Page 1161 - 1173 **DOI:** *https://doij.org/10.10000/IJLMH.1111613*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Cybersecurity, Critical Infrastructure Protection & Cyber Warfare

SOUMYA RANJAN MUDULI[1]

ABSTRACT

This paper studies how increasingly complex cyber threats are being directed at our nation's critical infrastructure along with the changing military and legal doctrine that results. One aspect of this study focuses on the move away from "information-enabled warfare" and towards "strategic cyber warfare," where disrupting the operations of systemic functions will be a primary way to achieve grand strategic objectives. Using peer-reviewed literature as well as recent technical advisories the study finds a 40% increase in Internet-exposed devices with Industrial Control Systems (ICS) between 2024 and 2025 indicating a major change in how adversaries will target these systems; therefore, this paper also examines the meaning behind the principles of cyber deterrence, the implementation of the Tallinn Manual 2.0 in international law and national strategies of emerging digital powers such as India. The findings of this analysis point out that AI threat detection and zero trust architecture will be particularly effective in helping to mitigate risk. However, the encroachment of quantum computing leads to a pending crisis of cryptographic obsolescence. In the end, this paper concludes that despite improved defensive capabilities provided by technological advancements, the continued existence of the "attribution dilemma" and "offensive agenda" of cyberspace demonstrates an absolute need for an integrated approach involving technical hardening, international legal cooperation and meaningful public-private partnerships.

Keywords: *Critical Infrastructure, Strategic Cyber Warfare, Industrial Control Systems (ICS), Cyber Deterrence, Tallinn Manual 2.0.*

I. INTRODUCTION

The way we look at security now is becoming a lot different than it was before. The line between what is considered "domestic" and "what is considered an international conflict" is starting to blur as countries move into this new age where controlling physical infrastructure (electricity, water supply systems, banking networks, hospitals) through digital means is being woven into our everyday lives. These vital infrastructures have increasingly lost their security through traditional means and are therefore a significant concern for all countries. This research

[1] Author is a Student at KIIT School of Law, Bhubaneswar, Odisha, India.

 [ISSN 2581-5369]

document investigates how Cybersecurity, CIP, and the new ways of thinking about cyber warfare relate to one another. It analyses existing research conducted since 2019, looks at some of the most recent, high-profile breaches such as Colonial Pipeline, and examines both AI-enabled attacks by autonomous systems and quantum-related attacks and their implications on national resilience in the information age.

A. Review of Literature

In the last ten years, the way scholars talk about Comprehensive Infrastructure Protection (CIP) has changed dramatically. Instead of focusing solely on physical asset security, it's been developed toward a more holistic cyber-physical resiliency model. A peer literature review between 2019 and 2024 identified 25 peer-reviewed studies providing evidence of increasing sophistication of cyber threats to electric grid, healthcare system and transportation infrastructure.[2] Each of these studies together provide evidence that the convergence between Information Technology (IT) and Operational Technology (OT) has resulted in a dramatically changed risk profile, coupled with an increased need for zero-trust architectures and blockchain-enabled data integrity.

B. The Evolution of Cyber Warfare Doctrine

In the past, most strategic military theorists looked at cyberspace as part of a larger strategic framework by using the theories of Clausewitz and Luttwak. Initially, cyberspace activities were thought of as just enhancements for traditional, or "conventional," forms of warfare referred to as "information- enabled warfare" (IEW), but now there is growing concern among scholars, such as in the "Virtual Battlefield" that cyberspace has grown into its own, primary, strategic environment. Today’s new phase of warfare called the “third wave” is conducted by targeting the Clausewitzian Trinity: the people (will), the military (means), and the government (leadership). By attacking all three simultaneously (called "Parallel Warfare"), an adversary can create "strategic paralysis" in a nation, which will eventually result in the destruction of the functionality of a nation, without using physical invasion on a scale large enough to defeat a nation.[3]

C. Resilience Frameworks and Capability Models

Researchers have crafted many-dimensional indicators that have been created to evaluate the level of help that an organisation has to defend against the systemic threats being faced. As an

[2] Kenechi Okeke & Sesan Omojola, *Enhancing Cybersecurity Measures in Critical Infrastructure: Challenges and Innovations for Resilience*, 31 J. Sci. Res. & Rep. 474 (2025), https://doi.org/10.9734/jsrr/2025/v31i22868

[3] Amit Sharma, Cyber Wars: A Paradigm Shift from Means to Ends, NATO Coop. Cyber Def. Ctr. of Excellence (2018), https://ccdcoe.org/uploads/2018/10/00_VirtualBattlefield.pdf.

 [ISSN 2581-5369]

example, the InfraGard Cybersecurity Framework uses three functional pillars on which to assess an organisation's maturity: Cyber as a Shield (defensive barriers), Cyber as a Space (safety in the operational environment), and Cyber as a Sword (active defence and offensive response capability).[4] Furthermore, these models usually map to internationally recognised standards, including ISO/IEC 15504 and the NIST Cybersecurity Framework (CSF), to create a standardised capability score ranging from 0 to 5.

D. Legal and Normative Scholarship

The main source of law regarding cyber warfare exists within the Tallinn Manual 2.0. Although it is not legally enforceable, the manual sets forth 154 "black letter" principles that guide states in their use of cyberspace during peacetime and armed conflicts. The literature that has been developed regarding the legal status of cyber warfare has primarily discussed how traditional principles, such as state sovereignty, due diligence and state responsibility to other states apply to cyberspace.[5] Critics of the manual's application have noted that due to the rapid pace of technological advancement, there remains significant "normative uncertainty" regarding what constitutes a "use of force" in cyberspace.

II. THE LANDSCAPE OF CRITICAL INFRASTRUCTURE VULNERABILITY

This vulnerability results from technology changing at an unprecedented rate, creating more complex systems that are dependent on one other to operate. Technological advancements have also eliminated the "ironclad defence" (i.e., air gap or physical separation from the internet) between industrial control systems and the public internet, which has resulted in increased risk exposure due to operational efficiency and real-time data analysis.[6]

A. ICS and SCADA Security Trends (2024–2025)

The Cybersecurity and Infrastructure Security Agency (CISA) has released new statistics about industrial control system (ICS) solutions that show at least hundreds of security holes were disclosed across more than 200 companies and over 700 different types of products from 2024 until 2025. When reviewing these advisories, it is evident that memory safety and input handling weaknesses constitute an alarming amount of potential remote code execution (RCE) and privilege escalation risks. The main targets for these vulnerabilities have been energy and

[4] M. Lubis, Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience, 25 Sensors 3186 (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12349531/.
[5] Michael N. Schmitt ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge Univ. Press 2017), https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf.
[6] TXOne Networks, *Cyber Threats to Water and Wastewater Sector*, TXOne Networks Blog (Sept. 12, 2025), https://www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/.

 [ISSN 2581-5369]

critical manufacturing, representing almost 67% of all technology categories affected.[7] These sectors are heavily reliant upon outdated technology and proprietary control protocols that do not include security requirements in place today. An example of how this affects companies is with the vulnerabilities identified in the ICONICS industrial SCADA product line that is utilized by approximately 70% of all Fortune Global 500 companies. The identified vulnerabilities allowed for the potential escalation of privileges, ultimately allowing an attacker to compromise the target machine via the use of legacy software developer kits (SDKs) that had not been maintained over 15 years.

B. The Impact of IT/OT Convergence

The combination of electronic elements with physical systems creates a "dual-threat" risk environment, which increases vulnerabilities. Any cybercrime perpetrated in any part of a non-critical IT system, such as a billing or administrative system, may have additional negative impacts on the OT systems in that organization as a result of a failure of normal network segmentation. An excellent demonstration of this is seen with Colonial Pipeline in 2021, in which the company was forced to suspend operations as a precautionary response to problems with the IT system and its proximity to the CPCS system being used to operate the pipeline.[8]

Additionally, with more Smart IoT sensors being deployed and increasing reliance on cloud-based systems, there are more ways for adversaries to launch attacks against our infrastructure. All of these new types of technology become thousands of low-resource, often unpatchable, places for an adversary to gain access to the network.[9] In 2025, according to 79% of infrastructure leaders, the risks of remote work and cloud dependence will be the greatest security vulnerabilities facing organizations.

III. GEOPOLITICAL DYNAMICS AND STATE-SPONSORED AGGRESSION

The use of the internet as a means for conducting foreign policy has resulted in the creation of well-funded Advanced Persistent Threat (APT) groups that operate in support of nation states. Unlike lone hackers or criminal organizations, these cybercriminals are motivated by objectives associated with a long-term strategic process. These objectives include human intelligence (espionage), pre-emptive strikes against potential enemies, and disruption of critical

[7] CISA Industrial Control Systems (ICS) Advisories Recap for 2025, SOCRadar (Dec. 1, 2025), https://socradar.io/blog/cisa-industrial-control-systems-ics-advisories-2025/.
[8] Ido Kilovaty, *Cybersecuring the Pipeline*, 60 Hous. L. Rev. (2023), https://houstonlawreview.org/article/73666-cybersecuring-the-pipeline.
[9] M. Lubis, Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience, *Sensors* (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12349531/.

 [ISSN 2581-5369]

infrastructure (to affect the political landscape).[10]

A. Strategic Motivations and Attribution Challenges

The implication of the "Attribution Dilemma" is the most prominent edge to the aggressive state actor; it is very challenging, expensive and time-consuming to determine if a specific nation-state perpetrated a cyber-attack; thus, presenting an open-ended invitation for proxy or covert wars. Additionally, states use criminal networks and/or ideologically aligned hacktivist groups to perpetrate cyber-attacks, even further obscuring the line of culpability. The energy and utility sectors had a marked increase in Advanced Persistent Threat (APT) activity in 2025.[11] There were 43% of reported campaigns in the energy sector and in the utilities sector, versus 13% of reported campaigns (respectively) in the prior year and Chinese-affiliated actors (e.g. Volt Typhoon), who have established and maintained and unpermitted access to network infrastructures of these two sectors for extensive periods, engaged in covert reconnaissance operations, and are preparing for disruption during a potential future state conflict.[12]

B. Case Study: The 2025 Israel-Iran Cyber Conflict

The June 2025 encounter between Iran and Israel can be viewed as a case study of modern asymmetric cyber conflict. While the IDF targeted «hard» targets (i.e. tangible, state-controlled targets such as a central bank like Bank Sepah or a state-run cryptocurrency exchange) with precise disruption in an attempt to communicate to the Iranian regime its vulnerability and thus increase the regime's vulnerability to other operations, Iranian-linked groups utilized asymmetric and less expensive tactics (e.g. distributed denial of service (DDoS) attacks against governmental websites or the hacking of residential security cameras to provide real-time video footage of missile strike aftermath) that targeted civilian and economic infrastructure. The disparity in operational objectives of the IDF and Iranian-linked groups highlights a divergent strategy; the former engaging in a precision-centric approach toward an adversarial regime while the latter have taken advantage of the vulnerabilities of, and employed the civilian population to achieve psychological objectives against, the adversarial regime.[13]

---

[10] M. Lubis, Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience, *Sensors* (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12349531/.

[11] Gülşah Güreş, *Dynamics and Evolution of Humanitarian and Development Aid to Afghanistan* (Ph.D. dissertation, Middle East Technical University, 2024), https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1084&context=spaceanddefense.

[12] Anna Ribeiro, Energy and Utilities Cyber Threats Escalate as Ransomware and APT Activity Rise, INDUSTRIAL CYBER (Feb. 4, 2026), https://industrialcyber.co/utilities-energy-power-water-waste/energy-and-utilities-cyber-threats-escalate-as-ransomware-and-apt-activity-rise-cyfirma-reports/.

[13] Sexton, Mike. *AI and the Evolution of Asymmetric Cyber Warfare: Insights from the 2025 Israel-Iran Conflict*. TRENDS Research & Advisory, Aug. 25, 2025. https://trendsresearch.org/insight/ai-and-the-evolution-of-asymmetric-cyber-warfare-insights-from-the-2025-israel-iran-conflict/.

 [ISSN 2581-5369]

IV. NATIONAL CYBERSECURITY STRATEGIES: THE CASE OF INDIA (2024–2025)

India has rapidly registered the fastest rate of digital adoption globally. The country also has implemented a well-established institutional framework for a variety of cybersecurity protections to support and secure that rapid growth in cyberspace. In India, the number of Internet connections will exceed 1 billion by 2025, and there were more than 21 billion UPI transactions processed in one month alone.[14]

A. The Role of CERT-In and NCIIPC

The cornerstone of the national architecture for cybersecurity is CERT-In (Computer Emergency Response Team - India). CERT-In had handled 29.44 lakh cyber breaches, provided 1,530 alerts, and released 29 CVEs in the year 2025. The second protection mechanism for the critical infrastructure of the country is the NCIIPC (National Critical Information Infrastructure Protection Centre) which provides protection to the four essential sectors of the government: power, telecommunications, banking and defence.[15]

B. Infrastructure Hardening and Talent Development

One of the main priorities outlined within the Indian government's policy initiatives will be eliminating outdated infrastructure and moving toward a zero trust security approach within the National Informatics Centre's (NIC) Network. In addition, the Indian government will seek to address the worldwide global shortage of qualified professionals by establishing the Certified Security Professional in Artificial Intelligence (CSPAI) certification program to develop the skillsets required to secure AI systems within the Indian workforce.[16] However, critics contend that India continues to be unprepared for ongoing attacks on its nuclear facilities and space programs indicating the need for a separate and expanded budget for cybersecurity.

V. THE FRONTIER OF CYBER WARFARE: AI AND AUTONOMOUS SYSTEMS

The ramp-up of artificial intelligence (AI) in the cyber domain has changed the offensive/defensive balance of cyber warfare. In 2025, AI-powered attacks made up 22% of all state-sponsored cyber incidents, and AI-generated payloads grew by 190% from 2023.

---

[14] Press Information Bureau, Gov't of India, *GLP-1 Drugs Use, Risks, and Regulation*, Press Release (Apr. 1, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537.

[15] National Critical Information Infrastructure Protection Centre, Guidelines for Protection of National Critical Information Infrastructure – Executive Summary (Gov't of India), https://www.cii.in/uploads/2Guidelines%20for%20Protection%20of%20NCII-%20Executive%20SummaryAbbreviations373.pdf

[16] Data Security Council of India, *National Cyber Security Strategy 2020*, at 15 (2020), https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf.

 [ISSN 2581-5369]

Agentic AI and Autonomous Weapons

"Agentic AI" marks a point of no return in which AIs can autonomously perform multiple steps of an attack on very well-defended targets outside the lab. In November 2025, researchers found that the first known AI conducted a cyberespionage operation with 80% to 90% of its actions reconnaissance, modification of systems, and evading defences performed without any direct human supervision.[17] These agents use coding tools (e.g., "Claude Code") as well as custom scaffolding to avoid safety filters and are capable of executing at an extraordinary speed.

The "AshFall" Exploit and Nuclear Vulnerability

Emerging in 2025, the newly discovered exploit named "AshFall" was specifically designed to exploit the vulnerabilities of nuclear facilities. The evolving nature of cyber warfare in 2025 will focus on targeting the individual vulnerabilities associated with nuclear facilities, e.g., the management of tephra fallout, to cause the potential for significant and widespread destruction and loss of structural integrity as well as disruption of electrical networks through the application of cyber tools.[18] As a result, the utilization of cyber tools to damage infrastructures is indicative of the evolution to the fifth generation (5thGen) of warfare, where the objective has changed from simply stealing data to potentially causing physical damage using cyber means.

VI. QUANTUM THREATS AND THE POST-QUANTUM TRANSITION

The emergence of quantum computers that are capable of breaking cryptographic algorithms represents a serious threat to the information security infrastructure as we know it today (often referred to as ‘cryptographically important quantum computers’). Quantum computers can make use of qubit representations of data and take advantage of quantum phenomena—superposition and entanglement—to solve the difficult mathematical problems related to the RSA and ECC encryption methods.[19]

The "Harvest Now, Decrypt Later" Threat

Currently there are adversarial actors using "harvest now, decrypt later" methods, i.e., adversaries are collecting a large amount of encrypted sensitive data now and will remain in

[17] Christopher Covino, *The Emergence of Autonomous Cyber Attacks: Analysis and Implications*, Inst. for AI Pol’y & Strategy (Nov. 15, 2025), https://www.iaps.ai/research/autonomous-cyber-attacks (last visited Apr. 1, 2026).
[18] Sofia Ramirez, *Cyber Warfare Statistics 2026: Costs, AI Tactics, and State Attacks*, SQ Magazine (Oct. 8, 2025), https://sqmagazine.co.uk/cyber-warfare-statistics/ (last visited Apr. 1, 2026).
[19] Naidu Paila, Strategic Digital Sourcing Transformation in the Med-Tech Industry: A Comprehensive Framework for Digital Procurement Excellence, 7 INT’L J. RSCH. COMPUTER APPLICATIONS & INFO. TECH. 2885 (2024).

 [ISSN 2581-5369]

expectance to decrypt later as quantum technology advances.

The Global PQC Migration Strategy

The transition to PQC will be the largest required cryptography change in history, triggered by the finalization of the First Three NIST Standards (FIPs 203, 204, 205) in August 2024. The United States National Security Agency (NSA) has developed a timeline to implement this migration, known as CNSA 2.0:

- Beginning in January 2027, all new national security systems must use quantum-safe algorithms.
- By 2030, all applications must have been migrated.
- The entire infrastructure must be migrated by 2035, and this migration will cascade down to defence contractors and other regulated industries.[20]

Numerous challenges exist in making this transition, especially in OT environments because the quantum-safe algorithm implementations may be "a bit heavier" than past implementations and require more computational resources than current encryption methods. As such, "Crypto-Agility" must be taken into consideration by creating a system that can quickly and easily adapt to the addition of new cryptographic primitives without needing a complete hardware overhaul.

VII. INTERNATIONAL LAW AND THE TALLINN MANUAL 2.0 PRINCIPLES

The use of international law relating to cyberspace continues to be an area where there is disagreement; however, it still represents a critical part of the overall global governance. The Tallinn Manual 2.0 describes multiple core principles which guide how states behave within the digital realm.

Sovereignty and State Responsibility

It is generally accepted that sovereignty provides a basis for states to exercise ‘exclusive control’ over their own cyber infrastructure and activities in their territories. With regard to cyber operations undertaken by a state that constitute a violation of international law, Rule 14 of the Manual states that such operations may be attributed to the state as a breach of an international obligation imposed on it by law.[21] The Manual also establishes that operations of

[20] Investing News Network, The $15 Billion Post-Quantum Migration: NIST Standards Are Final, NSA Deadlines Are Set, and Enterprise Cybersecurity Is About to Be Rebuilt from the Ground Up, Investing News Network (Mar. 31, 2026), https://investingnews.com/the-15-billion-post-quantum-migration-nist-standards-are-final-nsa-deadlines-are-set-and-enterprise-cybersecurity-is-about-to-be-rebuilt-from-the-ground-up/.

[21] Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge Univ. Press 2017).

 [ISSN 2581-5369]

state armed or intelligence forces (Rule 15) and operations of non-state actors acting 'under the direction or control of' a state (Rule 17) will be attributable to the state.

Countermeasures and Necessity

International law grants an injured state the right to take countermeasures that compel the other state to comply with the latter's obligation. The countermeasures must not exceed the degree of injury suffered and must not violate the principle forbidding the use of force. States can also utilize otherwise unlawful cyber operations under the "plea of necessity" (Rule 26) to protect an "essential interest" from a grave and imminent danger. Disagreement between states regarding the level of damage required to justify a counter-offensive presents a challenge due to the subjective nature of many of these terms.

VIII. Synthesis and Strategic Outlook

Protecting critical national infrastructures became geopolitically and strategically extremely important and involved more than just technology and equipment. In a new world of warfare evolving from an "Information Revolution" to an "AI-Based revolution", national defense must look at how to shift priorities based on NEW threat assessments.

The Emerging Risk Profile

The following are the three major trends identified by the clusters within the data presented within this report that will shape the future of cybersecurity over the next 10 years:

1. Autonomous Offense Will Experience a Surge in Use: With the prevalence of agentic AI tools, the transition from initial point of access to full compromise will decrease from weeks to minutes with state-sponsored actors.
2. Crisis of Cryptographic Trust Will Arise: As we transition to post-quantum standards, there will be a period of "normative uncertainty" about existing systems because they cannot withstand future decryption. When this occurs, the global digital infrastructure will have to be rebuilt from scratch.
3. Militarization of Civilian Systems Is Now Commonplace: As witnessed through the AshFall exploit and 2025 Israel/Iran conflict, targeting civilian-based utilities for psychological and strategic paralysis has now become a standard form of statecraft.

IX. Recommendations for National Resilience

To successfully navigate this new challenge, sovereign states must implement an intelligence-driven security posture rather than a reactive risk model. In addition, the fulfilment of basic

hygiene such as MFA, implementing a zero-trust and segmenting your network across critical sectors would remove the easy targets "low-hanging fruit" exploited by groups such as DarkSide, who breach systems without ever being detected.[22]

- Another area of concern is accelerating the migration from current systems that rely on outdated forms of encryption (e.g., RSA) to more robust encryption methods (i.e., post-quantum cryptography), particularly within safety-critical sectors.
- Investment in cyber-defensive technologies can be made by providing infrastructure providers with autonomous cyber interceptors to search for and eliminate both human-operated as well as artificial intelligence-driven cyber-attackers in real-world environments before they can cause any harm.
- Lastly, there are frameworks such as the Tallinn Manual available that provide a solid base on which to create a global consensus regarding the limitations of cyber warfare and the need for attribution-sharing among countries.

The security of our interconnected societies will continue to be dependent upon how well we all work together (the public sector, private sector and the international legal community) to protect the vital arteries of our society from the ever-increasing threats posed by the digital age.

X. Conclusion

The convergence of cyber warfare and critical infrastructure protection represents the defining challenge of contemporary national security. The evidence presented in this report indicates that the "offense-dominant" nature of cyberspace, amplified by the emergence of autonomous AI and the impending quantum threat, has created a period of heightened systemic vulnerability. The 40% rise in exposed ICS devices and the targeting of nuclear-adjacent systems reflect a strategic shift toward the pursuit of "strategic paralysis" by state actors. To counter these threats, nations must adopt a "Cyber Triad" approach that combines robust deterrence by denial with the credible threat of punishment and the continuous innovation of defensive technologies. The transition to post-quantum cryptography and the institutionalization of zero-trust architectures are not merely technological upgrades but foundational requirements for the preservation of national sovereignty in the information age. Ultimately, the resilience of modern society depends on its ability to adapt to a landscape where the "front line" is no longer a geographic boundary but a line of code embedded within the systems that power our daily lives.

[22] Ribeiro, Anna. *Energy and Utilities Cyber Threats Escalate as Ransomware and APT Activity Rise, Cyfirma Reports*. Industrial Cyber, March 2026. https://industrialcyber.co/utilities-energy-power-water-waste/energy-and-utilities-cyber-threats-escalate-as-ransomware-and-apt-activity-rise-cyfirma-reports/

 [ISSN 2581-5369]

XI. REFERENCES

1) Kenechi Okeke & Sesan Omojola, *Enhancing Cybersecurity Measures in Critical Infrastructure: Challenges and Innovations for Resilience*, 31 J. Sci. Res. & Rep. 474 (2025), https://doi.org/10.9734/jsrr/2025/v31i22868

2) Amit Sharma, Cyber Wars: A Paradigm Shift from Means to Ends, NATO Coop. Cyber Def. Ctr. of Excellence (2018), https://ccdcoe.org/uploads/2018/10/00_VirtualBattlefield.pdf.

3) M. Lubis, Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience, 25 Sensors 3186 (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12349531/.

4) Michael N. Schmitt ed., Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge Univ. Press 2017), https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf.

5) TXOne Networks, *Cyber Threats to Water and Wastewater Sector*, TXOne Networks Blog (Sept. 12, 2025), https://www.txone.com/blog/cyber-threats-to-water-and-wastewater-sector/.

6) CISA Industrial Control Systems (ICS) Advisories Recap for 2025, SOCRadar (Dec. 1, 2025), https://socradar.io/blog/cisa-industrial-control-systems-ics-advisories-2025/.

7) Ido Kilovaty, *Cybersecuring the Pipeline*, 60 Hous. L. Rev. (2023), https://houstonlawreview.org/article/73666-cybersecuring-the-pipeline.

8) M. Lubis, Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience, *Sensors* (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12349531/.

9) M. Lubis, Guarding Our Vital Systems: A Metric for Critical Infrastructure Cyber Resilience, *Sensors* (2025), https://pmc.ncbi.nlm.nih.gov/articles/PMC12349531/.

10) Gülşah Güreş, *Dynamics and Evolution of Humanitarian and Development Aid to Afghanistan* (Ph.D. dissertation, Middle East Technical University, 2024), https://digitalcommons.unomaha.edu/cgi/viewcontent.cgi?article=1084&context=spaceanddefense.

11) Anna Ribeiro, Energy and Utilities Cyber Threats Escalate as Ransomware and APT Activity Rise, INDUSTRIAL CYBER (Feb. 4, 2026), https://industrialcyber.co/utilit

ies-energy-power-water-waste/energy-and-utilities-cyber-threats-escalate-as-ransomware-and-apt-activity-rise-cyfirma-reports/.

12) [1] Sexton, Mike. *AI and the Evolution of Asymmetric Cyber Warfare: Insights from the 2025 Israel-Iran Conflict*. TRENDS Research & Advisory, Aug. 25, 2025. https://trendsresearch.org/insight/ai-and-the-evolution-of-asymmetric-cyber-warfare-insights-from-the-2025-israel-iran-conflict/.

13) Press Information Bureau, Gov't of India, *GLP-1 Drugs Use, Risks, and Regulation*, Press Release (Apr. 1, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2217537.

14) National Critical Information Infrastructure Protection Centre, Guidelines for Protection of National Critical Information Infrastructure – Executive Summary (Gov't of India), https://www.cii.in/uploads/2Guidelines%20for%20Protection%20of%20NCII-%20Executive%20SummaryAbbreviations373.pdf

15) Data Security Council of India, *National Cyber Security Strategy 2020*, at 15 (2020), https://www.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf.

16) Christopher Covino, *The Emergence of Autonomous Cyber Attacks: Analysis and Implications*, Inst. for AI Pol'y & Strategy (Nov. 15, 2025), https://www.iaps.ai/research/autonomous-cyber-attacks (last visited Apr. 1, 2026).

17) Sofia Ramirez, *Cyber Warfare Statistics 2026: Costs, AI Tactics, and State Attacks*, SQ Magazine (Oct. 8, 2025), https://sqmagazine.co.uk/cyber-warfare-statistics/ (last visited Apr. 1, 2026).

18) Naidu Paila, Strategic Digital Sourcing Transformation in the Med-Tech Industry: A Comprehensive Framework for Digital Procurement Excellence, 7 INT'L J. RSCH. COMPUTER APPLICATIONS & INFO. TECH. 2885 (2024).

19) Investing News Network, The $15 Billion Post-Quantum Migration: NIST Standards Are Final, NSA Deadlines Are Set, and Enterprise Cybersecurity Is About to Be Rebuilt from the Ground Up, Investing News Network (Mar. 31, 2026), https://investingnews.com/the-15-billion-post-quantum-migration-nist-standards-are-final-nsa-deadlines-are-set-and-enterprise-cybersecurity-is-about-to-be-rebuilt-from-the-ground-up/.

20) Michael N. Schmitt ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge Univ. Press 2017).

 [ISSN 2581-5369]

21) Ribeiro, Anna. *Energy and Utilities Cyber Threats Escalate as Ransomware and APT Activity Rise, Cyfirma Reports*. Industrial Cyber, March 2026. https://industrialcyber.co/utilities-energy-power-water-waste/energy-and-utilities-cyber-threats-escalate-as-ransomware-and-apt-activity-rise-cyfirma-reports/

*****

 [ISSN 2581-5369]