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.