requiring students to develop problem-solving skills in dynamic, high-pressure contexts. Clinical education in this setting ensures that students engage with real clients while being closely supervised by faculty and industry professionals (Susskind et al. 2024). This combination of authentic engagement and structured oversight allows students to build both confidence and competence, ensuring their recommendations are actionable and aligned with professional standards (Irby and Hamstra 2016).

Clinical education has been shown to be effective across multiple disciplines: medicine (Gruppen, Mangrulkar, and Kolars 2012), law (Chavkin 2002; Bloch 2010), social work (Fortune, Lee, and Cavazos 2005), and engineering (Tembrevilla, Phillion, and Zeadin 2024). Cybersecurity clinics represent a natural extension of this tradition, providing an applied learning framework that not only strengthens the workforce pipeline but also contributes directly to national security needs. Owusu (2023) reinforces this point by situating cybersecurity clinics within the teaching hospital tradition, highlighting their ability to integrate research, service, and education into a single model. While Owusu's study emphasizes the curricular shortcomings of traditional cybersecurity programs, our analysis underscores how clinics address these gaps through supervised, real-world practice that prepares graduates to mitigate risks, respond to incidents, and contribute to broader cyber resilience.

While sharing the general principles of experiential learning, cybersecurity clinics exhibit distinctive characteristics that differentiate them from other applied learning approaches. These include:

Hands-on practice in live settings: Students assess vulnerabilities and implement mitigation strategies for organizations that often lack internal cybersecurity expertise. This mirrors the way medical students refine diagnostic skills through clinical rotations (Issenberg et al. 2005; Gruppen, Mangrulkar, and Kolars 2012).

Direct client engagement with real stakes: Deliverables affect the resilience of municipalities, nonprofits, and small businesses. Errors or omissions have real-world consequences, reinforcing accountability (Benner et al. 2009).

Structured supervision and reflective practice: Faculty and professional mentors oversee engagements and lead post-engagement debriefs, integrating technical, ethical, and strategic considerations (Cantillon and Dornan 2014).

Competency-based assessment: Students are evaluated on demonstrated ability to deliver usable, effective security recommendations, echoing competency-based models in medical and legal education (Carraccio et al. 2002; Epstein 2007).

Collaborative and interdisciplinary learning: Teams draw from law, policy, and technical disciplines, preparing students for the cross-functional collaboration required in modern cybersecurity (Thistlethwaite 2012; Salas et al. 2012; Hammick et al. 2007).

Bertone, Wagner, and Pauli (2025) corroborate the importance of these features, showing through a systematic literature review that experiential models grounded in Kolb's cycle consistently outperform traditional lecture-based instruction in preparing job-ready graduates. They further map clinic activities—such as audits, incident response planning, and policy drafting—to the NICE Cybersecurity Workforce Framework (NIST 2023), demonstrating alignment with industry-defined roles and competencies. Our analysis builds on these findings by highlighting that clinics not only prepare students for the workforce but also strengthen the cybersecurity posture of underserved institutions, linking pedagogy directly to resilience.

3.2 Cybersecurity Clinics as a Scalable Model for National Resilience: Bridging Workforce Development and Real-World Defense

Cybersecurity clinics represent more than an educational innovation; they are a scalable, field-tested model for strengthening national cyber resilience by systematically training the next generation of cybersecurity professionals while simultaneously securing vulnerable institutions. Through hands-on practice, direct client engagement, structured supervision, competency-based assessment, collaborative learning, and interdisciplinary training, these clinics address critical gaps in both workforce development and national security strategy. Studies show that hands-on services are preferred over static resources such as technology or toolkits for clientele with low resources. When asked to rank solutions that could improve their cybersecurity posture, nonprofits most commonly ranked proactive consulting services first, over both funding and technology (CLTC Berkeley 2024).

Services can provide what tools cannot: a human connection that tailors recommendations to an organization's goals, resources, and constraints. Clinics deliver services like maturity assessments, where consultants evaluate an organization's practices against standards and prioritize improvements to the most high-risk areas. Most critically, services foster a two-way relationship in which cities can ask questions and learn about cybersecurity, empowering them to advocate for longer-term improvements.

Beyond their immediate impact, clinics also demonstrate how decentralized cybersecurity units can coordinate nationally to scale impact. The growing network of cybersecurity clinics, through the consortium of cybersecurity clinics, enables universities to share best practices, standardize methodologies, and replicate successful interventions across different regions and sectors. This collaborative framework ensures that cybersecurity expertise is not siloed within elite institutions but rather expanded into communities where cyber resilience is most urgently needed.

The effectiveness of cybersecurity clinics is not just theoretical—data from existing programs demonstrates their impact in improving cybersecurity for client organizations, developing a skilled workforce, and contributing to national security efforts. The next section presents case study data from leading cybersecurity clinics, illustrating their tangible contributions to cyber resilience, the challenges they address, and the lessons they offer for expanding this model further.

4 CYBERSECURITY CLINIC AS CASE STUDIES

Cybersecurity clinics occupy an important niche in the spectrum of cyber-resilience initiatives: they embed education and public service within a single organizational model, offering a rare mechanism for rapidly bolstering the cyber defenses of under-resourced local governments, nonprofit organizations, and small businesses.

This section presents comparative case studies of three flagship programs—the MIT Cybersecurity Clinic, UC Berkeley's Citizen Clinic, and Indiana University's Cybersecurity Clinic. Each clinic emerged from a different disciplinary context, yet all translate the principles of PIT into practice. The analysis draws on program documentation, reported outcomes, and scholarly literature to show how these clinics contribute to national security by hardening local targets, building workforce capacity, and creating a distributed infrastructure for cyber-resilience. The section concludes by situating these case studies within the broader Consortium of Cybersecurity Clinics and reflecting on how clinics address the under-resourcing of local actors, the hybrid threat environment, and the challenge of power projection.

4.1 MIT Cybersecurity Clinic — Urban Cybersecurity in New England

The MIT Cybersecurity Clinic [3] was launched within the Department of Urban Studies and Planning (DUSP) as an extension of its long-standing interest in urban systems and critical infrastructure. Unlike traditional semester-long courses, MIT's clinic operates year-round in a "perpetual" or club-style format. Students complete a four-week certification module that introduces the fundamentals of cyber risk assessment and the clinic's signature methodology, "Defensive Social Engineering." After certification, students—drawn from computer science,

3. MIT Cybersecurity Clinic: https://urbancyberdefense.mit.edu/cybersecurityclinic/

engineering, and urban planning—join small teams supervised by faculty and advanced peers and work with client communities during the remaining eight to ten weeks of the semester. As of fall 2025, over 120 students have completed training and received certification. Because students can stay engaged over multiple semesters, the clinic benefits from cumulative institutional knowledge and sustained client relationships. This continuity reflects experiential learning literature, which emphasizes iterative practice and reflection as core to professional formation (Kolb 1984; Kolb and Kolb 2005).

The clinic's client roster consists principally of municipal governments, local hospitals, and other public-serving institutions in New England. These organizations often lack dedicated cybersecurity staff and struggle to identify and prioritize vulnerabilities across legacy systems. Students begin with in-depth vulnerability assessments guided by the Defensive Social Engineering framework, which emphasizes organizational behavior and low-cost interventions. Teams then produce written recommendations, including risk prioritization, policy updates, and staff training strategies. The clinic's continuity allows for follow-up engagements, enabling adjustments as organizational capacity evolves.

From an educational standpoint, the MIT clinic exemplifies a rigorous example of experiential learning: students conduct real assessments, negotiate with city managers, and draft policy documents. The faculty-supervised structure ensures accountability, addressing concerns that novice practitioners might misconfigure systems or overlook legal obligations. Engagements also foster reciprocal learning: students gain insight into the budgetary and political constraints of local governance, while municipal personnel learn to integrate risk-management principles into everyday operations.

Strategically, MIT provides a distributed rapid-response capacity. Because teams can mobilize quickly and operate year-round, the clinic effectively extends state-level cyber initiatives into local contexts. National security research underscores that adversaries exploit municipal vulnerabilities as stepping-stones into critical infrastructure. By raising the baseline of municipal cyber hygiene, the MIT clinic reduces national exposure. In this sense, MIT contributes to deterrence by denial: it deprives adversaries of easy domestic targets, thereby reinforcing the credibility of U.S. power projection (Harknett and Stever 2011).

MIT's clinic is one of the first cyber clinics and provides many critical resources to other colleges and universities developing clinics in the Consortium of Cybersecurity Clinics. For example, MIT's clinic reviewed all 108 controls in the industry-leading NIST Cybersecurity Framework [4] and narrowed them down to a list of just 23 controls most relevant to small organizations to use in its maturity assessments. This assessment is available for free for other consortium member universities to quickly adopt an assessment methodology.

4. https://www.nist.gov/cyberframework

The perpetual model also brings challenges. Sustained funding and coordination across semesters are essential, and maintaining continuity as students graduate or cycle out can be difficult. The faculty must ensure that institutional knowledge is not lost between cohorts, and there is a risk that higher-profile municipalities receive more consistent support than smaller or more remote towns.

4.2 UC Berkeley's Citizen Clinic — Defending Human Rights Nonprofits in the Bay Area

UC Berkeley's Citizen Clinic, launched in 2018 by the Center for Long-Term Cybersecurity (CLTC) [5], responded to escalating cyber threats against civil society organizations. Structured as a semester-long elective, the clinic recruits graduate and advanced undergraduate students from across disciplines, including information science, public policy, law, and computer science. Students begin with classroom instruction on legal frameworks, privacy principles, and threat modeling, followed by team-based client projects under faculty supervision. Unlike MIT's perpetual format, Citizen Clinic is organized as a service-learning course; its intensive semester structure supports deep engagements but constrains long-term continuity. As of fall 2025, the Citizen Clinic had supported over 230 nonprofits with their cybersecurity defenses.

Berkeley is distinctive for its focus on "politically vulnerable" nonprofits—organizations advocating for reproductive rights, LGBTQ+ communities, election integrity, and other causes frequently targeted by harassment or disinformation campaigns (Brooks 2018). Many operate on limited budgets and lack cybersecurity staff, making them especially vulnerable in the hybrid threat environment. Clinic teams conduct risk assessments of communications tools, data management, and staff anonymity practices. For example, students supporting the Women's Options Center analyzed vulnerabilities in messaging apps and browsers, producing guidelines for secure communication. Another team working with the Traverse Project crafted protocols to protect investigators from both digital and physical threats.

Beyond technical interventions, Berkeley students advise clients on legal and policy issues, such as compliance with data-protection laws or handling online harassment. They also provide cyber-hygiene workshops, translating technical practices into accessible training for staff and volunteers. This context-sensitive approach reflects the PIT ethos: effective cybersecurity requires tailoring to the social and political realities of vulnerable communities.

Pedagogically, Citizen Clinic exemplifies service learning: students apply interdisciplinary knowledge in service to real community needs. As with law and medical clinics, learning occurs through supervised practice, professional responsibility, and reflection. Scholars argue that such models bridge the gap between academic curricula and workforce expectations; Bertone, Wagner, and Pauli (2025) highlight that clinics allow students to acquire practical

5. https://cltc.berkeley.edu/program/cybersecurity-clinic/

experience often demanded for "entry-level" cybersecurity jobs, addressing the workforce mismatch.

Notably, the Citizen Clinic has concurrent undergraduate and graduate-level course offerings, where more advanced students can work with more technically mature clientele while undergraduates can learn teambuilding and communications skills. Students across both courses are often paired across majors, with a student team consisting of a few computer science and engineering majors paired with law, political science, and business students. In this way, students learn to apply their subject matter expertise and integrate their skills with other majors to create a cohesive service for clients.

From a strategic standpoint, Citizen Clinic demonstrates that civil society resilience is integral to national security. Hybrid threat campaigns increasingly target nonprofits to erode trust and polarize societies. By defending reproductive health providers and election-integrity advocates, Berkeley contributes to democratic durability—a key component of national power projection. Protecting these organizations enhances U.S. credibility abroad by showing that domestic democratic institutions are robust against adversary interference.

The clinic also faces challenges. The semester format creates difficulties in sustaining long-term client relationships. Faculty must rebuild institutional knowledge each term, and follow-up depends on whether students re-enroll. While the model excels in responsiveness and interdisciplinarity, it risks episodic engagement rather than continuous resilience.

4.3 Indiana University Cybersecurity Clinic — Rural Cybersecurity and Research in the Midwest

Indiana University's (IU) Cybersecurity Clinic [6], founded in 2019 within the Ostrom Workshop, addresses persistent under-resourcing among small and rural municipalities, private utility providers, and non-profits. Operating as a semester-long course, the clinic assembles interdisciplinary teams from law, computer science, cyber risk management, informatics, business, and policy. All participants complete the Google cybersecurity certificate before the semester, ensuring baseline competence. IU maintains partnerships with the Center for Applied Cybersecurity Research (CACR) and the REN-ISAC, linking student work with state and regional cybersecurity initiatives.

IU works extensively with small towns, counties, nonprofits, schools, and utilities in Indiana and the Midwest. These clients often lack dedicated IT departments and depend on generalist administrators. Student teams conduct governance audits, technical assessments, and compliance reviews; they draft tailored incident-response plans and train staff. One Indiana town, previously denied cyber insurance, secured coverage after IU students developed a formal incident-response plan. Another project supported HUD-funded community action agencies

6. https://cyberrisk.iu.edu/career-prep/cyberclinic.html, also see reference Indiana University (2019)

serving 60,000 low-income residents, where IU teams identified authentication vulnerabilities and recommended improvements. In contrast to the clinics at MIT and Berkeley, the IU Clinic operates on bespoke service provision for clients. This leads to significant challenges in continuity and increases the administrative load while making the course content necessarily more dynamic than static.

The IU clinic integrates technical, legal, and policy dimensions of cyber governance. Students learn to translate technical findings into actionable policies within municipal codes and procurement rules. This responds to scholarship highlighting the gap between cybersecurity curricula and the specific needs of the public sector. IU's explicit partnership with state entities positions the clinic as a local-to-state bridge, reinforcing the multi-level governance literature that emphasizes vertical integration in cyber resilience.

Strategically, IU underscores the importance of defending the "last mile" of national security: small towns and utilities that manage water, energy, and emergency services. Public administration research notes that these are frequent targets yet seldom prioritized in national strategies. By providing incident-response plans and training, IU reduces vulnerabilities that could otherwise be exploited as entry points into national systems. Alumni who pursue public-sector roles further contribute to closing the workforce gap in municipal cybersecurity.

4.4 The Consortium of Cybersecurity Clinics

The Consortium of Cybersecurity Clinics [7], formally established in May 2021, represents a coordinated effort to expand the clinic model across colleges and universities. Its purpose is to facilitate knowledge-sharing, standardize best practices, and lower barriers for new clinics to launch. In effect, it transforms decentralized, campus-based programs into components of a federated system, ensuring that universities not only train professionals but also actively contribute to national resilience.

The Consortium's origins reflect the governance gaps clinics were designed to address. UC Berkeley's Citizen Clinic, founded in 2018, pioneered a focus on nonprofits vulnerable to politically motivated cyber threats. Indiana University followed in 2019 with its clinic for local governments and utilities, explicitly tackling the cyber fragility of critical infrastructure institutions. MIT launched its program in the same period, serving municipalities and hospitals across New England amid a wave of ransomware attacks crippling local governments. By 2021, leaders from Berkeley, IU, MIT, and the University of Alabama began exploring the need for a shared forum. This initiative quickly attracted additional partners—including the University of Georgia, Rochester Institute of Technology, the R Street Institute, and the Global Cyber Alliance—culminating in the official establishment of the Consortium.

7. https://cybersecurityclinics.org/

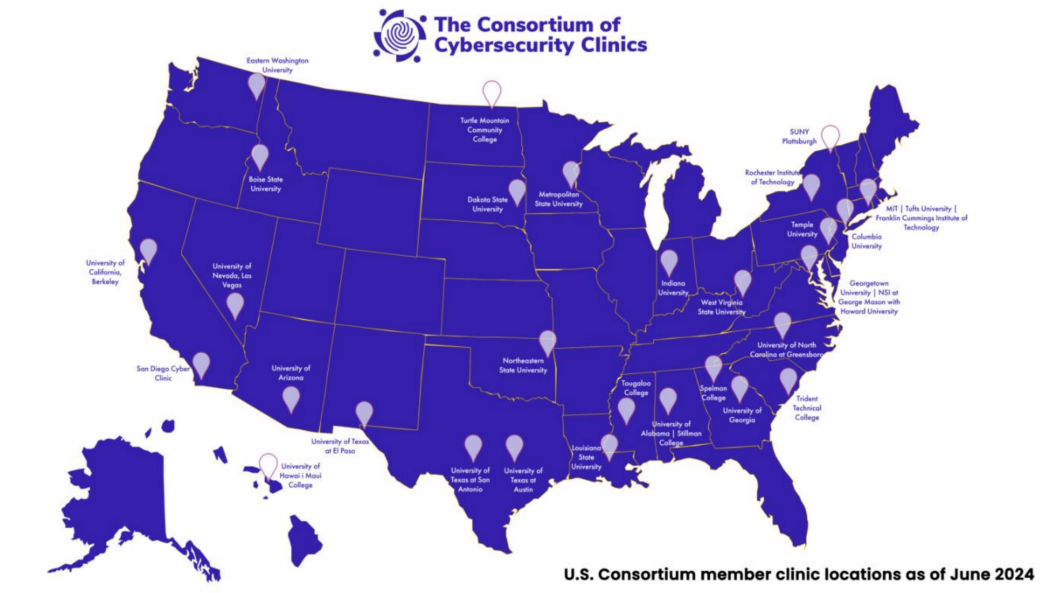


Figure 1. Map of the location of member clinics of the Consortium of Cybersecurity Clinics in June 2024

Since its formation, the Consortium has expanded rapidly. By early 2025, the Consortium's membership included 56 member clinics worldwide, with 41 member clinics in 27 U.S. states and the District of Columbia (Figure 1). The Consortium has international affiliates in Canada, Taiwan, and Indonesia. Member institutions include large research universities, small liberal arts colleges, community colleges, women's colleges, and minority-serving institutions. The reach of this network demonstrates the portability of the model across institutional types. Its collective impact is already visible: in the 2024–25 academic year alone, 2,200 students participated in clinics, providing services to over 700 organizations, including small municipalities, hospitals, and nonprofits (Nagamine and Perematko 2025). Clinics thereby serve as both training pipelines and protective infrastructures, addressing simultaneously the workforce and resilience deficits that scholars identify as central to national vulnerability (Norris and Mateczun 2022; Norris, Mateczun, and Forno 2022; Preis and Susskind 2022).

Beyond direct service, the Consortium functions as a collaborative knowledge hub. Member clinics co-develop curricula, define best practices, and refine standardized methodologies. Solutions devised in one region—such as IU's incident-response templates, Berkeley's protocols for politically vulnerable nonprofits, or MIT's "Defensive Social Engineering" framework—are shared and adapted by peers elsewhere. This networked learning process exemplifies what Ostrom (1990, 2010) describes as polycentric governance: resilience emerges not from centralized hierarchies but from multiple centers of initiative coordinated through shared norms and mutual trust. The Consortium functions as a knowledge commons, pooling experience and innovation into resources accessible across contexts, while maintaining local adaptability.

The Consortium can also be read, following Polanyi (1944), as a protective counter-movement. Commercial cybersecurity systematically underserves municipalities, nonprofits, and schools, leaving them vulnerable despite their systemic importance. Clinics, underwritten by universities and philanthropy, re-embed cybersecurity in civic institutions rather than leaving it subject to market exclusion. Google.org's $25 million commitment in 2023 [8] to expand the Consortium nationwide illustrates this protective logic: philanthropy is investing in institutions that shield vulnerable communities from systemic digital risks.

The Consortium's growth also carries international implications. Partnerships with clinics in Sri Lanka, Peru, and elsewhere demonstrate the adaptability of the model in contexts of constrained state capacity and heightened hybrid threats. These global linkages extend the PIT ethos beyond U.S. borders, reinforcing democratic resilience while contributing to U.S. soft power. The Consortium thus functions simultaneously as capacity-building infrastructure and as a signal of credibility abroad: that resilience at home is institutionalized and exportable.

Finally, the Consortium addresses the research gap identified by municipal cybersecurity scholars. Norris et al. (2021) and Hossain et al. (2024) highlight the absence of systematic, comparable data on local vulnerabilities due to underreporting and inconsistent standards. The Consortium creates conditions for comparative analysis across hundreds of engagements, enabling the accumulation of empirical knowledge that can inform both scholarship and policy. Each clinic generates situated evidence; the Consortium aggregates these into longitudinal insights, transforming practice into theory-building.

Taken together, the Consortium is more than a scaling mechanism. It represents the institutionalization of a governance innovation: redistributing expertise to underserved communities, sustaining resilience through polycentric coordination, and countering the exclusions of markets by embedding cybersecurity within civic institutions. By federating clinics into a national and international network, the Consortium embodies Ostrom's (2010) insight that robust governance arises from polycentric systems and Polanyi's claim that protective institutions emerge to safeguard society from systemic disruption. It demonstrates that cybersecurity resilience in the twenty-first century must be produced not only by states or markets, but also by federated civic institutions capable of mobilizing knowledge, talent, and legitimacy at scale.

4.5 High-Impact Interventions for Local Governments, Communities, and Critical Infrastructure Providers

The comparative analysis of MIT, Berkeley, and Indiana University indicates that cybersecurity clinics are best conceptualized not as isolated pedagogical ventures but as institutionalized responses to difficulties in the protection of local and civic infrastructure. The persistence of municipal under-resourcing and lack of institutional capacity has been documented across

8. Google.org (2023), https://cyberclinics.withgoogle.com/

decades of public administration scholarship: cities and counties routinely operate with outdated technology, minimal IT staff, and administrators with limited technical literacy (Caruson, MacManus, and McPhee 2012; Norris et al. 2021; Norris, Mateczun, and Forno 2022). More recent studies highlight the consequences of this gap, showing how ransomware attacks against municipalities cascade into service disruptions that erode public trust and generate economic loss far beyond the immediate jurisdiction (Preis and Susskind 2022; Hossain et al. 2024). Yet despite these risks, municipal cyber resilience has remained marginal in both national strategy and scholarly analysis. Clinics, therefore, represent a distinct governance innovation, intervening in precisely those spaces that state and federal agencies have struggled to reach and that private firms often ignore due to lack of profitability.

What distinguishes clinics from other interventions is the way they redistribute technical capacity into local contexts while simultaneously generating legitimacy through trusted university affiliations. MIT's perpetual structure embeds continuity into municipal engagements, creating a form of standing capacity otherwise absent at the community level. Berkeley's service-learning orientation demonstrates that the defense of civil society organizations—often excluded from critical infrastructure definitions—is a matter of national security when adversaries exploit them to polarize societies or undermine democratic legitimacy. IU's integration with state entities illustrates the possibility of vertical alignment in which clinic outputs feed directly into broader policy architectures. Taken together, the cases show that clinics do not merely tell municipal IT and administrative staff what to do but enable a virtuous capacity-building environment in which resilience is co-produced by universities, local governments, nonprofits—and through the Consortium—national networks.

This mode of distributed governance resonates with broader theoretical work on collaborative and networked governance. Ansell and Gash (2008) argue that in complex policy domains, durable solutions emerge when authority is shared across organizational boundaries and when intermediaries build trust and facilitate cooperation. Clinics occupy precisely this intermediary role. They leverage the institutional credibility of universities to convene local actors, provide a structure for collaboration, and generate both technical and normative guidance. The Consortium then scales this logic, enabling horizontal exchange of curricula, methodologies, and lessons learned. In this way, clinics enact a governance model that is adaptive, decentralized, networked, and polycentric in structure, which are attributes that scholars of cyber strategy argue are essential for resilience in adversarial environments characterized by uncertainty and speed (Deibert 2013; Nye 2019).

The implications for national security are significant. Cyber strategy debates have long emphasized the difficulty of deterrence in the digital domain, particularly against gray-zone tactics and hybrid threats where attribution is contested, and thresholds for retaliation are ambiguous (Libicki 2009; Harknett and Stever 2011). In such contexts, deterrence by denial—raising the cost and reducing the feasibility of attacks—becomes critical. Clinics

advance this form of deterrence not through centralized federal investment but by hardening local and nonprofit systems that adversaries routinely exploit. When a small town can secure cyber insurance due to an incident response plan produced by IU students, or when a human rights organization resists harassment thanks to protocols developed by Berkeley teams, the effect is not just local protection but the closure of potential attack vectors that could have been leveraged to destabilize larger networks or fuel disinformation campaigns. These micro-level interventions accumulate into macro-level resilience, shifting the calculus of adversaries who rely on exploiting precisely these vulnerabilities.

Clinics also challenge the assumption that national resilience must be primarily technical. The Berkeley case underscores that civil society is as much a target in hybrid conflicts as power grids or pipelines. By defending politically vulnerable nonprofits, clinics protect the institutions of democratic life that underpin soft power. This dimension is often overlooked in cyber strategy, which privileges critical infrastructure and military systems. Yet as Nye (2004) reminds us, credibility and legitimacy are central to international influence. The protection of advocacy organizations, election-integrity groups, and other nonprofit actors ensures that democratic societies retain both the functional capacity and moral authority necessary for global leadership. Clinics thus contribute to power projection not only by securing physical systems but also by safeguarding the societal fabric that adversaries seek to unravel.

The scaling effect of clinics through the Consortium is equally consequential. This expansion represents more than institutional proliferation; it constitutes the emergence of a distributed national cyber infrastructure. Google.org's $25 million commitment to fund clinics in every state by 2030 illustrates growing recognition of clinics as viable instruments of policy. In institutional terms, this network reduces reliance on episodic grants or ad hoc initiatives, creating a baseline of continuity that adversaries cannot easily exploit. From a governance perspective, the Consortium demonstrates the possibility of federated resilience: local contexts remain primary, but capacity is coordinated and amplified through shared standards and mutual support.

By generating data through engagements, clinics also fill a gap in the empirical foundation of scholarship. Norris and Mateczun (2022) lament the absence of systematic information on municipal cyber vulnerabilities due to underreporting and inconsistent frameworks. Clinics, by conducting hundreds of audits and incident response plans, accumulate precisely the kinds of knowledge that can inform both policy and research. Each engagement produces empirical material—patterns of vulnerabilities, recurring governance failures, effective low-cost interventions—that is otherwise inaccessible. In this sense, clinics function not only as service providers but also as laboratories of resilience, generating situated knowledge that can inform theory-building in public administration and international security alike.

The workforce implications further reinforce the governance innovation argument. Owusu (2023) positions clinics within the teaching-hospital tradition, where students learn through

practice under supervision, embedding both competence and ethos. Bertone, Wagner, and Pauli (2025) emphasize clinics as a mechanism to bridge the experience gap in cybersecurity education, where "entry-level" jobs paradoxically demand prior experience. The cases analyzed here extend these insights: clinics not only prepare students for the labor market but also orient them toward public service. IU alumni entering municipal IT, MIT students mentoring city staff, Berkeley graduates defending NGOs—these trajectories illustrate the creation of a workforce aligned with civic responsibility. From a governance standpoint, this matters because the sustainability of resilience depends not only on institutional design but on human capital willing to serve outside the highest-paying private firms. Clinics, therefore, help resolve what the literature identifies as one of the most intractable challenges of cybersecurity governance: the recruitment and retention of talent in the public sector.

Taken together, the comparative analysis suggests that cybersecurity clinics represent a governance innovation with profound implications for both domestic resilience and international power projection. They redistribute capacity into vulnerable nodes ignored by markets and underserved by states. They enact distributed, networked governance models that scholars argue are essential in complex, uncertain domains. They advance deterrence by denial by closing off easy avenues of attack at the municipal and nonprofit levels. They protect not only infrastructure but the democratic institutions that constitute soft power. They scale nationally through the Consortium, forming a federated infrastructure of resilience. They cultivate a workforce oriented toward civic protection, addressing long-standing gaps in public sector capacity.

In this sense, cybersecurity clinics demonstrate that national security in the digital age cannot be reduced to either federal agencies or private firms. Instead, resilience must be understood as a distributed function produced by multi-level, cross-sectoral collaboration. Clinics exemplify how public-interest technology can serve as both an educational model and a security innovation, weaving together pedagogy, service, and governance into an adaptive infrastructure of resilience.

5 CONCLUSION: POLICY PATHWAYS FOR SCALING CYBERSECURITY CLINICS

Cybersecurity clinics have demonstrated their value in strengthening digital resilience, providing hands-on training for students, and bridging the cybersecurity gap for under-resourced organizations. The case studies of the MIT, UC Berkeley, and Indiana University cybersecurity clinics illustrate how clinics operate as scalable, workforce-driven interventions that address both local and national security concerns. However, realizing the full potential of these clinics requires strategic policy support to sustain and expand their impact.

One of the most effective ways to scale cybersecurity clinics is through federal and state investment in workforce development initiatives that integrate clinics into the broader national cybersecurity strategy. Expanding programs like Congressionally-funded State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP) can give states much-needed funds to invest in their universities, both to maintain existing clinics and to start up new clinics in regions without any. Creating a new Cyber Peace Corps could institutionalize these efforts, embedding cybersecurity clinics within national service programs that provide structured funding, mentorship, and long-term client support. Drawing lessons from the U.S. Digital Service, policymakers could develop mechanisms that place trained cybersecurity students into public sector roles, strengthening municipal and state cybersecurity defenses while simultaneously building a pipeline of skilled professionals.

Beyond federal initiatives, states and municipalities can play a key role in supporting cybersecurity clinics by forming regional consortia that connect universities, community colleges, local governments, and nonprofit organizations. Cybersecurity threats are not confined by jurisdiction, and a clustered approach—where institutions collaborate to share best practices, standardize training, and establish sustainable funding models—can help scale the clinic model beyond individual universities. Public-private partnerships, particularly with industry stakeholders invested in national cybersecurity, can further expand these efforts by funding clinics, providing professional mentorship, and creating pathways for students into the workforce.

Additionally, integrating cybersecurity clinics into existing grant programs and workforce funding streams would provide long-term financial sustainability. Agencies such as CISA [9] and NIST [10] could establish dedicated funding for university-affiliated cybersecurity clinics, ensuring their integration into national cybersecurity resilience plans. This could include grants for faculty mentorship, student stipends, and infrastructure investments that allow clinics to expand their services to more communities. The U.S. National Science Foundation (NSF) CyberCorps Program could be used to encourage the creation and spread of cybersecurity clinics to provide more hands-on training for future public-sector cybersecurity professionals.

Ultimately, cybersecurity clinics offer a unique opportunity to shape public policy research and innovation. By engaging in applied cybersecurity work, clinics generate real-time insights into emerging threats, regulatory gaps, and the challenges faced by local governments and nonprofits. Establishing mechanisms to translate these insights into policy recommendations—such as formal partnerships between cybersecurity clinics and government advisory boards—could improve national cybersecurity policymaking and regulatory frameworks.

Cybersecurity is an area of increasing strategic importance, and bipartisan consensus exists around the need to strengthen national defenses. Cybersecurity clinics represent a proven,

9. CISA - Cybersecurity and Infrastructure Security Agency, https://www.cisa.gov/
10. NIST - National Institute of Standards and Technology, https://www.nist.gov/

scalable, and interdisciplinary model for addressing this challenge. By implementing policies that institutionalize, fund, and integrate clinics into the national cybersecurity strategy, the U.S. can enhance its cyber workforce, protect critical infrastructure, and extend digital resilience to the communities that need it most.

ABOUT THE AUTHORS

Isak Nti Asare is Assistant Dean for Undergraduate Education at the Hamilton Lugar School of Global and International Studies at Indiana University-Bloomington. He also serves as the Executive Director of the University's Cybersecurity Clinic, the co-director of the Cybersecurity and Global Policy Program, and faculty lead for the Hacking for Defense (H4D) program. His work sits at the intersection of cybersecurity, artificial intelligence, and public-sector innovation. His applied research and innovation portfolio includes more than 140 mission-driven projects with the U.S. Department of Defense, the Department of State, international organizations, critical infrastructure providers, and municipalities.

Scott J. Shackelford is Associate Vice President and Vice Chancellor for Research at Indiana University-Bloomington. He is also the Provost Professor of Business Law and Ethics at the Indiana University Kelley School of Business. Professor Shackelford has written more than 100 articles, book chapters, essays, and op-eds for diverse publications, and his research has been covered by an array of outlets, including Politico, NPR, CNN, Forbes, Time, the Washington Post, and the LA Times. Both Professor Shackelford's academic work and teaching have been recognized with numerous awards, including a Harvard University Research Fellowship, a Stanford University Hoover Institution National Fellowship, a Notre Dame Institute for Advanced Study Distinguished Fellowship, the 2014 Indiana University Outstanding Junior Faculty Award, the 2015 Elinor Ostrom Award, and the 2022 Poets & Quants Best 40-Under-40 MBA Professors Award.

Jungwoo Chun is an applied social scientist with expertise in public policy and planning. He is a Lecturer in Climate, Sustainability, and Negotiation at the Department of Urban Studies and Planning (DUSP) at the Massachusetts Institute of Technology (MIT). He co-directs the MIT Cybersecurity Clinic, supported by the Google Cybersecurity Clinics Fund, and the MIT Renewable Energy Clinic, initially funded by the Preston Werner Foundation. Additionally, he serves as the Assistant Director of the MIT Science Impact Collaborative (SIC), where he promotes research, teaching, and public service focused on managing public interest technology (PIT).

Sarah Powazek is the Program Director of Public Interest Cybersecurity at the UC Berkeley Center for Long-Term Cybersecurity (CLTC), where she leads flagship research on defending low-resource organizations like nonprofits, municipalities, and schools from cyber attacks. She serves as Co-Chair of the Cyber Resilience Corps, a network of cybersecurity volunteer organizations, and as Senior Advisor for the Consortium of Cybersecurity Clinics, advocating for the expansion of clinical cyber education around the world. Sarah hosts the Cyber Civil Defense Summit, an annual mission-based gathering of cyber defenders to protect the nation's most vulnerable public infrastructure. Sarah previously worked at CrowdStrike Strategic Advisory Services, and as the Program Manager of the Ransomware Task Force at the Institute for Security and Technology.

ACKNOWLEDGMENTS

This project would not have been possible without the invaluable research support of several stellar students, including Jane Allen, Madelyn Gamble, and Tanner Wilburn. It was funded in part by the U.S. Army Cyber Institute and Google.org. Special thanks to our colleagues across the Consortium of Cybersecurity Clinics for contributing to this project.

REFERENCES

Allyn, Bobby. 2019. "23 Texas Towns Hit with Ransomware Attack in New Front of Cyberassault," August 20, 2019. https://www.npr.org/2019/08/20/752695554/23-texas-towns-hit-with-ransomware-attack-in-new-front-of-cyberassault.

Ansell, Chris, and Alison Gash. 2008. "Collaborative Governance in Theory and Practice." *Journal of Public Administration Research and Theory* 18 (4): 543–571. https://doi.org/10.1093/jopart/mum032.

Beerman, Jack, David Berent, Zach Falter, and Suman Bhunia. 2023. "A Review of Colonial Pipeline Ransomware Attack." In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW),* 8–15. IEEE. https://doi.org/10.1109/CCGridW59191.2023.00017.

Benner, Patricia, Molly Sutphen, Victoria Leonard, and Lisa Day. 2009. *Educating Nurses: A Call for Radical Transformation.* Vol. 15. John Wiley & Sons.

CLTC Berkeley (UC Berkeley Center for Long-Term Cybersecurity). 2024. *CyberCAN: Cybersecurity for Cities and Nonprofits.* Berkeley Center for Long-Term Cybersecurity. https://cltc.berkeley.edu/publication/cybercan-cybersecurity-for-cities-and-nonprofits/.

Bertone, Benjamin, Patrick Wagner, and Julia Pauli. 2025. "Experiential Learning: Innovative Approaches to Post-Secondary Cybersecurity Education." *Journal of Cybersecurity Education, Research and Practice* 2025 (1): 15.

Bloch, Frank S. 2010. *The Global Clinical Movement: Educating Lawyers for Social Justice.* Oxford: Oxford University Press.

Borghard, Erica D., and Shawn W. Lonergan. 2017. "The Logic of Coercion in Cyberspace." *Security Studies* 26 (3): 452–481. https://doi.org/10.1080/09636412.2017.1306396.

Brooks, Sean. 2018. *Defending Politically Vulnerable Organizations Online.* Center for Long-Term Cybersecurity, University of California, Berkeley. White Paper. https://cltc.berkeley.edu/publication/defending-politically-vulnerable-organizations-online/.

Cantillon, Peter, and Tim Dornan. 2014. "Who Needs Beds?" *Perspectives on Medical Education* 3:399–400. https://doi.org/10.1007/s40037-014-0146-8.

Carraccio, Carol, Susan D. Wolfsthal, Robert Englander, K. Ferentz, and C. Martin. 2002. "Shifting Paradigms: From Flexner to Competencies." *Academic Medicine* 77 (5): 361–367. https://doi.org/10.1097/00001888-200205000-00003.

Caruson, Kelli, Susan A. MacManus, and Brian D. McPhee. 2012. "Cybersecurity Policy-Making at the Local Government Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success." *Journal of Homeland Security and Emergency Management* 9 (2): 20120003. https://doi.org/10.1515/jhsem-2012-0003.

Chavkin, David F. 2002. *Clinical Legal Education: A Textbook for Law School Clinical Programs.* New York: LexisNexis.

Chodakowska, Aneta, Sławomira Kańduła, and Joanna Przybylska. 2022. "Cybersecurity in the Local Government Sector in Poland: More Work Needs to Be Done." *Lex Localis – Journal of Local Self-Government* 20 (1): 161–192.

CISA (Cybersecurity and Infrastructure Security Agency). 2024. *Cyber Guidance for Small Businesses: A Different Kind of Cybersecurity Advice.* Cybersecurity and Infrastructure Security Agency website. https://www.cisa.gov/cyber-guidance-small-businesses.

Clarke, Richard A., and Robert K. Knake. 2019. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats.* Penguin.

Deibert, Ronald J. 2013. *Black Code: Inside the Battle for Cyberspace.* Signal.

Epstein, Ronald M. 2007. "Assessment in Medical Education." *New England Journal of Medicine* 356 (4): 387–396. https://doi.org/10.1056/NEJMra054784.

Everton, Bailey Jr. 2024. "Dallas Ransomware Attack Exposed Info for 200,000 People," July 19, 2024. https://www.govtech.com/security/dallas-ransomware-attack-exposed-info-for-200-000-people.

Fortune, Anne E., Maryann Lee, and Adriana Cavazos. 2005. "Achievement Motivation and Outcome in Social Work Field Education." *Journal of Social Work Education* 41 (1): 115–129. https://doi.org/10.5175/JSWE.2005.200300318.

Fox-Sowell, Sophia. 2024. "Ransomware, Malware, and Cyberattacks: The State of Play in 2024," January 30, 2024. https://statescoop.com/ransomware-malware-cyberattacks-cis-report-2024/.

Frandell, A., and M. Feeney. 2022. "Cybersecurity Threats in Local Government: A Sociotechnical Perspective." *The American Review of Public Administration* 52 (8): 558–572. https://doi.org/10.1177/02750740221125432.

Google.org. 2023. *A $10 Million Program to Train Students in Cybersecurity Across Europe.* Google.org. https://www.google.org/our-work/initiatives/cybersecurity/.

Gruppen, Larry D., Rajesh S. Mangrulkar, and Joseph C. Kolars. 2012. "The Promise of Competency-Based Education in the Health Professions for Improving Global Health." *Human Resources for Health* 10:43. https://doi.org/10.1186/1478-4491-10-43.

Hammick, Marilyn, D. Freeth, I. Koppel, S. Reeves, and H. Barr. 2007. "A Best Evidence Systematic Review of Interprofessional Education: BEME Guide No. 9." *Medical Teacher* 29 (8): 735–751. https://doi.org/10.1080/01421590701682576.

Harknett, Richard J., and James A. Stever. 2011. "The New Policy World of Cybersecurity." *Public Administration Review* 71 (3): 455–460. https://doi.org/10.1111/j.1540-6210.2011.02366.x.

Hatcher, William, Wesley L. Meares, and John Heslen. 2020. "The Cybersecurity of Municipalities in the United States: An Exploratory Survey of Policies and Practices." *Journal of Cyber Policy* 5 (2): 302–325. https://doi.org/10.1080/23738871.2020.1792956.

Hossain, S. T., Tan Yigitcanlar, Khoa Nguyen, and Yan Xu. 2024. "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework." *Applied Sciences* 14 (13): 5501. https://doi.org/10.3390/app14135501.

Indiana University. 2019. *First-of-its Kind Cybersecurity Clinic to Train 21st-Century Cyber Professionals.* Indiana University News. https://news.iu.edu/live/news/26157-first-of-its-kind-cybersecurity-clinic-to-train.

Irby, David M., and Stanley J. Hamstra. 2016. "Parting the Clouds: Three Professionalism Frameworks in Medical Education." *Academic Medicine* 91 (12): 1606–1611. https://doi.org/10.1097/ACM.0000000000001190.

Issenberg, S. Barry, William C. McGaghie, Emil R. Petrusa, David L. Gordon, and Rosalyn J. Scalese. 2005. "Features and Uses of High-fidelity Medical Simulations That Lead to Effective Learning: A BEME Systematic Review." *Medical Teacher* 27 (1): 10–28. https://doi.org/10.1080/01421590500046924.

Kolb, Alice Y., and David A. Kolb. 2005. "Learning Styles and Learning Spaces: Enhancing Experiential Learning in Higher Education." *Academy of Management Learning & Education* 4 (2): 193–212. https://doi.org/10.5465/amle.2005.17268566.

Kolb, David A. 1984. *Experiential Learning: Experience as the Source of Learning and Development.* Englewood Cliffs: Prentice-Hall.

Kolb, David A., Richard E. Boyatzis, and Charalampos Mainemelis. 2001. "Experiential Learning Theory: Previous Research and New Directions." In *Perspectives on Thinking, Learning, and Cognitive Styles,* edited by Robert J. Sternberg and Li-fang Zhang, 227–247. Mahwah: Lawrence Erlbaum Associates.

Libicki, Martin C. 2009. *Cyberdeterrence and Cyberwar.* RAND Corporation.

Liska, Allan. 2019. "Early Findings: Review of State and Local Government Ransomware Attacks." https://www.recordedfuture.com/blog/state-local-government-ransomware-attacks.

Mastercard. 2025. "Under Cyber Siege: How Well Are Cities Protecting Themselves?," May 20, 2025. https://www.mastercard.com/us/en/news-and-trends/perspectives/2024/under-cyber-siege-how-well-are-cities-protecting-themselves.html.

McGuinness, Tara Dawson, and Hana Schank. 2021. *Power to the Public: The Promise of Public Interest Technology.* Princeton University Press.

McKay, Tom. 2018. "Atlanta Ransomware Attack Throws City Services into Disarray," March 23, 2018. https://www.reuters.com/article/usa-georgia-cyber/atlanta-ransomware-attack-throws-city-services-into-disarray-idUSL1N1R51V9.

Nagamine, Matthew, and Nick Perematko. 2025. "Growth and Impact: Clinics Reach New Heights," October 1, 2025. https://cybersecurityclinics.org/blog/growth-and-impact-clinics-reach-new-heights/.

NBC News. 2018. "Baltimore's 911 Emergency System Hit by Cyberattack," March 28, 2018. https://www.nbcnews.com/news/us-news/baltimore-s-911-emergency-system-hit-cyberattack-n860876.

NIST (National Institute of Standards and Technology). 2023. *Workforce Framework for Cybersecurity (NICE Framework), Revision 1.* NIST Special Publication 800-181r1. Gaithersburg, MD: U.S. Department of Commerce. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf.

Norris, Donald F., and Laura K. Mateczun. 2022. "Cyberattacks on Local Governments 2020: Findings from a Key Informant Survey." *Journal of Cyber Policy* 7 (3): 294–317. https://doi.org/10.1080/23738871.2023.2178319.

Norris, Donald F., Laura K. Mateczun, and Richard F. Forno. 2022. *Cybersecurity and Local Government.* Wiley-Blackwell.

Norris, Donald F., Laura K. Mateczun, Anupam Joshi, and Tim Finin. 2021. "Managing Cybersecurity at the Grassroots: Evidence from the First Nationwide Survey of Local Government Cybersecurity." *Journal of Urban Affairs* 43 (8): 1173–1195. https://doi.org/10.1080/07352166.2020.1727295.

Nye, Joseph S. 2004. *Soft Power: The Means to Success in World Politics.* New York: Public Affairs.

Nye, Joseph S. 2019. *Protecting Democracy in an Era of Cyber Information War.* Belfer Center for Science and International Affairs.

Oracle. 2020. *Cloud Threat Report 2020.* Oracle. https://www.oracle.com/security/cloud-threat-report-2020/.

Ostrom, Elinor. 1990. *Governing the Commons: The Evolution of Institutions for Collective Action.* Cambridge University Press.

Ostrom, Elinor. 2010. "Beyond Markets and States: Polycentric Governance of Complex Economic Systems." *American Economic Review* 100 (3): 641–672. https://doi.org/10.1257/aer.100.3.641.

Owusu, Samuel. 2023. "Bridging the Cybersecurity Workforce Skill Gap with Experiential Learning: The Role of Cybersecurity Clinics." PhD diss., Marymount University. https://doi.org/https://www.proquest.com/openview/e439166b65e8c7b62981aa299eb2b5a7/1.pdf.

Pattison-Gordon, J. 2024. "How Can Cities Keep Nonprofit Groups Cyber Secure?," November 19, 2024. https://www.govtech.com/security/how-can-cities-keep-nonprofit-groups-cyber-secure.

Perlroth, Nicole. 2019. "Ransomware Attacks Are Becoming More Aggressive," August 22, 2019. https://www.nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html.

Polanyi, Karl. 1944. *The Great Transformation: The Political and Economic Origins of Our Time.* New York: Farrar & Rinehart.

Preis, Benjamin, and Lawrence Susskind. 2022. "Municipal Cybersecurity: More Work Needs to Be Done." *Urban Affairs Review* 58 (2): 614–629. https://doi.org/10.1177/1078087420973760.

Salas, Eduardo, Scott I. Tannenbaum, Kurt Kraiger, and Kathryn A. Smith-Jentsch. 2012. "The Science of Training and Development in Organizations: What Matters in Practice." *Psychological Science in the Public Interest* 13 (2): 74–101. https://doi.org/10.1177/1529100612436661.

Susskind, Lawrence, Jeffrey Chun, Daniel Beron, Anika Chaudhuri, and Sarthak Paul. 2024. "A University-Based Clinical Approach to Renewable Energy Facility Siting in the United States." *Cell Reports Sustainability* 1 (1): 100002. https://doi.org/10.1016/j.crsus.2023.100002.

Tembrevilla, Gerald, André Phillion, and Melec Zeadin. 2024. "Experiential Learning in Engineering Education: A Systematic Literature Review." *Journal of Engineering Education* 113 (1): 195–218. https://doi.org/10.1002/jee.20575.

Thistlethwaite, Jill E. 2012. "Interprofessional Education: A Review of Context, Learning, and the Research Agenda." *Medical Education* 46 (1): 58–70. https://doi.org/10.1111/j.1365-2923.2011.04143.x.

World Economic Forum. 2022. *The Global Risks Report 2022, 17th Edition.* World Economic Forum. Geneva. https://www.weforum.org/reports/global-risks-report-2022.

Zengler, Evan. 2022. "The Cybersecurity Salary Gap Between Public and Private Sectors," August 30, 2022. https://www.axios.com/2022/08/30/cybersecurity-public-private-salary-gap.

Zoghbi, M. 2024. "94% of SMBs Attacked: Cybersecurity for Small Businesses in 2024," October 11, 2024. https://www.genatec.com/blog/94-of-smbs-attacked-cybersecurity-for-small-businesses-in-2024.

Received 18 March 2025; Revised 21 October 2025; Accepted 5 November 2025

WEST POINT
PRESS

https://cyberdefensereview.army.mil/