Journal of Science, Technology and Social Transformation Volume 2, Issue 03, 2026

Critical Infrastructure as the New Battlefield: Cyber Warfare and the Future of National Security

John Oluwatosin Kuforiji

Ec-council University - eccu.edu Canada

Abstract

Critical infrastructure, the power grids, water systems, pipelines, financial networks, and communication backbones that keep modern societies functioning, has quietly become one of the most contested spaces in international security. This article examines how the convergence of information technology (IT) and operational technology (OT), the expansion of internet-connected industrial control systems, and the logic of grey-zone competition have turned power stations, refineries, and water utilities into de facto battlefields. Drawing on documented incidents including Stuxnet (2010), the BlackEnergy and Industroyer attacks on Ukraine's power grid (2015-2016), the Colonial Pipeline ransomware attack (2021), the Volt Typhoon pre-positioning campaign attributed to China (2023-2024), and the 2025 intrusion into a Norwegian dam control system, the article traces the evolution of critical infrastructure as a target of state and non-state cyber operations. It situates these developments within deterrence theory, arguing that models built for the nuclear age translate poorly into cyberspace because of persistent attribution problems and the blurred line between espionage and preparation for sabotage. The article further evaluates institutional responses, particularly the work of the United States Cybersecurity and Infrastructure Security Agency (CISA) and allied governments, and identifies structural weaknesses legacy technology, fragmented public-private governance, and workforce shortages that continue to leave infrastructure exposed. It concludes that national security strategy must treat resilience, rather than deterrence alone, as the central pillar of defense against this new form of warfare, and offers policy recommendations for narrowing the gap between threat and preparedness.

Keywords: critical infrastructure, cyber warfare, national security, operational technology, deterrence theory, cybersecurity policy, industrial control systems. DOI: 10.64235/9qe6a114

Introduction

In April 2025, someone sitting far from Norway quietly took control of the software running a small dam near Bremanger, in the country's west, and opened a valve for four hours before anyone noticed (Infosecurity Magazine, 2026). Nobody was hurt. No headline compared it to a missile strike. Yet security officials who later attributed the intrusion to pro-Russian hackers understood exactly what had happened: an adversary had reached across a border, through a weak password on an internet-facing control panel, and manipulated a piece of physical infrastructure as easily as flipping a switch (Infosecurity Magazine, 2026). That is the quiet, unglamorous shape of twenty-first-century warfare.

For most of human history, infrastructure — roads, dams, granaries, power stations was something armies fought over, not something they fought through. Critical infrastructure was targeted with bombs, artillery, or sabotage teams operating behind enemy lines, and its destruction was a visible, attributable act of war. That distinction has collapsed. Today, the same networks that keep water flowing, electricity

Corresponding Author: John Oluwatosin Kuforiji Ec-council University - eccu.edu Canada E-mail: Johnkuforiji@gmail.com

How to cite this article: Kuforiji JO (2026). Critical Infrastructure as the New Battlefield:

Cyber Warfare and the Future of National Security *Journal of Science, Technology and Social Transformation* 2(3), 42-50.

Source of support: Nil

Conflict of interest: None

running, and fuel moving are reachable from anywhere with an internet connection, and the actors reaching for them are just as often intelligence services, criminal syndicates, and ideologically motivated hacktivists as they are uniformed militaries (CSIS, 2025; HSToday, 2025). Infrastructure has not simply become a target in war; it has become a battlefield in its own right, one where hostilities can be conducted persistently, deniably, and below the threshold that would normally trigger a military response.

This shift matters because critical infrastructure sits at the intersection of everyday civilian life and national defense capability. A compromised power grid is not only an inconvenience for households; it is a constraint on hospitals, water treatment, financial systems, and military logistics (Congressional Research Service [CRS], 2025). A ransomware attack on a single pipeline operator can, within days, alter fuel prices and travel patterns across an entire region, as the United States discovered when the Colonial Pipeline was forced offline in May 2021 (Al Jazeera, 2021). And the discovery that a state actor has spent years quietly burrowing into the networks that control water treatment plants and transportation systems as US officials say China's Volt Typhoon operation has done reframes cybersecurity as a matter of military preparedness rather than routine IT hygiene (Lostri, 2023; TechCrunch, 2024).

This article asks three interlocking questions. First, how has the targeting of critical infrastructure by cyber means evolved from a speculative concern into a documented, recurring feature of international conflict? Second, why has infrastructure specifically rather than military networks or government databases become such an attractive target for state and non-state actors alike? Third, what does this evolution demand of national security policy, given that the deterrence frameworks inherited from the nuclear era do not map cleanly onto a domain defined by ambiguity, deniability, and civilian ownership of the targets themselves? The remainder of the article proceeds as follows: Section 2 outlines the theoretical lens of deterrence and securitization used to interpret these events; Section 3 describes the methodology; Section 4 traces the historical evolution of attacks on critical infrastructure through a series of documented case studies; Section 5 explains the structural reasons infrastructure has become the preferred battlefield; Section 6 examines the national security implications; Section 7 reviews policy and institutional responses; Section 8 identifies persistent challenges; and Section 9 offers recommendations before the conclusion in Section 10.

Theoretical Framework: Deterrence in a Deniable Domain

The dominant lens through which scholars and policymakers have tried to understand hostile activity against critical infrastructure is deterrence theory, inherited largely from Cold War nuclear strategy. Classical deterrence rests on two mechanisms: deterrence by punishment, in which an adversary is dissuaded from attacking because the expected retaliation outweighs any gain, and deterrence by denial, in which an adversary is dissuaded because the attack is unlikely to succeed in the first place (Jensen, 2012). Both mechanisms depend on a condition that cyberspace routinely denies policymakers: confident, timely attribution. Jensen (2012) notes that cyber deterrence offers more flexibility than Cold War-era deterrence, including legal remedies and resilience-based denial strategies, but this flexibility also reflects how poorly the original framework fits the domain.

Interest in cyber deterrence as a coherent academic project rose sharply after the 2007 distributed denial-of-service campaign against Estonia and peaked between 2013 and 2016, before entering a marked decline that Smeets and Soesanto (2020) describe as the field having "matured" into skepticism. Their analysis of the volume of published scholarship shows that enthusiasm for deterrence as an organizing concept has been gradually replaced by frameworks emphasizing persistent engagement and resilience the idea that because attackers cannot reliably be threatened into inaction, defenders should instead focus on continuously contesting adversary access and reducing the payoff of intrusion. A parallel critique from the Massachusetts Institute of Technology's Cyber International Relations project goes further, arguing that cyber deterrence is conceptually strained because even the most cyber-capable states are probed and breached constantly without their capabilities producing any observable deterrent effect (MIT Center for International Studies, n.d.).

A second strand of theory, developed largely within information-systems and criminology scholarship, applies deterrence at the organizational and individual level, examining whether the threat of sanctions changes the behavior of intruders and insider threats. D'Arcy and Herath (2011) reviewed decades of this literature and found the findings uneven and often contradictory, suggesting that even well-established deterrence variables from criminology translate imperfectly into digital environments. More recent scholarship applies deterrence to alliance behavior rather than individual states: Chen (2024) examines NATO's 2022 Strategic Concept, the first instance of a state alliance issuing an explicit collective cyber deterrent threat, and concludes that cyber deterrence remains too immature, and international norms too underdeveloped, to generate reliably credible threats.

Alongside deterrence, this article draws on the logic of securitization the process by which an issue is elevated from routine policy into an existential security concern requiring extraordinary measures. The language used by US officials to describe Volt Typhoon is instructive here. FBI Director Christopher Wray told Congress that Chinese hackers were positioning themselves to disrupt American infrastructure and "cause real-world harm" when Beijing decided the moment was right, while CISA Director Jen Easterly called the campaign "the defining threat of our generation" in

some accounts of the hearing (TechCrunch, 2024). Such language performs a securitizing function: it moves critical infrastructure cybersecurity out of the technical domain of network administrators and into the political domain of national defense, justifying advisories, funding, and offensive postures that would be difficult to mobilize around a purely technical framing. Taken together, deterrence and securitization provide a useful pair of lenses: deterrence explains why adversaries are not obviously dissuaded from targeting infrastructure, while securitization explains why governments have begun treating infrastructure protection as a first-order national security priority rather than a private-sector concern.

Methodology

This article uses a qualitative, document-based case study methodology. It draws on publicly available government advisories (notably joint advisories issued by CISA, the Federal Bureau of Investigation, and the National Security Agency), congressional and legislative research reports, peer-reviewed and preprint technical literature on industrial control system security, and reporting from established security and policy outlets. Eight documented incidents spanning 2010 to 2025 were selected because each is independently verified by at least one government or recognized technical authority and because, together, they represent a range of actor types (state, state-linked, and criminal), target sectors (energy, water, transportation, fuel distribution), and attack objectives (sabotage, disruption, extortion, and strategic pre-positioning). The incidents are analyzed comparatively to identify patterns in tactics, targeting logic, and consequences, which are then interpreted through the theoretical framework outlined above. This approach does not claim to be exhaustive of all cyber incidents affecting infrastructure; rather, it treats these cases as illustrative of broader structural dynamics documented across a much larger body of threat intelligence.

The Historical Evolution of Attacks on Critical Infrastructure

The idea that a cyberattack could produce physical, kinetic-style consequences was, for most of the internet's early history, treated as a theoretical worst case rather than a documented reality. That changed in 2010 with the discovery of Stuxnet, a worm that infected Windows-based engineering systems and, upon finding its way to specific programmable logic controllers, caused centrifuges at Iran's Natanz uranium enrichment facility to spin erratically until they physically failed (arXiv:2205.11783, 2022). Stuxnet is widely regarded as the first confirmed case of malicious code causing deliberate physical destruction of industrial equipment, and it demonstrated something that had previously been debated in the abstract: that a sufficiently resourced actor could reach through digital networks to break physical machinery on the other side of the world without ever deploying a soldier or a missile.

Five years later, the target shifted from a single, heavily isolated nuclear facility to a civilian power grid serving ordinary households. On December 23, 2015, attackers remotely accessed the control centers of three Ukrainian electricity distribution companies, opened breakers at roughly thirty distribution substations, and cut power to more than 225,000 customers across the Ivano-Frankivsk, Chernivtsi, and Kyiv regions for up to six hours (Park & Walstrom, 2017; arXiv:2109.03945, 2021). The intrusion began, as so many do, with a spear-phishing email that installed a variant of the BlackEnergy malware, giving attackers a foothold in corporate networks from which they eventually pivoted into the supervisory control and data acquisition (SCADA) systems governing the grid itself (arXiv:2012.11375, 2020). Analysts at the SANS Institute later described the operation as a highly coordinated, multi-stage attack that also disabled backup power at the utility offices and flooded customer service phone lines to delay detection (Bezhan, 2016; Reuters, 2016, as cited in CBC News). It was, by consensus, the first confirmed power outage caused directly by a cyberattack.

Almost exactly a year later, on December 17, 2016, a second, more automated attack struck a transmission substation north of Kyiv using malware researchers named Industroyer or CRASHOVERRIDE, which was purpose-built to speak the communication protocols used by grid control equipment and could, in principle, be adapted to attack grids well beyond Ukraine (arXiv:2208.14225, 2022). According to Andy Bochman of the Idaho National Laboratory, the recurring targeting of Ukraine's grid was intended not only to punish Ukraine but to demonstrate to other potential adversaries what Russian-linked actors were capable of doing elsewhere (arXiv:2208.14225, 2022). That demonstration effect became impossible to ignore in June 2017, when the NotPetya malware attributed to Russian military intelligence and initially spread through a compromised Ukrainian accounting software update — escaped its intended target and propagated globally, disabling shipping, logistics, pharmaceutical, and energy companies and producing an estimated ten billion dollars in global losses, making it one of the most economically destructive cyber incidents on record (arXiv:2208.14225, 2022).

The next major turning point came not from a nation-state military unit but from a criminal ransomware syndicate. On May 7, 2021, the operator of Colonial Pipeline, which carries roughly forty-five percent of the fuel consumed on the US East Coast, discovered that a criminal group known as DarkSide had gained access to its network through a single compromised password on a virtual private network account that lacked multi-factor authentication (Wikipedia, 2025). Although the intrusion primarily affected the company's billing systems rather than the operational technology

Table 1: Major Documented Cyberattacks on Critical Infrastructure, 2010–2025

Year	*Incident*	*Target Sector*	*Attributed Actor*	*Documented Impact*
2010	Stuxnet	Nuclear enrichment (Iran)	State-sponsored (widely attributed to US/Israel)	Physical destruction of centrifuges at the Natanz facility
2015	BlackEnergy 3 grid attack	Electricity distribution (Ukraine)	Russia-linked actors	~225,000 customers lost power for up to six hours
2016	Industroyer/CRASHOVERRIDE	Electricity transmission (Kyiv)	Russia-linked actors	Automated substation attack; brief citywide outage
2017	NotPetya	Global logistics, shipping, energy, banking	Russian military intelligence (GRU)	Estimated $10 billion in global losses
2021	Colonial Pipeline ransomware	Fuel pipeline (US)	DarkSide criminal syndicate	5,500-mile pipeline shut down; East Coast fuel shortages
2023–24	Volt Typhoon	Energy, water, transportation, communications (US, Guam)	China state-sponsored	Multi-year covert access; pre-positioning for disruption
2025	Norwegian dam intrusion	Water/dam control system (Norway)	Pro-Russian hackers	Valve opened remotely for approximately four hours

that physically moves fuel, Colonial shut down the entire 5,500-mile pipeline as a precaution, triggering days of fuel shortages, panic buying, and price spikes across several states (Al Jazeera, 2021). Members of Congress wrote directly to the White House National Security Advisor describing the episode not as an isolated criminal act but as a demonstration that cybersecurity had become "an economic and national security challenge" in its own right (Al Jazeera, 2021). Colonial ultimately paid DarkSide roughly 4.4 million dollars in cryptocurrency, a substantial portion of which US law enforcement later recovered (Al Jazeera, 2021).

The most consequential recent development, however, is not a single disruptive event but a slow, patient campaign of pre-positioning. Beginning in 2023, CISA, the National Security Agency, the FBI, and allied Five Eyes agencies began warning that a Chinese state-sponsored group known as Volt Typhoon had compromised the information-technology networks of critical infrastructure organizations across communications, energy, transportation, and water and wastewater sectors in the continental United States and its territories, including Guam (Lostri, 2023). By February 2024, officials disclosed that some of these intrusions had persisted for at least five years, and that the group's behavior — extensive reconnaissance combined with an absence of any data theft consistent with traditional espionage — indicated the actors were not simply spying but positioning themselves to move laterally into operational technology systems and disrupt them during a future crisis (TechCrunch, 2024). CISA Director Jen Easterly stated publicly that her agency had found and eradicated Volt Typhoon intrusions across multiple infrastructure sectors and warned that what had been discovered was "likely just the tip of the iceberg" (TechCrunch, 2024). FBI Director Christopher Wray told a congressional hearing that the campaign's evident purpose was to be positioned to disrupt the US military's ability to mobilize in the early stages of a conflict, most plausibly one connected to Taiwan (TechCrunch, 2024).

Table 1 summarizes these incidents alongside the 2025 Norwegian dam intrusion described in the introduction, illustrating both the escalating sophistication of the tactics involved and the widening range of sectors and geographies affected.

Why Critical Infrastructure Has Become the New Battlefield

Three structural forces explain why critical infrastructure, rather than purely military or governmental targets, has become the preferred terrain of contemporary cyber conflict. The first is the convergence of information technology (IT) and operational technology (OT). Industrial control systems that once operated in physical isolation the so-called "air

gap" have, over the past two decades, been progressively connected to corporate networks and, in many cases, the open internet, in pursuit of efficiency, remote monitoring, and predictive maintenance (Vanlyssel, 2024). This connectivity brings real operational benefits, but it also means that vulnerabilities long familiar in enterprise IT security weak credentials, unpatched software, poor network segmentation now have a direct pathway to systems that control physical processes such as valves, breakers, and pumps. Vanlyssel's (2024) comparative analysis of the Stuxnet and Ukraine grid attacks concludes that the specific categories of weakness exploited in those landmark incidents remain widely present in US industrial control environments today, meaning the attack surface has not meaningfully closed even as awareness of the threat has grown.

The second force is the expansion of that attack surface driven by the energy transition itself. Rob Demain, CEO of the security firm e2e-assure, has argued that critical national infrastructure and distributed energy resources represent "the new frontier in cyber warfare," noting that solar installations and the inverters that connect them to the grid are frequently deployed with minimal security controls, creating the plausible prospect of thousands of small, poorly protected devices being hijacked simultaneously to mount a large-scale denial-of-service attack against a national grid (Infosecurity Magazine, 2026). Bitsight researchers separately documented a measurable rise of approximately twelve percent in cyberattacks against internet-facing industrial control and operational technology systems in 2025 alone, a trend consistent with the proliferation of connected, distributed, and often under-secured energy assets (Infosecurity Magazine, 2026).

The third and arguably most important force is strategic: infrastructure targeting offers a form of leverage that operates below the threshold of open warfare. Analysts examining the Volt Typhoon campaign describe it as a deliberate strategy of infrastructure infiltration intended to deter US intervention in a future Taiwan conflict by demonstrating a credible capacity to disrupt American civilian life at home, without requiring any visible military buildup (Bragg, 2025). This logic sometimes referred to as grey-zone or hybrid competition is attractive precisely because it is deniable. States can maintain access to civilian infrastructure indefinitely, using it as a form of latent coercive leverage, while avoiding the clear attribution that would normally justify a military response. The same logic explains the growing role of ideologically aligned but formally non-state actors: CISA's 2025 advisory on pro-Russia hacktivist activity documented opportunistic attacks against operational technology and industrial control systems across multiple countries, providing states with a layer of plausible deniability by allowing loosely affiliated hacktivist collectives, rather than uniformed personnel, to conduct the actual intrusions (CISA et al., 2025).

National Security Implications

The consequences of infrastructure-focused cyber operations extend across at least four dimensions of national security. The first is economic security. The Colonial Pipeline shutdown demonstrated how a narrowly targeted intrusion into a single company's billing systems could cascade into regional fuel shortages, price volatility, and disrupted logistics within days, despite the fact that the operational systems moving fuel were never directly compromised (Al Jazeera, 2021). This illustrates a broader vulnerability: because critical infrastructure sectors are deeply interdependent, an attack does not need to succeed against its most hardened operational target to produce serious economic disruption; it merely needs to compromise a connected system that operators feel compelled to shut down out of caution.

The second dimension is military readiness. US officials assess that Volt Typhoon's positioning within transportation, energy, and communications networks is specifically intended to constrain the ability of the United States to project or sustain military power during a future crisis, particularly one involving Taiwan (TechCrunch, 2024). This reframes domestic infrastructure security as an issue directly coupled to force projection and alliance credibility: a state that cannot guarantee its ports, rail networks, and power grids will function during a crisis cannot fully guarantee its capacity to mobilize forces or honor security commitments abroad.

The third dimension concerns public trust and social stability. Infrastructure disruptions are unusually effective at generating public anxiety because they intrude directly into daily life fuel lines at gas stations, water advisories, and blackouts are experienced personally by millions of people simultaneously, in a way that a breach of a government database typically is not. This visibility is, from an adversary's perspective, part of the appeal: it allows a relatively contained technical intrusion to generate outsized psychological and political effects, a dynamic HSToday (2025) describes as warfare that can be "waged with a single keystroke" yet produce ripple effects across an entire population.

The fourth dimension is escalation risk. Because attribution in cyberspace is difficult and often contested, infrastructure intrusions create ambiguous situations in which a government may be uncertain whether it is facing routine espionage, criminal opportunism, or deliberate pre-positioning for wartime sabotage. Analysts examining Volt Typhoon warn that this ambiguity, combined with the erosion of an informal peacetime norm against targeting civilian infrastructure, raises the risk of what has been termed "mutually assured disruption," in which multiple states maintain latent capabilities to cripple each other's civilian systems, creating a fragile and poorly understood balance reminiscent of, but distinct from, nuclear deterrence (Bragg, 2025).

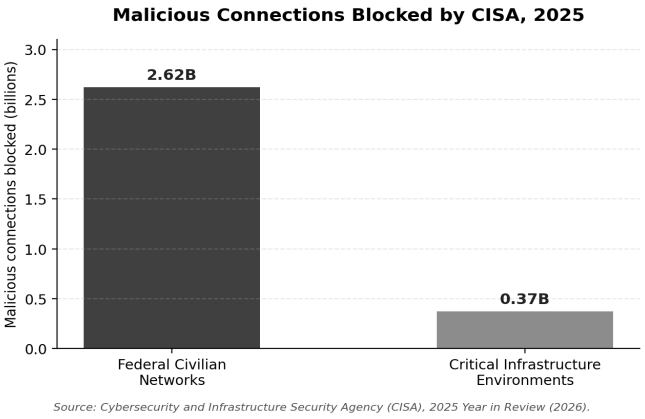


Figure 1: Malicious connections blocked by CISA across federal civilian and critical infrastructure networks in 2025 (CISA, 2026)

Policy and Institutional Responses

Government responses to these developments have concentrated most visibly in the United States around CISA, which functions as the national coordinator for critical infrastructure security and resilience. According to its own 2025 Year in Review, CISA scaled endpoint detection and response deployments to more than sixty federal agencies covering over 500,000 endpoints, blocked 2.62 billion malicious connections across federal civilian networks, and blocked a further 371 million malicious connections within critical infrastructure environments during the year (CISA, 2026). Figure 1 illustrates the scale of this defensive activity as reported by the agency.

Beyond raw defensive metrics, CISA expanded its voluntary CyberSentry monitoring program to forty-two critical infrastructure partners, released a Software Bill of Materials guide with the National Security Agency and nineteen international partners to help organizations manage software supply-chain risk, and introduced an updated set of Cross-Sector Cybersecurity Performance Goals intended to reflect current adversary tactics (CISA, 2026). The agency also worked with regional and sector-specific partners on undersea cable, space system, and information and communications technology supply-chain security, areas of growing concern as infrastructure dependencies extend beyond national borders (CISA, 2026).

At the policy level, the current US administration's cybersecurity strategy places explicit emphasis on shaping adversary behavior through a combination of offensive and defensive operations intended to erode the operating capacity of hostile actors, using the full range of instruments of national power (CSIS, 2025). CSIS analysts characterize this as a welcome signal in principle, while cautioning that its effectiveness will depend heavily on implementation, and that offensive operations and public attribution carry real diplomatic complications that must be weighed against their deterrent value (CSIS, 2025). Internationally, the same period has seen incremental movement toward collective attribution and coordinated cyber posture: NATO's 2022 Strategic Concept represented the first instance of an alliance issuing an explicit collective cyber deterrent threat, even though Chen's (2024) analysis concludes that supporting international norms remain underdeveloped.

Regulatory responses have also followed specific incidents. In the aftermath of the Colonial Pipeline attack, US authorities moved to impose new cybersecurity requirements on pipeline operators, a sector that had previously operated with comparatively light federal oversight of its cyber posture. More broadly, the Congressional Research Service notes that Congress has continued to grapple with the appropriate scope of CISA's authority and resourcing, even as the agency has faced organizational turbulence: media reporting in 2025 described a wave of senior leadership departures that observers feared could eventually affect up to a third of CISA's workforce, alongside state officials reporting diminished regional support (CRS, 2025). These tensions illustrate that institutional capacity, not merely policy intent, is now a central variable in critical infrastructure security.

Persistent Challenges

Despite this institutional activity, several structural challenges continue to limit the effectiveness of national responses. The first is attribution. Even well-resourced investigative efforts often cannot trace an intrusion back to specific individuals, and connecting hacking collectives to sponsoring governments remains difficult despite circumstantial evidence, giving hostile states plausible deniability and giving victim governments genuine pause before naming an attacker or retaliating (Park & Walstrom, 2017). This uncertainty directly undermines deterrence by punishment, since credible retaliation requires credible attribution.

The second challenge is the persistence of legacy technology. Many operational technology environments were engineered decades ago with multi-decade service lifespans and were never designed with contemporary cybersecurity threats in mind; retrofitting authentication, network segmentation, and intrusion detection onto such systems is technically difficult and operationally risky, since unlike a conventional IT system, a misconfigured patch on a control system can itself cause a physical failure (Vanlyssel, 2024). This helps explain why the same categories of vulnerability weak credentials, poor segmentation, unpatched software, insufficient monitoring recur across incidents separated by more than a decade, from Stuxnet in 2010 to the Norwegian dam intrusion in 2025.

A third challenge is the fragmented governance structure spanning public and private ownership. The overwhelming majority of critical infrastructure in market economies

is privately owned and operated, meaning that national security agencies must rely on voluntary information sharing, incentive-based regulation, and public-private partnership rather than direct control. Programs such as CyberSentry represent an attempt to bridge this gap, but their voluntary, partner-based structure means coverage remains uneven across the tens of thousands of infrastructure entities operating nationally (CISA, 2026).

A fourth challenge concerns the theoretical foundations of deterrence itself. As the review by D'Arcy and Herath (2011) and the broader assessment by Smeets and Soesanto (2020) suggest, decades of scholarship have failed to produce a settled, empirically validated model of how deterrence operates in cyberspace, leaving policymakers to act on frameworks whose real-world effectiveness remains contested. This theoretical uncertainty has practical consequences: strategies built on the assumption that visible offensive capability or the threat of retaliation will discourage infrastructure targeting may be poorly matched to adversaries who calculate that ambiguity, deniability, and the absence of an agreed international norm against targeting civilian infrastructure make the activity comparatively low-risk.

Finally, workforce capacity constrains every other element of the response. Organizational turbulence within agencies such as CISA, alongside a broader, well-documented global shortage of skilled operational technology security professionals, means that even well-designed policies and well-funded programs can be constrained by the availability of people capable of implementing them (CRS, 2025).

Policy Recommendations

Given these dynamics, this article advances five recommendations. First, national strategies should rebalance emphasis from deterrence toward resilience: because attribution and retaliation are unreliable levers, the more dependable path to security lies in reducing the payoff of intrusion through network segmentation, redundancy, and rapid recovery capability, so that even a successful intrusion produces limited disruption. Second, governments should continue extending mandatory, sector-specific minimum security baselines of the kind introduced for pipeline operators after the Colonial Pipeline attack to other critical infrastructure sectors that currently rely primarily on voluntary participation, since incidents such as Volt Typhoon demonstrate that voluntary adoption alone has not closed the gap between known best practice and operational reality.

Third, public-private information-sharing programs such as CyberSentry should be expanded and adequately resourced, with particular attention to smaller infrastructure operators who often lack the in-house expertise to detect the kind of long-dwelling, low-noise intrusions characteristic of pre-positioning campaigns. Fourth, international coordination on attribution and collective response, of the kind reflected in NATO's 2022 Strategic Concept and the multi-country advisories issued jointly by Five Eyes governments, should be deepened, since coordinated attribution among allies reduces the diplomatic and political cost borne by any single government that names an attacker. Fifth, sustained investment in workforce development for operational technology security is required, given that institutional capacity not merely funding or policy design increasingly appears to be the binding constraint on implementation, as illustrated by reported staffing turbulence within CISA itself (CRS, 2025).

Conclusion

The evidence assembled in this article points to a consistent and troubling pattern: critical infrastructure has moved from the periphery of security thinking to its center, not because policymakers chose this shift but because adversaries recognized, earlier than most defenders, that the systems ordinary people depend on every day are also among the most consequential and least defended targets available to them. From Stuxnet's physical destruction of centrifuges to the patient, multi-year positioning documented in the Volt Typhoon campaign, and from a targeted ransomware extortion against a single pipeline company to an opportunistic intrusion into a small Norwegian dam, the throughline is the same: infrastructure offers attackers outsized strategic and psychological leverage relative to the resources required to compromise it. Deterrence theory, built for a bipolar nuclear standoff between identifiable state actors, offers only partial guidance in a domain defined by ambiguous attribution and a wide range of state, state-linked, and criminal actors. What emerges instead is a security environment in which resilience the capacity to detect, contain, and recover from intrusion matters more than the threat of retaliation, and in which sustained institutional investment, rather than any single policy instrument, will determine whether critical infrastructure remains a viable battlefield for adversaries or becomes, through deliberate hardening, a far less attractive one. The stakes of getting this right are not abstract: they are measured in the number of hours a hospital keeps power, the reliability of the water coming out of a tap, and the speed with which a nation can respond when a valve, somewhere, is turned by a hand it never saw.

References

[1] Al Jazeera. (2021, June 7). US recovers most of $4.4M crypto ransom paid by Colonial Pipeline. https://www.aljazeera.com/economy/2021/6/7/us-recovers-most-of-4-4m-crypto-ransom-paid-by-colonial-pipeline

[2] Bezhan, F. (2016, January 5). Cyberattack on Ukrainian power grid looks to some like an apocalyptic first. Radio Free Europe/Radio Liberty.

[3] Bragg, B. (2025). QUICKLOOK: Volt Typhoon unveiled: China's cyber strategy for strategic disruption. https://bobbragg.substack.com/p/quicklook-volt-typhoon-unveiled-chinas

[4] Center for Strategic and International Studies. (2025). Securing U.S. critical infrastructure against evolving cyber threats.

https://www.csis.org/blogs/strategic-technologies-blog/securing-us-critical-infrastructure-against-evolving-cyber

[5] Chen, S. (2024). Uncharted virtual territory: NATO's expansion into cyber deterrence (Undergraduate senior thesis). Princeton School of Public and International Affairs. https://dataspace.princeton.edu/handle/88435/dsp01n870zv16t

[6] Congressional Research Service. (2025). Critical infrastructure: Emerging trends and policy considerations for Congress (Report No. R48878). Library of Congress. https://www.congress.gov/crs-product/R48878

[7] Cybersecurity and Infrastructure Security Agency. (2026). CISA's 2025 Year in Review: Driving security and resilience across critical infrastructure. https://www.cisa.gov/news-events/news/cisas-2025-year-review-driving-security-and-resilience-across-critical-infrastructure

[8] Cybersecurity and Infrastructure Security Agency, Federal Bureau of Investigation, National Security Agency, Department of Energy, & Environmental Protection Agency. (2025). Pro-Russia hacktivists conduct opportunistic attacks against US and global critical infrastructure (Advisory AA25-343A). CISA. https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-343a

[9] D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. European Journal of Information Systems, 20(6), 643–658. https://doi.org/10.1057/ejis.2011.23

[10] Effectiveness of SCADA system security used within critical infrastructure. (2020). arXiv. https://arxiv.org/pdf/2012.11375

[11] Cyberattacks on energy infrastructures: Modern war weapons. (2022). arXiv. https://arxiv.org/pdf/2208.14225

[12] Smart grid: Cyber attacks, critical defense approaches, and digital twin. (2022). arXiv. https://arxiv.org/pdf/2205.11783

[13] Vulnerabilities and attacks against industrial control systems and critical infrastructures. (2021). arXiv. https://arxiv.org/pdf/2109.03945

[14] Consistent and compatible modelling of cyber intrusions and incident response demonstrated in the context of malware attacks on critical infrastructure. (2025). arXiv. https://arxiv.org/pdf/2505.16398

[15] HSToday. (2025). Rising threats to critical infrastructure in the U.S. https://www.hstoday.us/subject-matter-areas/infrastructure-security/rising-threats-to-critical-infrastructure-in-the-u-s/

[16] Moetiara, E. (2020). Risk assessment of airborne PM2. 5 exposure of forest and land fire haze to petrol-pump officers in Pekanbaru. *Acta Scientific Medical Sciences*, *4*(9), 152-157.

[17] Adekoya, A. S. (2024). Enterprise Risk Compliance Architecture in Systemically Important Banks: Integrating Stress Testing, Capital Adequacy, and FX Exposure Modeling. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, *14*(02), 66-74.

[18] Anifowose, K. (2024). Development and Validation of an HPLC-Based Analytical Method for Simultaneous Quantification of Biomarkers in Human Biological Samples. *Well Testing Journal*, *33*(S2), 788-803.

[19] Adekoya, A. S. (2023). Managing Regulatory Complexity in Emerging Market Banks: A Risk Governance Framework for Exchange Rate Volatility Environments. *ADHYAYAN: A JOURNAL OF MANAGEMENT SCIENCES*, *13*(02), 70-76.

[20] Moetiara, E. (2023). Effectiveness of Integrated Occupational Health Protection Programs During Transboundary Haze Events: A Multi-Site Evaluation in the Oil and Gas Sector. *SRMS JOURNAL OF MEDICAL SCIENCE*, *8*(02), 161-166.

[21] Infosecurity Magazine. (2026). The evolving cybersecurity challenge for critical infrastructure. https://www.infosecurity-magazine.com/news-features/cybersecurity-for-critical/

[22] Jensen, E. T. (2012). Cyber deterrence. Emory International Law Review, 26, 773–827.

[23] Lostri, E. (2023, May 25). U.S. and partners release joint cybersecurity advisory on Volt Typhoon. Lawfare. https://www.lawfaremedia.org/article/u.s.-and-partners-release-joint-cybersecurity-advisory-on-volt-typhoon

[24] Park, D., & Walstrom, M. (2017, October 11). Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks. Jackson School of International Studies, University of Washington. https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

[25] Ravikumar, V. (2025). Therapeutic Bot: Ethical Concerns in AI therapy for Neurodivergence. *J Int Scient Re Rep*.

[26] Mehta, S. (2025). Enhancing Enterprise Data Governance Maturity Through Cloud Based Data Integration Frameworks in Modern Organizations. *International Journal of Technology, Management and Humanities*, *11*(01), 59-67.

[27] Begum, S., Hassaan, A., Hussain, M. A., Mudaber, M., Jamshaid, Z. A., Niaz, S., & Jobiullah, M. I. (2025). AI-driven fraud detection in real-time financial transactions: A deep learning approach. *Well Testing Journal*, *34*, 727-748.

[28] Rehan, H., Janjua, J. I., Ali, R. A., & Khan, T. A. (2025, December). AI-Driven DNA Insights and Public Health Data Integration for Enhancing Personal Healthcare in Critical Disease Prevention. In *2025 International Conference on AI-Driven STEM Education and Learning Technologies (AISTEMEDU)* (pp. 1-6). IEEE.

[29] Ezeagwuna, D. (2025). Artificial Intelligence for IT Service Management: Developing a Framework for ROI Optimization Using Service Now and Machine Learning Technologies. *Well Testing Journal*, *34*(S4), 394-419.

[30] Rehan, H., & Janjua, J. I. (2025, October). An Intelligent Data-Driven Framework for Measuring Consumer Experience in the Digital Platforms. In *2025 IEEE International Conference on Computing (ICOCO)* (pp. 500-505). IEEE.

[31] Mehta, S. (2025). Role of Metadata Management and Data Governance in Achieving Regulatory Compliance in Enterprise Data Ecosystems. *International Journal of Technology, Management and Humanities*, *11*(02), 144-152.

[32] Begum, S. (2025). Artificial intelligence and economic resilience: A review of predictive financial modelling for post-pandemic recovery in the United States SME sector. *International Journal of Innovative Science and Research Technology*, *10*(7), 3620-3627.

[33] Ezeagwuna, D. (2026). AI-Driven Intrusion Detection Systems for Cybersecurity. *Journal of Science Technology and Social Transformation*, *2*(02), 37-51.

[34] Mukherjee, C. (2026). AI-Based Detection of Deepfakes and Misinformation on Social Media. *Euro Vantage journals of Artificial intelligence*, *3*(2), 9-30.

[35] Mehta, S. (2026). Architecting AI Governance & 'Agent-ready'data layer: Semantic Governance for Autonomous AI workflows. *Journal of Science Technology and Social Transformation*, *2*(02), 29-36.

[36] Ezeagwuna, D. (2026). Digital Transformation and Business Resilience: How Service Now-Powered Automation Improves Organizational Performance, Risk Management, and Customer Satisfaction. *Journal of Data Analysis and Critical Management*, *2*(01), 48-62.

[37] Ojuri, M. A. (2021). Evaluating Cybersecurity Patch Management through QA Performance Indicators. *International Journal of Technology, Management and Humanities*, *7*(04), 30-40.

[38] Rehan, H., Akram, W., & Khan, M. B. S. (2026, May). Leveraging Gated Recurrent Units for Real-Time Tracking of Student Engagement in Healthcare LMS using LLM Analytics. In *2026 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 1-6). IEEE.

[39] Mehta, S. (2026). From Reactive cleanup to Real-time observability: Modernizing Enterprise Data Quality for RAG pipelines. *Journal of Science Technology and Social Transformation*, *2*(01), 35-44.

[40] Jobiullah, M. I., Begum, S., Ali, M. M., Rahman, M. M., Emon, M. S. A., & Fatima, K. (2026, April). A Machine Learning-based National Startup Capital Readiness Scoring Platform: Design, Implementation, and Comparative Evaluation. In *2026 9th International Conference on Inventive Computation Technologies (ICICT)* (pp. 1893-1899). IEEE.

[41] Ezeagwuna, D. (2026). Enhancing Organizational Cyber Resilience Through the NIST Cybersecurity Framework. *International Journal of Technology, Management and Humanities*, *12*(01), 124-140.

[42] Ojuri, M. A. (2023). AI-Driven Quality Assurance for Secure Software Development Lifecycles. *International Journal of Technology, Management and Humanities*, *9*(01), 25-35.

[43] Kola, J. N. (2026, June). Secure Financial Analytics Platforms for Regulatory Compliance and Risk Management. In *2026 IEEE 18th International Conference on Computational Intelligence and Communication Networks (CICN)* (pp. 794-801). IEEE.

[44] Rehan, H., Zimmerman, Z., & Janjua, J. I. (2026, May). Optimizer-Driven Techniques for Retuning Prompts on LLM Backend with Migration across Models for Healthcare and Cyber Security Operations. In *2026 Systems and Information Engineering Design Symposium (SIEDS)* (pp. 1-6). IEEE.

[45] Kola, J. N. (2026). Enterprise Business Intelligence and Financial Analytics with a focus on Enterprise Data Architecture and Predictive Risk Integration. *Adhyayan: A Journal of Management Sciences*, *16*(01), 20-28.

[46] Begum, S., Akbar, Z., Islam, M. S., Rahman, M. A., Rahman, M. M., Hossen, B., ... & Raj, M. W. Z. (2026, February). IHPO-XGBoost for ESG Performance Prediction: A High-Accuracy Machine Learning Framework. In *2026 5th International Conference on Sentiment Analysis and Deep Learning (ICSADL)* (pp. 1558-1564). IEEE.

[47] Adepoju, S. A., & Adepoju, M. A. (2024). From Portals to Case Graphs: A Reference Architecture and Benchmark for Safety Investigation Operations with Agentic Orchestration.

[48] Ojuri, M. A. (2022). Cybersecurity Maturity Models as a QA Tool for African Telecommunication Networks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *14*(04), 155-161.

[49] Khan, H. A. (2024). DATA-DRIVEN EPIDEMIOLOGICAL MODELING USING MACHINE LEARNING FOR DISEASE SPREAD FORECASTING AND PUBLIC HEALTH DECISION SUPPORT IN THE UNITED STATES. *International Journal of Applied Mathematics*, *37*(6s), 178-192.

[50] Begum, S. (2025). AI at scale: Predictive analytics as a strategic engine for national competitiveness in US startup and small business financing. *International Journal of Progressive Research in Engineering Management and Science Development*, *2582*, 7421.

[51] Kola, J. N. (2024). Longitudinal Cohort Intelligence for Self-Insured Employer Groups: A Predictive Framework for Healthcare Cost Trajectory Modeling and Proactive Risk Intervention. *Journal of Information Systems Engineering & Management*, *10*.

[52] Mehta, S. (2024). Architecting the Hub-and-Spoke Governance Model: Balancing Centralized Guardrails with Federated Domain Agility. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *16*(04), 206-215.

[53] Ojuri, M. A. (2022). The Role of QA in Strengthening Cybersecurity for Nigeria's Digital Banking Transformation. *Well Testing Journal*, *31*(1), 214-223.

[54] Ezeagwuna, D. (2024). Enterprise Workflow Automation and Workforce Productivity: Evaluating the Economic Benefits of Service Now Adoption Across Industries. *International Journal of Technology, Management and Humanities*, *10*(04), 299-313.

[55] Kola, J. N. (2024). Longitudinal Cohort Intelligence for Self-Insured Employer Groups: A Predictive Framework for Healthcare Cost Trajectory Modeling and Proactive Risk Intervention. *Journal of Information Systems Engineering & Management*, *10*.

[56] Reuters. (2016, January 11). Cyberattack that crippled Ukrainian power grid was highly coordinated. CBC News. https://www.cbc.ca/lite/story/1.3398492

[57] Smeets, M., & Soesanto, S. (2020). Cyber deterrence is dead. Long live cyber deterrence! Council on Foreign Relations, Net Politics. https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence

[58] TechCrunch. (2024, February 7). China-backed Volt Typhoon hackers have lurked inside US critical infrastructure for 'at least five years.' https://techcrunch.com/?p=2662372

[59] Vanlyssel, J. (2024). Securing U.S. critical infrastructure: Lessons from Stuxnet and the Ukraine power grid attacks. arXiv:2510.14185. https://www.arxiv.org/pdf/2510.14185

[60] Wikipedia. (2025). Colonial Pipeline ransomware attack. https://en.wikipedia.org/wiki/Colonial_Pipeline_ransomware_attack