International Journal of Creative and Open Research in Engineering and Management
ISSN: **3108-1754 (Online)**
Volume 02 Issue 05 May-2026 | Impact Factor: 3.5

Cybersecurity for Critical Infrastructure Strategies, Challenges and Future Directions

Prabhat Bisht
1 NIC, Chandigarh Haryana, INDIA (Orcid ID: https://orcid.org/0000 0001 6656 8115)
Email address: prabhatbisht@gmail.com
*Corresponding Author: prabhatbisht@gmail.com

How to Cite this Article:
Bisht, P. (2026). Cybersecurity for Critical Infrastructure Strategies, Challenges and Future Directions. International Journal of Creative and Open Research in Engineering and Management, 02(05). https://doi.org/10.55041/ijcope.v2i5.883

https://doi.org/10.55041/ijcope.v2i5.883

Abstract: Critical infrastructure systems—including energy grids, water supply networks, transportation systems, and healthcare facilities—are increasingly dependent on digital technologies, thereby expanding their exposure to cyber threats. This paper analyses the current cybersecurity landscape for critical infrastructure, with a focus on identifying key vulnerabilities such as legacy system limitations, inadequate security integration, and increased interconnectivity. To mitigate these risks, the study proposes strategic frameworks centred on Zero Trust Architecture and AI-driven threat detection to enable continuous monitoring and adaptive response. Furthermore, a comparative analysis of global best practices is presented to evaluate existing approaches and identify gaps in implementation. The paper also outlines future research directions aimed at enhancing system resilience, strengthening security frameworks, and supporting the reliable operation of essential services.

Keywords—component; formatting; style; styling; insert (key words)

1. INTRODUCTION

Critical infrastructure, including energy grids, water systems, transportation networks, healthcare services, and telecommunications forms the backbone of national security, public safety, and economic stability. In India, the rapid adoption of digital technologies such as the Internet of Things (IoT), cloud computing, and industrial automation has significantly enhanced the efficiency and responsiveness of these sectors. However, this digital transformation has also expanded the cyber-attack surface, exposing critical systems to a wide range of threats, including ransomware, advanced persistent threats, and state-sponsored attacks.

Cyber incidents targeting critical infrastructure can have severe and far-reaching consequences, such as large-scale power outages, disruption of essential healthcare services, and instability in transportation networks. India's diverse and evolving infrastructure landscape further intensifies these challenges, particularly due to the coexistence of legacy systems, increasing interconnectivity, and varying levels of cybersecurity maturity across sectors.

This paper investigates the current cybersecurity landscape of critical infrastructure in India by identifying key vulnerabilities in both legacy and modern systems. It evaluates the effectiveness of existing national frameworks, including the National Cyber Security Policy (2013), CERT-In guidelines, and directives issued by the National Critical Information Infrastructure Protection Centre (NCIIPC). To address emerging risks, the study proposes the adoption of advanced security approaches such as Zero Trust Architecture and AI-driven threat detection to enable continuous monitoring and proactive defense.

Furthermore, a comparative analysis of global best practices, including the NIST Cybersecurity Framework, is conducted to assess their applicability within the Indian context. The paper concludes by outlining future research directions focused on enhancing resilience, strengthening policy frameworks, and fostering public–private collaboration to ensure the secure and reliable operation of critical infrastructure.

2. LITERATURE REVIEW

Cybersecurity in critical infrastructure has evolved significantly over the past two decades due to rapid technological advancements and increasingly sophisticated cyber threats. This section reviews key literature on industrial control system (ICS) vulnerabilities, security frameworks, defence models, and policy developments, with a focus on the Indian context.

2.1 ICS Vulnerabilities and Stuxnet

The discovery of the Stuxnet worm marked a major turning point in industrial cybersecurity. Fallerie, Murchu, and Chien (2011) demonstrated how Stuxnet exploited multiple zero-day vulnerabilities to target Siemens programmable logic controllers (PLCs) in Iran's nuclear facilities. This attack highlighted the susceptibility of ICS to advanced, state-sponsored cyber threats and emphasized the need for specialized security mechanisms in operational technology (OT) environments.

2.2 Frameworks for Critical Infrastructure Protection

The National Institute of Standards and Technology (NIST) introduced the Cybersecurity Framework (CSF) to help organizations manage and mitigate cybersecurity risks. The framework is based on five core functions Identify, Protect, Detect, Respond, and Recover—and is widely recognized as a global standard for securing critical infrastructure due to its flexibility and risk-based approach.

2.3 Zero Trust Architecture

Kindervag (2010) proposed the Zero Trust model, which eliminates implicit trust within networks and enforces continuous verification of users and devices. This approach is particularly relevant to critical infrastructure, where traditional perimeter-based defenses are insufficient against insider threats and lateral movement. Zero Trust Architecture (ZTA) is increasingly adopted as a proactive security model.

2.4 AI and Machine Learning in Threat Detection

Advancements in artificial intelligence (AI) and machine learning (ML) have significantly improved cybersecurity capabilities. Sarker et al. (2021) highlight the use of ML algorithms in anomaly detection, intrusion prevention, and predictive analysis. These technologies enable real-time monitoring and adaptive responses, making them effective for securing complex infrastructure systems.

2.5 Indian Cybersecurity Policy and CERT-In Guidelines

India's cybersecurity framework is primarily guided by the National Cyber Security Policy (2013), supported by CERT-In and the National Critical Information Infrastructure Protection Centre (NCIIPC). These bodies provide guidelines for incident reporting, vulnerability management, and sector-specific security practices. However, the policy requires updates to address emerging technologies such as IoT, AI, and cloud computing.

2.6 Cybersecurity Challenges in Indian Critical Infrastructure

India has witnessed a growing number of cyberattacks targeting critical sectors such as energy, healthcare, and transportation. Many of these attacks involve advanced persistent threat (APT) groups exploiting vulnerabilities in SCADA and OT systems. The RedEcho campaign, which contributed to a power outage in Mumbai, exposed weaknesses in grid security and highlighted the risks posed by legacy systems and insufficient monitoring.

Studies by Chakraborty and Tiwari identify key systemic issues, including outdated policies, fragmented governance structures, and reliance on foreign technologies. The lack of centralized coordination further limits effective cyber defense.

2.7 IoT and Cloud Security Vulnerabilities

The integration of IoT and cloud computing has enhanced infrastructure efficiency but introduced new security risks. Almutairi and Sheldon identify vulnerabilities such as insecure APIs, insider threats, and adversarial attacks in IoT–cloud ecosystems. Similarly, Singh, Buyya, and Kim emphasize that cloud-based IoT environments increase the attack surface and introduce data privacy concerns. They recommend mitigation strategies such as encryption, access control, and device-specific security protocols.

2.8 Real-World Cyber Threats to Indian Infrastructure

India's critical infrastructure, particularly the power sector, has been repeatedly targeted by cyber espionage campaigns. Reports indicate attacks by groups such as RedEcho and TAG-38 using advanced malware like ShadowPad and leveraging compromised third-party systems. These incidents highlight persistent vulnerabilities in ICS environments and the need for proactive threat intelligence, intrusion detection systems, and continuous infrastructure hardening.

3. RESEARCH METHODOLOGY

3.1 Assessment of cybersecurity vulnerabilities in India's critical infrastructure sectors

India's critical infrastructure sectors such as energy, healthcare, transportation, water supply, finance and telecommunications are increasingly digitized, making them more efficient but also more vulnerable to cyber threats. This section provides a detailed assessment of the key cyber security vulnerabilities affecting these sectors.

3.1.1 Legacy Systems and Operational Technology (OT) Risks

Many infrastructure systems still rely on legacy technologies that were not designed with cyber security in mind. These systems often lack encryption, secure authentication, and patch management capabilities. The integration of OT with IT networks further increases exposure, enabling attackers to exploit outdated protocols and gain access to sensitive control systems.

3.1.2 IoT and Cloud Integration Challenges

The adoption of IoT devices and cloud platforms has revolutionized infrastructure management but introduced new vulnerabilities:
IoT Risks**:** Weak authentication, unpatched firmware, and lack of standardization.
Cloud Risks**:** API exploits, data breaches, and insider threats due to centralized data storage.
Studies by Almutairi and Sheldon, and Singh, Buyya, and Kim emphasize the need for scalable, adaptive security frameworks that incorporate encryption, access control, and blockchain-based verification.

3.1.3 Advanced Persistent Threats (APTs)

India has been targeted by APT groups such as RedEcho and TAG-38. These groups use sophisticated malware (e.g., ShadowPad) and exploit third-party devices to mask command-and-control communications. The RedEcho campaign, which led to a power outage in Mumbai, is a prime example of how ICS vulnerabilities can be exploited for geopolitical purposes.

3.1.4 Human Factors and Awareness

Cybersecurity awareness among infrastructure operators remains low. Common issues include:
Poor password hygiene, Lack of training on phishing and social engineering, Inadequate incident response protocols
These human factors often serve as the entry point for attackers, especially in sectors with limited IT support.

3.2 Critical Infrastructure Sectors

3.2.1 Energy: Smart grids and nuclear facilities are prime targets due to their strategic importance. The 2019 Kudankulam nuclear plant breach exposed vulnerabilities in operational technology (OT) systems. Smart grids are vulnerable **to** False Data Injection Attacks **,** SCADA system exploits and ransomware**.**
3.2.2 Healthcare: Hospitals face ransomware attacks and data breaches, threatening patient safety and privacy. The AIIMS ransomware incident is a notable example
3.3.3 Finance: Banks and financial institutions suffer from phishing, malware implants, and data theft. ICICI Bank's vendor portal malware attack and the Central Bank phishing compromise highlight systemic risks
3.3.4 Telecommunications: Telecom networks are vulnerable to DDoS attacks and espionage. Spoofing of domains and exploitation of APIs (e.g., DigiLocker) are common.
3.3.5 Transportation & Water Supply: Interconnected systems like smart meters and traffic control are susceptible to cascading failures from cyberattacks. Smart meters and automated control systems are vulnerable to malware and DDoS.

3.3 Cybersecurity Frameworks in India: An Analytical Overview.

India's cybersecurity is primarily guided by **CERT-In guidelines** and the **National Cyber Security Policy (2013)** . However, these frameworks lack provisions for emerging technologies like AI, IoT and quantum computing in mitigating cyber security also the absence of a centralized cybersecurity authority leads to fragmented responses and jurisdiction overlaps.

3.3.1 CERT-In: CERT-In Guidelines (2025)

Mandate and Scope

The 2025 guidelines from the Indian Computer Emergency Response Team (CERT-In), in accordance with Section 70B of the Information Technology Act, 2000, require an annual cybersecurity audit for any organization running digital systems. The audit spans numerous areas like network infrastructure, cloud infrastructure, artificial intelligence-based systems, IoT, and industrial control systems (ICS/OT). The guidelines focus on the adoption of international standards like ISO/IEC 27001, OWASP, CVSS, EPSS and Software Bill of Materials

Major mandate of CERT In: Monitor and analyze cybersecurity incidents.

- Issue alerts, advisories, and vulnerability notes.
- Coordinate incident response across sectors.
- Conduct cybersecurity drills and training.
- Collaborate with international CERTs and organizations.
- Support implementation of cybersecurity policies and standards.

Strengths

Mandatory Compliance: In contrast to the NCSP the CERT-In guidelines are obligatory, promoting higher accountability.
Risk-Based Approach: Organizations are motivated to implement lifecycle-based audits and ongoing monitoring methodologies.
Data Governance: Tight procedures are specified for handling, storage, and disposal of audit information.
Alignment with National Strategy: The guidelines align with India's overall Digital Public Infrastructure (DPI) mission, bolstering national cyber resilience.
Major Strength:

- Centralized coordination of cybersecurity incidents.
- Real-time threat intelligence and advisories.
- Strong institutional support and legal mandate.
- International collaboration with global CERTs.

Limitations

Operational Burden: Small businesses can struggle to comply with the audit demands because they do not have the necessary resources.

Skill Shortages: Enforcing new audit procedures requires high levels of upskill among cybersecurity professionals.
Risk of Formalism: Audits tend to become procedural instead of substantive, which defeats their purposes.
Enforcement Complexity: The graded penalties may be challenging to enforce on a consistent basis given varying industries and firm sizes.
Major Limitations:

- Reactive posture in handling emerging threats.
- Limited outreach to SMEs and citizens.
- Resource constraints in staffing and infrastructure.
- Coordination gaps with other cybersecurity agencies.

Table 1 Pros of CERT IN

Strength	Description
National Coordination	Acts as the central agency for responding to cybersecurity incidents across India.
24/7 Monitoring	Provides round-the-clock threat monitoring and incident response.
Sectoral Expansion	CERT-In has expanded to cover fintech, telecom, and healthcare sectors.
Cyber Alerts & Advisories	Regularly publishes vulnerability alerts, patches, and best practices for organizations.
International Collaboration	Works with global CERTs and organizations like FIRST, AP-CERT, and ITU.
Capacity Building	Conducts training programs, workshops, and cyber drills for government and private entities.

Table 2: Cons of CERT In

Limitation	Description
Reactive Approach	Often criticized for being more reactive than proactive in threat mitigation.
Limited Public Engagement	Lacks strong outreach to SMEs and citizens for cyber hygiene awareness.
Resource Constraints	Faces challenges in scaling operations due to budget and manpower limitations.
Coordination Gaps	Overlaps with other agencies like NCIIPC and I4C can lead to fragmented responses.
Transparency Issues	Limited public disclosure of incident statistics and response outcomes.
Slow Response to Zero-Day Threats	Sometimes lags in issuing advisories for emerging vulnerabilities.

3.3.2 NCSP: National Cyber Security Policy (2013)

Mandate and Objectives
The NCSP, originally launched in 2013 by the Ministry of Electronics and Information Technology (MeitY), aims to create a secure cyber ecosystem in India. Its key objectives include, Government of India, was a landmark initiative to create a secure and resilient cyber environment. The policy sought to protect information and infrastructure in cyberspace, establish prevent and respond capabilities against cyber threats, and lower vulnerabilities through institutional frameworks, public-private partnerships, and capacity building.
Its key objectives include

- **Building trust** in IT systems and transactions.
- **Creating an assurance framework** for security policies and global standards.
- **Strengthening regulatory mechanisms** for cybersecurity.
- **Enhancing protection** of critical information infrastructure.
- **Safeguarding privacy** and reducing economic losses from cybercrime.
- **Promoting global cooperation** in cybersecurity.

India's **National Cyber Security Policy (NCSP)** represent a comprehensive and evolving framework to safeguard the nation's cyberspace amid rising threats. Here's a detailed overview:

Strengths

Comprehensive Vision: The policy gave a comprehensive outlook for cybersecurity, including preventive and responsive measures.

Institutional Development: It suggested the formation of the National Critical Information Infrastructure Protection Centre (NCIIPC) and strengthened the position of the Indian Computer Emergency Response Team (CERT-In).

Capacity Building: Training, awareness, and the development of capable cybersecurity manpower were given priority.

Multi-Stakeholder Engagement: The policy promoted collaboration among government, industry, academia, and civil society.

Limitations

Absence of Legal Enforceability: The policy was advisory in nature and lacked binding enforcement provisions.

Technological Obsolescence: It failed to predict the fast pace of advancements in technologies like artificial intelligence, blockchain, and the Internet of Things (IoT).

Fragmented Implementation: Coordination between diverse stakeholders remained erratic, causing uneven implementation of the policy.

Absence of Periodic Review: The policy did not provide for regular reviews, making it obsolete in the light of evolving threats.

Table 3 Pros of NCSP

Advantage	Details
Comprehensive Framework	The NCSP provides a foundational structure for securing India's cyberspace, covering critical infrastructure, public services, and private sector engagement
Institutional Support	Agencies like CERT-In, NCIIPC, and NCCC have been instrumental in threat detection, incident response, and coordination
Public Awareness Initiatives	Campaigns such as Cyber Swachhta Kendra and digital hygiene programs have improved citizen awareness
Legal and Regulatory Evolution	The introduction of the **Digital Personal Data Protection Act (DPDP)** and sector-specific cyber laws has strengthened data governance
Capacity Building	Training programs and cybersecurity education initiatives have expanded, especially in collaboration with academia and industry
Global Engagement	India has increased participation in international cyber diplomacy and threat intelligence sharing

Table 4 Cons of NCSP

Limitation	Details
Fragmented Governance	Overlapping roles among CERT-In, NCIIPC, and other bodies lead to coordination issues and delayed responses
Reactive Posture	The policy is often criticized for being more reactive than proactive, especially in handling zero-day vulnerabilities and ransomware
Workforce Shortage	India faces a significant gap in skilled cybersecurity professionals, affecting implementation and innovation.

Limited Budget Allocation	Cybersecurity receives less than 0.25% of the national budget, which is inadequate given the scale of threats
Inadequate Protection for SMEs and Rural Areas	Smaller enterprises and rural digital infrastructure remain under protected due to resource constraints
Slow Policy Updates	The NCSP (2013) has not been comprehensively revised to address emerging threats like AI-driven attacks, misinformation, and quantum computing

3.3.3 National Cyber Security Strategy (NCSS)

The NCSS 2025 builds on the NCSP and introduces advanced measures to tackle modern cyber threats.
Key highlights include

AI-Powered Threat Detection

Real-time monitoring using AI-driven platforms.
Deepfake detection systems to combat misinformation.

Quantum-Safe Encryption

Testing quantum-resistant encryption for banking and government networks.
Blockchain-based frameworks for secure financial transactions.

Cyber Resilience & Crisis Management

Expansion of CERT-In to fintech and telecom sectors.
Cyber Crisis Management Plans and mock drills across ministries and critical sectors

Public-Private Collaboration

Partnerships with tech giants and startups for R&D and ethical hacking.
Indigenous cybersecurity solutions for defence and banking.

International Cooperation

Collaboration with QUAD nations (US, Japan, Australia) on cyber defence.

The **National Cyber Security Strategy (NCSS)** is designed to:

- **Protect critical information infrastructure (CII)** across sectors like finance, energy, defense, and healthcare.
- **Strengthen cyber resilience** through proactive threat detection, incident response, and recovery mechanisms.
- **Promote indigenous cybersecurity innovation** and reduce dependency on foreign technologies.
- **Enhance public-private partnerships** for collaborative defense.
- **Build capacity** through training, awareness, and academic programs.
- **Foster international cooperation** on cyber norms and threat intelligence sharing.

Table 5 Pros of NCSS

Advantage	Description
Comprehensive Coverage	Addresses technical, legal, institutional, and human aspects of cybersecurity.
AI & Quantum Integration	Incorporates emerging tech like AI for threat detection and quantum-safe encryption.
CERT-In Expansion	Sector-specific CERTs improve incident response in fintech, telecom, and healthcare.
Cyber Hygiene Campaigns	Public awareness initiatives like Cyber Swachhta Kendra reduce botnet infections.
Global Collaboration	Partnerships with QUAD nations and others enhance strategic cyber defense.

Table 6 : Cons of NCSS

Limitation	Description
Implementation Gaps	Policy execution varies across states and departments.
Skill Shortage	India faces a deficit of trained cybersecurity professionals.
Regulatory Overlap	Multiple agencies (MeitY, NCIIPC, CERT-In) sometimes lack coordination.
Limited Budget Allocation	Compared to global standards, cybersecurity funding is relatively low
Slow Legal Reform	Data protection laws and cybercrime legislation lag behind evolving threats.

3.4 Future Roadmap and Emerging Challenges

To strengthen the cybersecurity posture of India's critical infrastructure, a multi-dimensional roadmap is required, integrating technological innovation, policy reform, and capacity development.

3.4.1 Technical Enhancements

- Deployment of **AI-driven Security Operations Centers (SOCs)** across government ministries to enable real-time threat detection and response.
- Investment in **quantum-resistant cryptography** to address future risks from quantum computing advancements.
- Adoption of **blockchain-based identity management systems** for secure and tamper-proof authentication mechanisms.

3.4.2 Capacity Building

- Introduction of a **National Cybersecurity Fellowship Program** to develop skilled professionals in cybersecurity.
- Establishment of **dedicated cybersecurity universities or centers of excellence**, in collaboration with premier institutions such as IITs and NITs.

3.4.3 Policy and Legal Reforms

- Accelerated implementation of the **Digital Personal Data Protection (DPDP) Act, 2023**.
- Development of a **Cybersecurity Insurance Framework** to mitigate financial risks for organizations impacted by cyber incidents.

3.5 Global Engagement

- Active leadership in shaping **international cyber norms**, particularly within United Nations platforms.
- Strengthening **regional CERT collaboration** for cross-border threat intelligence sharing.
- Organization of an annual **India Cyber Defence Summit** to foster collaboration among policymakers, researchers, and industry stakeholders.

3.6 Key Challenges and Gaps

Despite notable progress, several challenges continue to hinder India's cybersecurity readiness:

- Rapid rise in **AI-powered cyberattacks and ransomware campaigns**
- Persistent **shortage of skilled cybersecurity professionals**
- Regulatory gaps and **limitations in enforcement of data protection frameworks**
- Lack of a unified cybersecurity governance architecture

3.7 Formulation of Institute like Cyber Swachhta Kendra (CSK)

Mandate and Scope

The Cyber Swachhta Kendra, launched in 2017 under MeitY and operated by CERT-In, focuses on botnet detection, malware analysis, and cyber hygiene awareness.

Core Functions
Detection and removal of botnet infections Malware analysis and threat intelligence sharing of security advisories public awareness initiatives on cybersecurity practices Collaboration with ISPs, academia, and industry partners.

3.8 Digital Personal Data Protection Act (DPDP), 2023

Mandate and Scope
The DPDP Act, enacted in 2023, represents India's first comprehensive legislation on data protection. It governs the processing of personal data and applies to both domestic and international entities handling Indian user data.

Key Provisions
- Consent-based data processing framework
- Rights of individuals, including data access, correction, and erasure
- Obligations for organizations to ensure security and data minimization
- Special requirements for Significant Data Fiduciaries (SDFs)
- Establishment of the Data Protection Board of India (DPBI)
- Cross-border data transfer under a regulated approach

Strengths
- Provides legal clarity and structured governance
- Enhances individual control over personal data
- Aligns partially with global standards such as GDPR
- Supports digital economy growth and innovation

Conclusion

The increasing digitization of critical infrastructure in India has significantly enhanced operational efficiency and service delivery; however, it has also expanded the attack surface and introduced complex cybersecurity challenges. This study highlights vulnerabilities arising from legacy systems, the convergence of IT and OT environments, rapid adoption of IoT and cloud technologies, and human factors collectively pose substantial risks to national security and public safety. The growing frequency of advanced persistent threats (APTs) and ransomware attacks further underscores the urgency for robust and adaptive cybersecurity measures. The analysis of existing frameworks, including the National Cyber Security Policy (2013), CERT-In guidelines, and initiatives led by NCIIPC, reveals that while India has established a foundational cybersecurity ecosystem, significant gaps remain in terms of policy modernization, enforcement, coordination, and preparedness for emerging technologies.

The absence of a unified governance structure and the challenges associated with skill shortages and resource constraints continue to limit the overall effectiveness of cybersecurity efforts. To address these challenges, this paper emphasizes the adoption of advanced security paradigms such as Zero Trust Architecture and AI-driven threat detection, which enable continuous monitoring, proactive defense, and resilience against sophisticated cyber threats. Furthermore, aligning national strategies with global best practices, including frameworks such as the NIST Cybersecurity Framework, can strengthen India's security posture and provide a structured approach to risk management.

Looking ahead, a comprehensive and multi-layered strategy is essential to secure critical infrastructure systems. This includes investments in next-generation technologies such as quantum-resistant cryptography, strengthening public–private partnerships, enhancing cybersecurity awareness and workforce development, and implementing robust legal frameworks such as the Digital Personal Data Protection Act (2023). Additionally, increased international cooperation and proactive threat intelligence sharing will play a crucial role in addressing cross-border cyber threats. In conclusion, ensuring the security and resilience of critical infrastructure requires a holistic, adaptive, and forward-looking approach. By integrating technological innovation, policy reforms, and

capacity building, India can establish a resilient cybersecurity ecosystem capable of safeguarding its critical assets against evolving threats and ensuring long-term national stability and growth.

References

[1] Ghosh, S. (2022, September 15). *Securing India's critical infrastructure: Biggest challenges and how to overcome them*. ETCISO. https://cio.economictimes.indiatimes.com/news/strategy-and-management/securing-indias-critical-infrastructure-biggest-challenges-and-how-to-overcome-them/94219128

[2] Chakraborty, A., & Tiwari, S. (2025). An analytical study on challenges and gaps in India's cyber security framework. *International Journal of Criminal, Common and Statutory Law*, 5(1), 4–7. https://www.criminallawjournal.org/article/110/5-1-3-412.pdf

[3] Singh, N., Buyya, R., & Kim, H. (2024). Securing cloud-based Internet of Things: Challenges and mitigations. *Sensors*, 25(1), Article 79. https://doi.org/10.3390/s25010079

[4] Recorded Future. (2022, April 6). *Continued targeting of Indian power grid assets by Chinese state-sponsored activity group*. https://www.recordedfuture.com/research/continued-targeting-of-indian-power-grid-assets

[5] Press Information Bureau. (2025, March 28). *Government of India taking measures to protect critical infrastructure from cyber threats*. Ministry of Electronics and Information Technology. https://pib.gov.in/PressReleasePage.aspx?PRID=2116341