Strategic Threat Analysis & Cyber Resilience in National Critical Infrastructure

Course: Advanced Cyberwarfare Programme

Course Code: ACW804 - Cyber Warfare in Critical Infrastructure

Date: May 21, 2025

Version 1.0

Table of Content

1. Executive Summary

This report analyzes the evolving cyber threat landscape targeting national critical infrastructure (CI) and proposes strategies to enhance resilience. Critical infrastructure sectors, including energy, water, healthcare, and finance, are increasingly the **primary targets for sophisticated cyberattacks** by nation-state actors and advanced persistent threats (APTs). Actors like China pose a significant threat, with their capabilities consolidated under entities like the People's Liberation Army Strategic Support Force (PLASSF), viewing cyberspace as a strategic commanding height. Recent real-world incidents, such as those affecting energy grids and healthcare systems, highlight the **vulnerability of CI to disruption**, economic losses, and potential life-safety issues. Analysis of attacks like Stuxnet demonstrates the capability of cyber weapons to cause physical damage, marking a significant shift in offensive operations. These incidents underscore that attackers employ sophisticated, often low-noise and fileless techniques to achieve objectives.

Current traditional security measures are proving inadequate against these evolving threats, necessitating a **paradigm shift towards more robust defense strategies**. Key recommendations for enhancing national resilience include adopting **Zero Trust frameworks**, which emphasize continuous verification, least privilege, and microsegmentation to contain breaches. Implementing **proactive risk management and threat intelligence** capabilities is crucial for identifying emerging vulnerabilities and understanding attacker methodologies. Enhanced technical controls such as behavioral monitoring, strong access controls, and network segmentation are essential. While AI holds promise for improving threat detection and automated response, challenges like adversarial AI and data privacy must be addressed. Protecting CI requires **close collaboration among government, the private sector, and Computer Emergency Readiness Teams (CERTs)**.

In conclusion, safeguarding critical infrastructure from increasingly sophisticated cyber warfare necessitates a strategic, multi-layered approach. Implementing modern security frameworks like Zero Trust, investing in advanced threat intelligence and detection, and fostering strong cross-sector collaboration are **critical steps to bolster national cyber resilience** and counter the evolving digital threats to vital sectors.

2. Intelligence Brief & Literature Review

2.1: Cyber Warfare in the context of Critical Infrastructure

Critical infrastructure (CI) encompasses vital sectors such as energy grids, water systems, healthcare networks, transportation, and financial systems. Cyber warfare, in the context of critical infrastructure, involves hostile acts using computer networks or systems to achieve political or national security objectives. It is often described as operations undertaken by nation-state actors and advanced persistent threats (APTs). Unlike traditional malware focused on espionage or financial gain, cyber warfare operations can be specifically engineered to target industrial control systems (ICS) or operational technology (OT). The objective is typically to disrupt, spy on, or degrade these vital sectors, with the potential to cause severe, even physical, damage.

Cyber operations are considered "attacks" under international humanitarian law when they are "acts of violence against the adversary", and the targeting of critical infrastructures has always been a key concern for states in cybersecurity discussions. The severity of a cyber operation, its scale and effects (including incapacitating critical infrastructures), and the specific intent of the operating state's leadership can determine whether it constitutes an "armed attack" triggering the right to self-defense under the UN Charter. However, establishing clear legal definitions and thresholds for cyber warfare remains a challenge internationally. The European Union Agency for Cybersecurity (ENISA) highlighted the paradigm shift introduced by cyber weapons like Stuxnet, emphasizing the need for enhanced protection of critical information infrastructure.

2.2 Historical and Recent Cyber-Attacks on National CI

The history of cyber warfare targeting critical infrastructure includes landmark cases that demonstrated the potential for digital attacks to cause physical disruption.

One such foundational example is **Stuxnet**, a sophisticated computer worm discovered in 2010. Stuxnet is widely regarded as the world’s first true cyber weapon, engineered specifically to target industrial control systems. Its primary target was Iran’s Natanz uranium enrichment facility, where it exploited zero-day vulnerabilities to sabotage centrifuge operations while aiming to remain undetected. Stuxnet successfully caused mechanical failures in this critical part of Iran’s nuclear infrastructure, demonstrating that cyber warfare could indeed inflict physical destruction and marking a new era in digital conflict and national security threats. Operation Shadow Strike, detailed in one source, explicitly leans into Stuxnet as a historical case study, deriving core principles from its effectiveness in targeting critical infrastructure to stunt an adversary's military potential.

More **recent incidents** highlight the evolving tactics and continuing focus on critical sectors. An analysis published in June 2024 notes that the cybersecurity landscape has become increasingly perilous, with critical infrastructure facing a multitude of threats over the past year. **GPS spoofing** is presented as an advanced technique used by cyber adversaries targeting critical infrastructure, notably affecting the maritime and transportation sectors. A notable example involved the manipulation of GPS signals to disrupt critical shipping routes and logistics networks. This resulted in misdirected shipments and potential near-misses at sea, severely undermining the integrity of global positioning data crucial for these sectors. This incident serves as a specific illustration of sophisticated tactics used to disrupt essential services by undermining critical operational data.

Another very recent example involves a **cyber attack on major hospitals in London**. This incident, reported to be a critical IT incident affecting pathology services (which include blood transfusions), led to the cancellation or redirection of a number of procedures. It affected large London hospitals like Guy's and St Thomas's NHS trust and King's College Hospital. This case exposes the vulnerability of critical IT systems within healthcare to cyberattacks and demonstrates the potential for disruption to essential, life-critical services. While the exact nature and perpetrators were not immediately clear, the impact on patient care underscored the severity of attacks on critical healthcare infrastructure.

2.3 Strategic Motivations Behind Attacks on Critical Infrastructure

The motivations driving cyberattacks on critical infrastructure are multifaceted, ranging from geopolitical objectives to less sophisticated goals. Primarily, these attacks are seen as operations by nation-state actors and APTs aiming to **disrupt, spy on, or degrade vital sectors**. The objective can be to **achieve national objectives in cyberspace**, including gaining leverage or disabling an adversary's capabilities. State actors are known to be constantly **probing critical infrastructure** in various countries. The effectiveness demonstrated by attacks like Stuxnet in inflicting severe physical damage has shown just how valuable weaponized cyberattacks can be in stunting an adversary's military potential.

While strategic goals often involve geopolitical significance or establishing dominance, other motivations can also play a role, sometimes intertwined with state activity. These can include **espionage** or, less commonly for pure cyber warfare (though prevalent in general cybercrime), **financial gain**, such as demanding ransomware payments. Some attacks might also be driven by activist groups with political leanings or simply the pursuit of **notoriety** among peers by exploiting vulnerable systems. Discussions around cyber threats also touch upon the potential for deliberate misrepresentation of the threat, perhaps for reasons of advocacy or resource allocation. Ultimately, strategic motivations in the context of CI attacks often revolve around **gaining a tactical or strategic advantage** over an adversary, disrupting their society, economy, or military capabilities by targeting the essential services they rely upon.

2.4 Commonly Targeted Sectors and Their Vulnerabilities

Several sectors are consistently identified as prime targets for cyberattacks within critical infrastructure due to their vital role and inherent vulnerabilities. These include:

- **Power grids** and **energy networks**: These are foundational for all other CI sectors.
- **Water systems**: Essential for public health and safety.
- **Healthcare networks**: Critical for public well-being and life safety.
- **Transportation**, including **maritime operations** and **seaports**: Vital for logistics, economy, and movement.
- **Financial systems**: Crucial for economic stability and operations.
- **Government IT infrastructure**: Stores sensitive data and supports essential functions.
- **Communication networks**, including **undersea cables**: Essential for connectivity and control.

These sectors are vulnerable for a variety of reasons. The **rapid digitalization** and increasing interconnectedness of previously isolated operational technology (OT) systems expose them to digital threats. Many critical systems still rely on **antiquated hardware, software, and outdated computer operating systems**, making them highly vulnerable to both known and newly discovered vulnerabilities. **Outdated operational technology** and its integration with IT systems create attack vectors. Simple **misconfigurations**, such as in proxy auto-configuration files, can also be exploited to redirect traffic and facilitate unauthorized access. The fundamental

interdependence of critical infrastructures, particularly their reliance on the power grid, means that an attack on one sector can cascade and affect others, magnifying the impact. Furthermore, the **criticality** of these sectors makes them attractive targets as disrupting them can have wide-ranging severe consequences, including disruption of services, economic losses, and loss of public trust.

3. Case Study: Industroyer2 Cyberattack on Ukraine's Power Grid

In April 2022, Ukraine's Computer Emergency Response Team (CERT-UA), in collaboration with cybersecurity firm ESET, identified a sophisticated cyberattack targeting the nation's power grid. This attack involved a variant of the Industroyer malware, dubbed **Industroyer2**, designed to disrupt high-voltage electrical substations by exploiting the IEC 60870-5-104 (IEC-104) protocol. The malware was scheduled for execution on April 8, 2022, but was detected and neutralized before causing any operational impact .

This incident mirrors a previous attack in December 2016, where the original Industroyer malware caused a blackout in Kyiv, affecting approximately 20% of the city's power supply for about an hour .

The attack is attributed to the **Sandworm** group, also known as **APT44**, a cyber unit within Russia's military intelligence agency, the GRU. Sandworm has a history of conducting cyber operations against Ukraine, including the 2015 and 2016 power grid attacks, and the 2017 NotPetya malware campaign .

The **targeted infrastructure** comprised high-voltage electrical substations within Ukraine's power grid. Industroyer2 was specifically engineered to interact with industrial control systems (ICS) and operational technology (OT) devices, such as protection relays and circuit breakers, using the IEC-104 protocol. The malware's configuration files contained hardcoded information tailored to the victim's environment, indicating prior reconnaissance and a deep understanding of the targeted systems.

- **Malware Used:** Industroyer2, a successor to the original Industroyer malware, written in C++. Unlike its predecessor, Industroyer2 is a standalone executable with a narrower focus on the IEC-104 protocol .

- **Attack Vector:** While the exact initial access method remains undisclosed, it's believed that the attackers gained entry through compromised credentials or phishing campaigns, followed by lateral movement within the network to reach the ICS environment .
- **Lateral Movement:** The attackers likely used standard administrative tools and protocols to navigate the network, avoiding detection by blending in with legitimate traffic.
- **Payloads:** Industroyer2's payload was designed to send malicious commands to ICS devices, manipulating their operations to disrupt the power supply. The malware could open and close circuit breakers, effectively controlling the flow of electricity .

Due to the timely detection and intervention by CERT-UA and ESET, the attack was thwarted before execution, preventing any disruption to the power grid. Had the attack succeeded, it could have caused significant power outages, affecting critical services such as healthcare, transportation, and communication, and potentially leading to economic and societal disruptions.

- **Economic Impact:** While this specific incident did not result in financial losses, previous attacks like NotPetya have caused billions in damages globally, highlighting the potential economic ramifications of such cyber threats .
- **Social Impact:** Repeated cyberattacks on critical infrastructure can erode public trust in governmental institutions and essential services, leading to increased anxiety and societal unrest .

The swift response by CERT-UA and ESET involved isolating affected systems, analyzing the malware, and implementing mitigation strategies to prevent execution. The incident prompted international cybersecurity communities to share information and reinforce defenses against similar threats. Global reactions included heightened alerts and advisories from cybersecurity agencies, emphasizing the need for robust protection of critical infrastructure and collaboration among nations to counter state-sponsored cyber threats.

3.1 MITRE ATT&CK Framework Reference

Technique ID	Tactic	Technique Name	Description
T0800	Collection	Automated Collection	Industroyer2 can automatically collect data from targeted devices without manual intervention.
T0806	Control	Brute Force I/O	Iterates across a device's Information Object Addresses (IOAs) to modify their ON/OFF states.
T0836	Impair Process Control	Modify Parameter	Alters specified IOAs for designated Application Service Data Unit (ASDU) addresses to either the ON or OFF state.
T0855	Impair Process Control	Unauthorized Command Message	Sends command messages from the compromised device to target remote stations, modifying IO state values through operations like Select Before Operate I/O, Select/Execute, and Invert Default State.
T0881	Inhibit Response Function	Service Stop	Terminates specified processes (e.g., PServiceControl.exe and PService_PDD.exe) to prevent restart, hindering system recovery.
T0801	Discovery	Monitor Process State	Uses General Interrogation commands to monitor device IOAs and their state values.
T0888	Discovery	Remote System Information Discovery	Polls target devices for connection status, data transfer status, Common Address (CA), IOAs, and IO state values across multiple priority levels.

T0843	Discovery	Process Discovery	Identifies active processes on the system to understand the operational environment.

4. National Resilience & Defense Strategy

Cyber Defense Strategy Proposal: Enhancing National Resilience in The African Republic

Date: May 21, 2025

Subject: Strategic Action Plan for Protecting Critical Infrastructure against Cyber Threats

The African Republic, like many nations, is vulnerable to these evolving threats. The potential consequences of a successful cyberattack on critical infrastructure are severe and wide-ranging, including disruption of essential services, significant economic losses, and erosion of public trust. As demonstrated by historical cases like the attacks on Ukraine's power grid using malware like Industroyer, cyber operations can precede or accompany conventional actions and inflict severe physical damage when used against critical infrastructure. The African Republic must adopt a robust, proactive, and multi-layered approach to enhance its cyber resilience and protect its vital national assets. This document outlines a strategic action plan to achieve this objective.

4.1. Threat Modeling and Risk Prioritization for CI Sectors

A fundamental step in building national resilience is conducting comprehensive threat modeling and prioritizing risks across critical infrastructure sectors. The landscape of threats against CI is complex and rapidly evolving, involving a multitude of actors and attack vectors.

- **Identifying Threats and Actors:** Key threat actors include nation-state actors and Advanced Persistent Threats (APTs), terrorists, cybercriminals, and activist groups. These actors employ various sophisticated tactics, including ransomware, AI-driven phishing, supply chain attacks, DDoS attacks, exploitation of outdated operational technology (OT) and interconnected systems, and insider threats. Some actors may simply seek notoriety, while others have financial, political, or strategic motivations, including disrupting physical operations or causing severe consequences like loss of life.
- **Assessing Vulnerabilities:** Critical infrastructure systems, often based on antiquated hardware and software or featuring increasing convergence of IT and OT systems, present significant vulnerabilities. Misconfigurations, such as those exploited through

PAC files, can also create pathways for unauthorized access and data exfiltration. The reliance of critical services on the power grid means that grid failures cascade and affect all connected sectors.

- **Prioritizing Risks:** Risks should be prioritized based on the potential scale and effects of an attack. Attacks aiming to incapacitate critical infrastructures, even without causing direct physical destruction, could amount to significant harm. Consequences include disruption of critical services, significant economic losses, damage to public trust and reputation, and severe life-safety issues, particularly from disruption of services like healthcare or water. Prioritization should focus on sectors with the highest potential impact on national security and public safety.

This phase requires continuous threat intelligence gathering to update target profiles and identify emerging vulnerabilities.

4.2. Policies & Frameworks

Establishing clear policies and regulatory frameworks is crucial for governing cyberspace operations and mandating security standards for CI.

- **Defining Cyber Warfare and Legal Boundaries:** A strategic framework requires establishing clear legal and ethical parameters for cyber operations, ensuring adherence to international law, including principles of distinction, proportionality, and necessity. This involves developing internationally accepted definitions for terms like "cyber warfare" and clarifying when cyber operations constitute an "armed attack" under international law, such as Article 51 of the UN Charter. Incorporating cyber warfare regulations into frameworks like the Geneva Conventions is essential to ensure humanitarian principles are upheld.
- **Mandating Cybersecurity Standards:** Implementing cybersecurity resilience standards for critical infrastructure, such as energy grids, financial institutions, and communication networks, is necessary to reduce vulnerabilities. These policies should mandate robust measures across CI sectors. While specific frameworks like NIST, ISO, or EU NIS2 are mentioned in the assignment requirements, the sources broadly advocate for mandated resilience standards and adherence to international norms.
- **Formalizing Incident Handling:** Policies should include formalizing incident response playbooks and standardizing incident handling protocols to ensure swift containment and

forensic readiness following an attack. This standardizes processes and ensures consistent action across different sectors.

- **Addressing Legal Challenges:** Policies must also address legal challenges, such as strengthening attribution mechanisms to accurately identify perpetrators, which reduces the risk of misdirected retaliation and enhances accountability. Discussions around issues like anticipatory self-defense in the cyber domain highlight the need for evolving legal frameworks.

4.3. Technical Controls: Segmentation, Monitoring, and OT Security

Implementing robust technical controls is vital for protecting CI from the tactical execution of cyberattacks. A multi-layered, proactive approach integrating advanced detection, response, and recovery techniques is recommended.

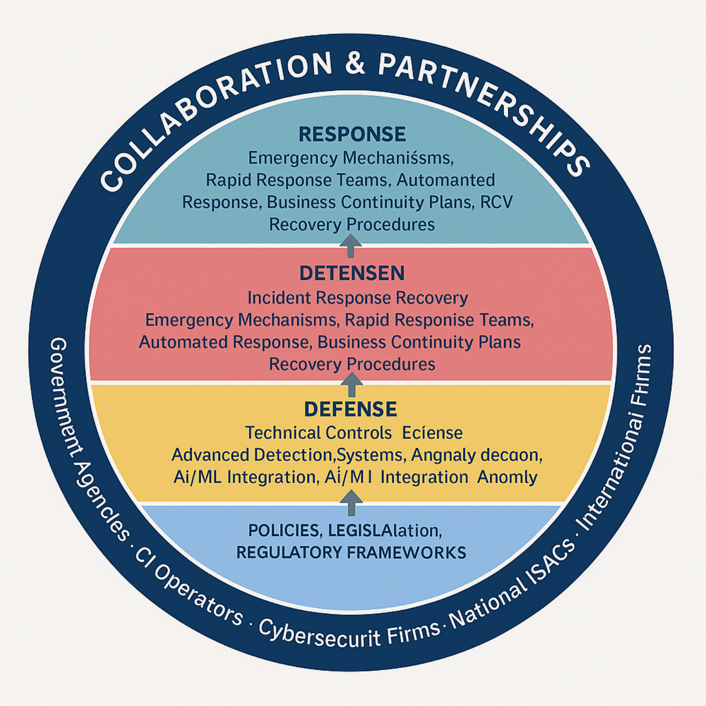
- **Network Segmentation and Microsegmentation:** Implementing network segmentation, utilizing VLANs, strict ACLs, network zoning, and host firewalls, is crucial for isolating internal servers and containing breaches. Microsegmentation further enhances security by dividing networks into smaller, isolated zones, which is particularly critical for OT environments.
- **Advanced Monitoring and Anomaly Detection:** Comprehensive, continuous monitoring of network traffic and system activities is essential to detect anomalies indicating a breach in progress. Advanced detection systems, including threat intelligence and anomaly detection techniques, are needed. Tools like Zeek, Suricata, and Wazuh + ELK Stack can support deep packet inspection, signature-based and behavioral-based intrusion detection, and centralized logging and alerting. Artificial Intelligence (AI) and Neural Networks can enhance these capabilities by examining vast data collections instantly, identifying irregularities, and improving detection accuracy while minimizing false positives.
- **Operational Technology (OT) Security:** Given the vulnerabilities in outdated OT and interconnected systems within CI, specific focus is needed on OT security. This includes integrating AI/ML technologies across OT/ICS environments for enhanced anomaly detection and operational resilience. Cyber-Informed Engineering practices advocate designing security into systems from the outset, reducing vulnerabilities in OT/ICS architecture.

- **Implementing Foundational Security Measures:** Core technical controls like enforcing strong password policies and enabling Multi-Factor Authentication (MFA) for access to critical systems are fundamental defenses against credential-stuffing and compromised accounts. Robust patch management is also essential to address known vulnerabilities. For high-security systems, employing air-gapped networks and quantum encryption can provide additional layers of protection.

The Zero Trust framework provides a robust strategic approach to technical controls, emphasizing continuous verification, least privilege access, microsegmentation, MFA, and comprehensive monitoring across the network, regardless of location.

4.4. Emergency Response Plan and Resilience Posture

Developing a comprehensive emergency response plan and building a resilient posture are critical for minimizing the impact of cyber incidents and ensuring continuity of essential services.


COLLABORATION & PARTNERSHIPS
RESPONSE
Emergency Mechaniśsms,
Rapid Response Teams, Automanted
Response, Business Continuity Plans, RCV
Recovery Procedures
DETENSEN
Incident Response Recovery
Emergency Mechanisms, Rapid Responise Teams,
Automated Response, Business Continuity Plans
Recovery Procedures
DEFENSE
Technical Controls Ecíense
Advanced Detection,Systems, Angnaly decαon,
Ai/ML Integration, Ai/M I Integration Anomly
POLICIES, LEGISLAlation,
REGULATORY FRAMEWORKS
Government Agencles · CI Operators · Cybersecurit Firms · National ISACs · International FHrms

- **Standardized Protocols and Training:** Formalizing incident response playbooks and standardizing protocols are necessary for swift containment, analysis, and recovery. Regular training exercises, including tabletop scenarios and live-fire simulations, are crucial for IT and security staff to practice incident handling, credential rotation, and rollback procedures. Training should be relevant for each level of command and included in military curriculum where applicable.

- **Ensuring Business Continuity:** Resilience is a fundamental business continuity strategy for critical infrastructure, where disruptions have real-world consequences. This includes ensuring forensic readiness to support post-incident investigations. Plans must account for maintaining operations even if digital systems are compromised, potentially relying on manual procedures for essential functions, as demonstrated by the London hospitals incident.
- **Adaptive Measures and Redundancy:** Emergency plans should incorporate adaptive measures to counter detected enemy countermeasures. Ensuring abundant redundant Internet connectivity helps systems manage significant traffic volumes during DDoS attacks. Building redundant and stealthy Command and Control (C2) channels using decentralized infrastructures and advanced encryption protocols can ensure continuous control during complex operations. Automated incident response frameworks can provide real-time detection, containment, and mitigation.
- **Rapid Response Teams:** Developing specialized rapid incident response teams capable of swiftly neutralizing retaliatory actions is crucial for maintaining control of the cyber battlefield.

Educating the public and authorities about potential threats and response protocols is also part of building a resilient national posture.

4.5. Collaboration Roles between Government, Private Sector, and CERTs

Effective national resilience relies heavily on strong collaboration and information sharing among government entities, private sector organizations operating CI, and Computer Emergency Readiness Teams (CERTs).

- **Public-Private Partnerships:** Formal information exchange mechanisms concerning cyber threats, vulnerabilities, and incidents between the public and private sectors are crucial. This includes cooperation with Internet service providers and technology providers. Private companies, including tech firms and cybersecurity specialists, hold significant expertise and provide vital services, such as military satellite communications in the US context.

- **Cross-Sector Collaboration:** Collaboration is needed between security teams, operations personnel, and executive leadership within organizations managing CI, as well as across different CI sectors. This ensures a holistic approach to security.
- **Collaboration with Law Enforcement and Security Agencies:** Closer collaboration between Chief Information Security Officers (CISOs) in critical sectors (like financial institutions) and national police or cybercrime centers is important for investigating and combating cybercriminals and threats. Cyber-armies play a role in deterring, intercepting, and responding to attacks by adversarial nations, terrorists, and criminal actors.
- **International Cooperation:** Engaging with international cybersecurity bodies and allied nations is vital for developing shared protocols, norms, and intelligence-sharing platforms. Leveraging diplomatic channels helps manage attribution challenges and mitigate the risk of international escalation. Establishing a real-time threat intelligence sharing platform with allies can augment situational awareness and expedite decision-making.

Building strong alliances with cyber-friendly nations can also counterbalance potential diplomatic isolation and enhance collective security.

5. Conclusion

The evolving landscape of cyber warfare presents a significant and escalating threat to national critical infrastructure, driven by sophisticated nation-state actors and APTs. Entities like China's PLASSF demonstrate strategic focus and capabilities in this domain. Attacks range from potentially destructive operations targeting industrial control systems, as exemplified by Stuxnet's impact, to stealthy, low-noise techniques involving credential abuse and exploiting system configurations, highlighted in Operation Blacktrace. Countering these advanced threats necessitates a shift beyond traditional security models and navigating complex legal and ethical challenges. Building national resilience requires a proactive, multi-layered defense. This involves adopting frameworks like Zero Trust, enhancing threat intelligence, implementing robust technical controls, and fostering essential collaboration between government, the private sector, and CERTs. Prioritizing these comprehensive measures is crucial to safeguard vital sectors against the pervasive digital threats of the modern era.

6. References

Ashraf, M., Ahmad, F., & Iqbal, I. (2025). Advanced cybersecurity strategies leveraging neural networks for protecting critical infrastructure against evolving digital threats through proactive risk management and threat intelligence. *IECE Transactions on Neural Computing, 1*(1), 44–54.

Council on Foreign Relations. (n.d.). Tracking state-sponsored cyberattacks around the world.

Durojaye, H., & Raji, O. (2022). Impact of state and state-sponsored actors on the cyber environment and the future of critical infrastructure. *arXiv preprint arXiv:2212.08036.* Retrieved from https://arxiv.org/abs/2212.08036

ENISA. (2010). EU agency analysis of 'Stuxnet' malware: A paradigm shift in threats and critical information infrastructure protection. Retrieved from https://www.enisa.europa.eu/news/enisa-news/eu-agency-analysis-of-2018stuxnet2019-malware-a-paradigm-shift-in-threats-and-critical-information-infrastructure-protection-1enisa.europa.eu+1 tools.enisa.europa.eu+1

Goffer, M. A., Uddin, M. S., Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., … Hasan, R. (2025). AI-enhanced cyber threat detection and response: Advancing national security in critical infrastructure. *Journal of Posthumanism, 5*(3), 1667–1689.

Greenberg, A. (2022). Russia's Sandworm hackers attempted a third blackout in Ukraine. *WIRED.* Retrieved from https://www.wired.com/story/sandworm-russia-ukraine-blackout-gru

Industrial Cyber. (2024, June 30). Targeting critical infrastructure: Recent incidents analyzed - Industrial Cyber. Retrieved from https://scholar.smu.edu/cgi/viewcontent.cgi?article=1585&context=til

Melzer, N. (n.d.). *Cyberwarfare and international law.* Retrieved from https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf

New Eastern Europe. (2024). Lessons about cyber warfare from Russia's war against Ukraine. Retrieved from https://neweasterneurope.eu/2024/06/22/lessons-about-cyber-warfare-from-russias-war-against-ukraine/

Sky News. (n.d.). Cyber attack hits major London hospitals as procedures are cancelled.

Wikipedia contributors. (2023). *2015 Ukraine power grid hack.* Retrieved from https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack

Wikipedia contributors. (2025). *ATT&CK*. Retrieved from https://en.wikipedia.org/wiki/ATT%26CK

Wikipedia contributors. (2025). *Industroyer.* Retrieved from https://en.wikipedia.org/wiki/Industroyer

Wikipedia contributors. (2025). *Petya (malware family)*. Retrieved from https://en.wikipedia.org/wiki/Petya_(malware_family)

Wikipedia contributors. (2025). *Sandworm (hacker group)*. Retrieved from https://en.wikipedia.org/wiki/Sandworm_(hacker_group)