NOTES AND COMMENTS

POWER SECTOR PERIL: UNMASKING THE THREATS OF CYBER SECURITY

Abstract

The paper has attempted to provide a comprehensive overview on cybersecurity in the Indian power sector. It highlights the critical role of a stable and reliable electricity supply in the Indian economy. It further explores the current state of cybersecurity; addressing various challenges, vulnerabilities and potential consequences of cyber-attacks. Based on the recent cyber-attacks on the country, the paper emphasizes on the urgent need for robust measures. The power sector in India can fortify its cybersecurity defences, safeguard its critical infrastructure, sensitive data including customer information if these measures are adopted. The paper highlights these measures specifically for the Indian power sector. The paper concludes while emphasizing on the need for a proactive and holistic approach to cybersecurity which would ensure a secure and resilient power infrastructure for India's economic growth and overall development.

I Introduction

INDIAN POWER system is the second largest synchronous grid in the world, the third largest producer and fourth largest consumer of electricity in the world.[1] The power sector in India holds immense importance due to its pivotal role in driving the country's economic growth and development.[2] It serves as the backbone of various industries, including manufacturing, agriculture, healthcare, information technology, and telecommunications. Reliable and affordable energy supply enables these sectors to function effectively which in turn leads to development of the entire nation. One of the key reasons why the power sector is crucial in India is its impact on economic growth. Reliable and uninterrupted power supply is essential for industrial activities and manufacturing processes. Industries such as automobile, textiles, pharmaceuticals, and information technology rely heavily on electricity to operate machinery and equipment. A consistent power supply ensures smooth production processes, enhances productivity, and promotes overall economic development.

---

1 Editor, "Smart Grid: Vision for India", *Electrical India*,(Dec. 4, 2019), *available at:* https://www.electricalindia.in/smart-grid-vision-for-india/(last visited on Jan 12, 2024).

2 World Energy Outlook Special Report, "India Energy Outlook 2021", 8th Annual Global Conference on Energy Efficiency (2021), *available at:* https://www.iea.org/reports/india-energy-outlook-2021 (last visited on Jan.12, 2024).

Power sector also plays a critical role in agricultural activities. Agriculture not only employs more than 50% of Indian population[3] but also ensures food security in the country. Access to electricity is crucial for activities like irrigation, mechanization and post-harvest processing. Electric pumps and motors are used for drawing water from wells and irrigating fields, leading to increased agricultural productivity. Electricity is also used for storage and preservation of harvested crops which helps in reducing post-harvest losses. By providing reliable power supply to the agricultural sector, the power sector contributes to improving farmers' livelihoods and overall food production. No doubt subsidy on electricity has been a game changer for many political parties as it ensures a reliable vote bank.[4]

The power sector plays a crucial role in providing essential services to individuals as well as communities at large. Electricity lights homes, powers appliances, smoothens running of essential services like hospitals, schools, and public transportation systems. It enables access to education, healthcare, and communication facilities, thereby improving life quality for people in all walks of life. Reliable electricity supply is particularly crucial in remote and underprivileged regions, where access to basic amenities can be challenging. The power sector, through its infrastructure development and electrification initiatives, aims to bridge the gap and ensure equitable access to electricity for all. Infact, universalization of energy access was an important mandate of the Act of 2003. Though, even today 45% of the rural population is without electricity, India has come a long way in terms of ensuring electricity 24 into 7 to its people at a subsidized rate.[5]

With the recent emphasis on climate change and green energy, power sector in India is actively contributing to sustainable development and environmental conservation. The shift towards renewable energy sources such as solar, wind, and hydropower is reducing the dependence on fossil fuels and lowering carbon emissions. This transition aligns with global commitments to mitigate climate change and promotes a cleaner and greener energy future for India.With importance of this gravity; finally, India is able to generate sufficient amount of energy. From a power deficit, India has finally turned into power surplus nation.[6] From 2014 to 2021, India added power generation

3 Department of Agriculture, Cooperation & Farmers' Welfare, Ministry of Agriculture and Farmers' Welfare, Government of India, "Annual Report 20-21", *available at*: /https://agricoop.nic.in/Documents/annual-report-2020-21.pdf (last visited on Jan. 15, 2024).

4 Tongia,Rahul, *Delhi's Household Electricity Subsidies: Highly Generousbut Inefficient?* (Brookings India IMPACT SeriesNo. 042017, 2017).

5 P. C Maithani and Deepak Gupta, *Achieving Universal Energy Access in India: Challenges and the Way Forward* (SAGE Publications Pvt. Ltd., 1st edn., 2020).

6 PTI, "Peak power demand deficit almost wiped out, in 2020-21, says Union power ministry", *Economic Times*, Nov. 8, 2021, *available at*: https://economictimes.indiatimes.com/industry/energy/power/peak-power-demand-deficit-almost-wiped-out-in-2020-21-says-union-power-ministry/articleshow/87586640.cms (last visited on Apr. 12, 2023).

capacity of 160.8 GW, consisting of 83920 MW from fossil fuels while 76, 900 MW were from renewable sources.[7] Ministry of power is one of the most promising ministries in the Indian government.

In India, power is generated at three levels, centre, states and private. Private sector has the largest share of around 50% (2,10,278 MW), while the centre and states have 24% (1,00,005MW) and 25.5% (1,05,726) MW respectively (CEA. 2023).[8] Most of the energy is generated from fossil fuels. Though India has become a power surplus nation, power distribution is not equal, especially the areas in the north eastern part of the country face energy deficit. As discussed already, almost half of the rural population is without electricity. Universalization of sustainable energy at cost effective prices is still a dream. Though a lot of progress has been achieved in case of rural electrification, the quality of supply is still questionable.[9]

In the recent years, the power sector has witnessed a significant transformation with the adoption of digital technologies and the integration of advanced systems.[10] This digitalization has brought innumerable benefits which has improved efficiency, enhanced monitoring and control capabilities and boosted energy management of the power sector. The number of connected devices (*e.g.* smart thermostats and appliances) are growing rapidly, with the global stock projected to double over the next five years to reach 30-40 billion devices by 2025.[11] Automation of the critical infrastructure, smart grid mission have not only given the technological edge to Indian power sector but have also immensely increased the risks of cyber-attacks.Like many other critical infrastructure sectors in the country, even power sector is becoming increasingly vulnerable to cyber threats. According to Global Risks Report 2020 Cyber-attacks are among the top ten global risks in terms of likelihood and impact.[12]

---

7 Ministry of Power, Government of India, "CEA Power Sector at a Glance ALL India", 7(2023), *available at*: https://powermin.gov.in/en/content/power-sector-glance-all-india (last visited on April 12, 2023).

8 *Ibid.*

9 Mishra Prachee, "Overview of Power Sector"*PRS India policy analytical reports* (Sep., 2019). *available at:* https://prsindia.org/files/policy/policy_analytical_reports/Overview_of_the_Power_Sector_final_web.pdf(last visited on April 18, 2023).

10 PIB, "India's Power Sector Transformation: A Journey Towards Sustainable Energy and Universal Access", June 08, 2023, *available at:* https://pib.gov.in/FeaturesDeatils.aspx?NoteId=151483&ModuleId%20=%202 last visited on (June 21, 2023).

11 International Energy Agency, "Digitalization brings many benefits to the electricity system, but raises risks to cybersecurity"*, available at:* https://www.iea.org/reports/power-systems-in-transition/cyber-resilience(last visited on May 15, 2023).

12 World Economic Forum in partnership with Marsh and McLennan and Zurich Insurance Group, "The Global Risks Report 2020 Insight Report", (15th edn., 2020), *available at:* https://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf (last visited on Feb. 15, 2024).

With the rapid integration of information technology and automation systems in power generation, transmission, and distribution processes, the sector has become more interconnected and exposed to various cyber risks. The vulnerability of the power sector to cyber threats stems from several factors. One of the prime reasons are its reliance on complex networks, increasing use of digital control systems and the potential for significant economic and societal impact in the event of a cyber-attack. (Importance of power sector in boosting Indian economy has already been discussed in detail).

One of the primary reasons for the vulnerability of the power sector is its extensive reliance on interconnected networks.[13] Power generation and distribution systems are connected through a vast network of computers, communication systems, and sensors, allowing for efficient monitoring and control. However, this interconnectedness also creates potential entry points for cyber attackers. A successful cyber-attack on a single point in the network could propagate through the system, disrupting operations, and could cause widespread power outages.

Another major factor contributing to the vulnerability of the power sector is increasing use of digital control systems.[14] As power infrastructure becomes more automated and digitized, control systems and supervisory control and data acquisition (SCADA) systems are used to monitor and control power generation and distribution processes. While these systems enhance efficiency and reliability, they also introduce vulnerabilities that can be exploited by cyber attackers. Inadequate security measures, unpatched software vulnerabilities, and insufficient network segmentation can leave these control systems susceptible to unauthorized access and manipulation.

The potential impact of a cyber-attack on the power sector is significant, both in terms of economic and societal consequences. Power outages can disrupt essential services, impact industrial operations, and cause financial losses for businesses and individuals. Moreover, prolonged power outages can lead to public unrest, affecting the daily lives of citizens and creating social and economic disruptions. The recent attacks on the Indian power grid in Ladakh have garnered national security interest.[15] A ransomware gang Hive, recently hacked important data from Tata Power and

13 Justinas Jasiûnas, Peter D. Lund, Jani Mikkola, "Energy system resilience – A review" 150 *Renewable and Sustainable Energy Reviews*(111476, 2021), *available at*: https://www.sciencedirect.com/science/article/pii/S1364032121007577(last visited on May 25, 2024).

14 International Energy Agency, "Electricity Security matters more than ever", *Report on Power Systems in Transition, available at:* https://www.iea.org/reports/power-systems-in-transition/electricity-security-matters-more-than-ever (last visited May 30, 2024).

15 Outlook Web Desk, "Report Says Chinese Hackers Targeted Indian Power Grid, Govt Says Attacks Didn't Succeed", *Outllook India*, (Apr. 8, 2022) *available at:* https://www.outlookindia.com/national/report-says-chinese-hackers-targeted-indian-power-grid-govt-says-attacks-did-not-succeed-news-190593 (last visited Mar. 10, 2024).

leaked it on dark web.[16] Recent attacks in the Madhya Pradesh Power Management Company Limited (PMCL) were so grave that IT team from Delhi was called for audit. Emails of top officers were hacked creating a buzz even at the national capital. Earlier the server of the company was also hacked which brought the online services to a standstill. Such attacks have necessitated a strong need for cybersecurity laws exclusively for the power sector.

Power sector organizations collect and process vast amounts of data related to power generation, consumption patterns, billing information, and customer details. This data is not only valuable to the organization itself but also to potential cyber attackers.[17] Breaches of sensitive data can lead to financial fraud, identity theft, and compromise the privacy of individuals. A successful cyber-attack can erode public trust in the reliability and security of the power sector, leading to reputational damage and potentially hindering investments in the sector.

The dynamic nature of cyber threats thus necessitates a proactive approach to cybersecurity in the power sector.[18] Regular risk assessments, vulnerability scanning, and penetration testing are crucial to identify and address potential weaknesses in the system.[19]Additionally, ongoing monitoring of network traffic, anomaly detection, and incident response capabilities would also enable timely detection and mitigation of cyber threats.[20]

Thus, the significance of cybersecurity in the power sector cannot be ignored. It is essential for safeguarding critical infrastructure, preventing disruptions in power supply, protecting sensitive data and maintaining stakeholder trust. By implementing robust cybersecurity measures, regularly assessing risks, and fostering a culture of cybersecurity,

16 Mathur Shubhangi, "Amid Rising Cyberattacks on Utilities, Is India Geared Up to Protect Strategic Assets?*", Moneycontrol*, (Oct. 26, 2022), *available at:* https://www.moneycontrol.com/news/business/amid-rising-cyberattacks-on-utilities-is-india-geared-up-to-protect-its-strategic-assets-9381981.html (last visited Mar. 10, 2023).

17 Yuchong Li and Qinghui Liu*,* "A Comprehensive Review Study of Cyber-Attacks and Cybersecurity: Emerging Trends and Recent Developments"*,* 7 *Energy Reports*, 8176-8186 (Nov. 2021) *available at: https://www.sciencedirect.com/science/article/pii/S2352484721007289* (last visited Mar. 10, 2024).

18 Wenye Wang, Zhuo Lu, "Cybersecurity in the Smart Grid: Survey and Challenges", 57(5) *available at*: https://www.sciencedirect.com/science/article/abs/pii/S1389128613000042 *Computer Networks* (2013).

19 Rafat Leszczyna, "Standards on Cybersecurity Assessment of Smart Grid", *22 International Journal of Critical Infrastructure Protection* (Sep. 2018), *available at:* https://www.sciencedirect.com/science/article/abs/pii/S1874548216301421https://doi.org/10.1016/j.ijcip.2018.05.006 (last visited on Mar. 10, 2024).

20 Giuseppe Settanni, *et.al*.,"A Collaborative Cyber Incident Management System For European Interconnected Critical Infrastructures", 34(2) *Journal of Information Security and Applications* (166-182, June 2017), *available at* https://www.sciencedirect.com/science/article/abs/pii/S2214212616300576 (last visited on Mar. 08, 2024), *available at:* https://doi.org/10.1016/j.jisa.2016.05.005.

the power sector in India can effectively mitigate the risks associated with cyber threats and ensure the reliable and secure operation of power infrastructure.

II Overview of cybersecurity in the Indian power sector

According to the International Energy Agency (IEA), cybersecurity in the power sector can be defined as the "ability to prevent or defend against cyber-attacks and cyber incidents, preserving the availability and integrity of networks and infrastructure and the confidentiality of the information these contain".[21] According to the Indian Computer Emergency Response Team (CERT-In) cyber-attacks saw a four-fold jump in 2018 and recorded an 89 per cent growth in 2019.[22] When it comes to cybersecurity in the power sector, India faces unique challenges due to its large size, diverse geographic landscapes and evolving digital landscape. As the country continues to expand its power infrastructure and delve more into smart grids, it becomes need of the hour to prioritize cybersecurity for reliable and secure operation of the sector. This section in detail discusses the current status of cybersecurity in the energy sector.

The data from CERT shows that compared to other sectors, the energy sector has faced comparatively less cyber-attacks.[23] But this is not good news for the sector as the cyber criminals have now focussed their attention on this yet untouched sector. It was not because of advanced secured systems that this sector was saved but because other sectors seemed more rewarding.

Most of the cyber-attacks have been on IT firms but the trend is now shifting towards power sector as well. India has many legislations regulating the power sector. The most prominent is the Electricity Act, 2003. It is the most comprehensive and exclusive legislation for power sector and consolidates all laws relating to generation, transmission, distribution, and use of electricity. Being almost two decades old it hardly mentions anything about cybersecurity. Consequently, the Electricity Amendment Bill, 2022 has been placed in the house ensuring provisions for inspection of the national electricity grid for maintaining cyber hygiene in the network.[24] The union

21 International Energy Agency, "Enhancing cyber resilience in electricity systems" (Apr. 2021) *available at:* https://www.iea.org/reports/enhancing-cyber-resilience-in-electricity-systems (last visited on May 20, 2023).

22 Niti Kiran, Beware! Cybersecurity attacks in India grew 194% in 2020, *Business Today*, (Mar. 23, 2021), *available at*: https://www.businesstoday.in/latest/economy-politics/story/beware-cyber-security-attacks-in-india-grew-194-in-2020-291535-2021-03-23 (last visited on Apr. 4, 2023).

23 CERT-In, "India Ransomware Report 2022", (August 2022, at 4), *available at* https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2022.pdf. (last visited on Jan. 6, 2024).

24 PTI, "India's Electricity Grid to Be More Future Ready, Insulated from Cyber Attacks Soon: RK Singh"*The Economic Times*, (Sep. 1, 2022), *available at*: https://economictimes.indiatimes.com/industry/energy/power/indias-electricity-grid-to-be-more-future-ready-insulated-from-cyber-attacks-soon-rk-singh/articleshow/93931057.cms?from=mdr (last visited on Jan. 06, 2024).

power minister confirmed that India is facing various kinds of cyber-attacks in its transmission system.[25] But with the rising cyber threats, National Cybersecurity Policy (NCSP) was formally announced in 2013. It is a comprehensive framework established by the Indian government for guiding and regulating efforts to safeguard the nation's cyberspace from cyber threats. The vision of the policy is to build a secure and resilient cyberspace for citizens, businesses and government.[26]

Though India was one of the few countries which formulated a cybersecurity policy in 2013, not much has transpired in terms of a coordinated cyber approach. Unlike the United States, Singapore, and the United Kingdom where there is a single umbrella organisation dealing in cybersecurity, India has 36 different central bodies, most ministries have their own department which deals with their specific cyber issues. Each department has its own different reporting structure. Each state government has its own Computer Emergency Response Team (CERT). Thus, there is no integration of cyber issues in the country. The policy nowhere in the entire document mentions about power sector. This shows the pity state as well as under estimation of power related cyber-attacks in the country.

The policy also led to the establishment of the National Critical Information Infrastructure Protection Centre (NCIIPC) and the Indian Computer Emergency Response Team (CERT-In).

CERT-In responds to cyber threats, but time and again it has been late in conducting security checks, and often has released advisories once an attack has taken place.

Another important legislation saving the Indian cyberspace from various attacks; is the Information Technology Act. Enacted in 2000, this act is the key legislation governing cybersecurity in India. It provides legal recognition for electronic transactions, establishes offenses related to unauthorized access, hacking, and data breaches, and outlines penalties for cybercrimes.[27] The IT Act also empowers the Indian Computer Emergency Response Team (CERT-In) to coordinate cybersecurity efforts and respond to cybersecurity incidents. The Act also contains provisions related to cybersecurity and data protection. It empowers the government to prescribe rules and regulations

25 PTI, "India's Electricity Grid to Be More Future Ready, Insulated from Cyber Attacks Soon: RK Singh" *The Hindu, available at:* https://www.thehindu.com/news/national/indias-electricity-grid-to-be-more-future-ready-insulated-from-cyber-attacks-soon-union-power-minister/article65836339.ece(last visited on Jan.16, 2024).

26 Ministry of Electronics and Information Technology, Government of India, 'National Cybersecurity Policy', (2013), *available at*: https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf (last visited on Jan. 20, 2024).

27 Legislative Department, Ministry of Law, Justice and Company Affairs, " National Cybersecurity Policy (2013), *available at:* https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY (last visited on Feb. 16, 2024).

for securing electronic records and protecting computer systems and networks from hacking or any unauthorized access. One of the most confrontational features of the act is that it gives power to the government for issuing directions to intercept, monitor, or decrypt information in the interest of national security.

The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) was set up as one of the prime objectives of NCSP. It is a part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY) for creating a secure cyber space by detecting botnet infections in the country and notifying the same.[28] It enables cleaning and securing systems of end users thus preventing further infections. It operates with close coordination and collaboration with Internet Service Providers (ISP) and product/antivirus companies. This centre is being operated by the Indian Computer Emergency Response Team (CERT-In) under provisions of section 70B of the Information Technology Act, 2000.The National Critical Information Infrastructure Protection Centre (NCIIPC) is an organization of the Government of India created under section 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on January 16, 2014.[29] It is designated as the National Nodal Agency in respect of Critical Information Infrastructure Protection.

National Electricity Policy is the document that outlines the overall framework for developing India's electricity sector. The policy was first formulated in 2005 and was later revised in 2018. The key features of the policy were in consonance with the Act and aimed at rural electrification, sustainable and efficient energy distribution, transmission and generation. Recently, The Government of India established the National Smart Grid Mission (NSGM) in 2015 for planning and monitoring the implementation of smart grid policies and programs in India. The main goal of smart grids is to improve the reliability of power grids and make the grid suitable for the input of renewable energy through distributed generation.

From the cybersecurity perspective, the most crucial guidelines were released by Central Electricity Authority (CEA) in 2021.

The CEA (Cybersecurity in Power Sector) Guidelines, 2021 are first in the country to acknowledge the fact that the gap myth between the Information Technology (IT) and Operational Technology (OT) systems now stands shattered. Accordingly, six CERT's have been created. Each CERT would have its own Cyber Crisis Management Plan (C-CMP) to counter cyber-attacks and cyber terrorism.

28 Ministry of Electronics and Information Technology, Government of India, 'Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)', *available at*: https://www.csk.gov.in/ (last visited on May 10, 2023).

29 National Critical Information Infrastructure Protection Centre (NCIIPC) is an organization of the Government of India created under s. 70A of the Information Technology Act, 2000 (amended 2008), through a gazette notification on Jan. 16, 2014 based in New Delhi, India, *available at*: https://nciipc.gov.in/(last visited on May 4, 2024).

Various organizations and industrial associations in India have developed cybersecurity best practices and standards. For instance, Indian Standard on Information Security Management Systems (ISMS) has been published by the Bureau of Indian Standards (BIS) for cybersecurity. These best practices and standards provide guidelines for organizations to implement effective cybersecurity measures. ISMS continuously monitors and prevents risks related to information security and improves information security processes and strategies.[30] It also helps the organizations in managing information risks such as cyber-attacks, hacks, data leaks or theft.Complying with industry standards such as ISO/IEC 27001 and the NIST Cybersecurity Framework would also ensure baseline cybersecurity.

India has made strides in building cybersecurity capacity through above mentioned initiatives. The cybersecurity strategy 2020, prepared by Data Security Council of India (DSCI) in detail mentions strengthening people, structure, processes and capabilities.[31] It further mentions about skill development programs, training, and academic courses. Numerous government agencies, academic institutions, and private organizations offer cybersecurity training and certification programs to create a skilled workforce. Collaboration between different institutions would also enable each other to learn from mistakes and have a better and safe policy for all.Establishment of sector-specific Computer Emergency Response Teams (CERTs) also contributes to more enhanced cybersecurity capabilities. Importance of having well defined policies and procedures certainly play a significant role in reducing cyber threats.

III Comparative analysis with respect to European Union, United States, Singapore and Russia

For addressing cyber risks, countries around the globe are implementing various measures to enhance cybersecurity in their respective power sectors. This section, in detail, focuses on exploring the robust measures implemented by various countries for strengthening cybersecurity in their power sectors. The analysis will consider the efforts undertaken by the European Union (EU), United States (US), Singapore, and Russia. By examining the approaches of these countries, India can make a better and more secured cyberspace. Following are the best practices of the above-mentioned countries respectively.

---

30 Bureau of Indian Standards, 'Information Security Management Systems', *available at:* https://www.bis.gov.in/system-certification-overview/certification-process/systems-under-certification/information-security-management-systems/(last visited on Jan. 16, 2024).

31 Data Security Council of India (DSCI), 'DSCI Strategy 2020', *available at* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://beta.dsci.in/files/content/knowledge-centre/2023/National-Cyber-Security-Strategy-2020-DSCI-submission.pdf (last visited on Mar. 4, 2024).

European Union

The EU has implemented the Network and Information Security Directive (NIS-2 Directive)[32] which sets security and reports incident requirements for operators of all essential services; including the power sector. The European Union Agency for Cybersecurity (ENISA) provides guidelines and standards to enhance cybersecurity across member states.[33] ENISA has its own cyber crisis management structure often referred as 'CyCLONe'. It also fosters information sharing and collaboration, conducts specified exercises, and promotes research and innovation in cybersecurity.It plays a vital role in implementation of the NIS Directive by providing assistance to the member states regarding its transposition. It supports several working streams of the cooperation group, provides them with technical expertise and also provides the secretariat for the CSIRTs Network. It also organizes cyber exercises across pan Europe.

United States

The United States has the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards.[34] These standards establish cybersecurity requirements for power sector entities for ensuring the reliability and security of the electric grid in the country. The main objective of NERC is to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets (computers, software and communication networks) that support those systems.[35]Often regarded as America's Cyber Defense Agency, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for safeguarding critical infrastructures.[36] It offers resources, reports incidents and provides guidance on specific issues to the American power sector. It is one stop solution for reporting cyber-crimes in the entire country. Often collaborating with FBI, CISA releases guidelines to save United States from cyber crisis.

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a voluntary framework of cybersecurity best practices for organizations,

---

32 Directive (EU) 2022/2555 of the European Parliament and of the Council of December 14, 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)". *available at*: https://www.nis-2-directive.com/.

33 ENISA, 'Cybersecurity Policy', *available at:* https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new(last visited on Jan. 21, 2024).

34 North American Electric Reliability Corporation (NERC), *available at:* https://www.nerc.com/pa/Stand/Pages/Cyber-Security-Permanent.aspx (last visited on Jan. 02, 2024).

35 *Ibid.*

36 United States Government, 'Cybersecurity and Infrastructure Security Agency', *available at:* https://www.cisa.gov/ (last visited on June 21, 2023).

including power utilities.[37] Although it was voluntary in nature initially, after the passage of Executive Order 13800, (Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure), Framework became mandatory for United States federal government agencies, several federal, state, and foreign governments and insurance organizations. Some organizations may also require use of the framework for their customers or within their supply chain or specific purposes. All these make American power sector quite safe from cyberattacks.

Singapore has the Cybersecurity Act, which establishes a regulatory framework for the protection of critical information infrastructure (CII) sectors, including the power sector. CII owners are required to adhere to cybersecurity obligations and incident reporting.

Singapore

The Cyber Security Agency of Singapore (CSA) is responsible for overseeing national cybersecurity efforts and collaborates with CII sectors, including the power sector, to enhance cybersecurity capabilities.[38] According to the report published by the Singapore Cyber Landscape (SCL) with the help of efficient working system, Singapore has reduced its ransomeware attack to 132 in 2022 from 137 in 2021.[39] Improve in the local cyber hygiene and collaboration between various stakeholders led to these results.

Singapore thus focuses on promoting more cybersecurity awareness, conducting regular exercises, providing resources and guidance to organizations and more collaborative approaches for reaching such desired results. Singapore has also signed Cybersecurity Awareness Alliance with various countries.

Russia

Russia is a country, notoriously famous for its cybercrime as well as cybersecurity. From the damage done by NotPetya or attacks against Ukraine and Georgia, to Russia's hacking and leaking operations in US and European elections, Russia's offensive

37 National Institute of Standards and Technology (NIST), *available at:* https://www.nist.gov/cyberframework and https://www.nist.gov/cyberframework/frequently-asked-questions/framework-basics#basics(last visited on Jan. 2, 2024).

38 Cyber Security Agency of Singapore (CSA), *available at:* https://www.csa.gov.sg/ (last visited on Jan. 2, 2024).

39 Cyber Security Agency of Singapore (CSA) 'Phishing and Ransomware Continue to Pose Significant Risks to Organisations and Individuals Drop Seen in Number of Infected Infrastructure', Jan. 23, 2024, *available at:* https://www.csa.gov.sg/News-Events/Press-Releases/2023/phishing-and-ransomware-continue-to-pose-significant-risks-to-organisations-and-individuals-drop-seen-in-number-of-infected-infra(last visited on Jan. 30, 2024).

operations are consistent threat.[40] Russian cyber attacks have made news worldwide but the thing to learn from the country is that it has saved its power sector particularly from such attack. There is no specific cyber security legislation in the country. The Federal Law of July27, 2006 No. 149-FZ on information, information technologies and protection of information establishes the general regulations on the use of IT and information security, regulations applicable to search engines and messengers, website blocking tools, restrictions on the use of VPN, and other regulations on online activities.[41]

The country seems to have its own set of cybersecurity regulations and requirements for critical infrastructure sectors, including the power sector. The Federal Security Service (FSB) of Russia plays a crucial role in overseeing cybersecurity in critical infrastructure sectors, including the power sector.[42] Russia has also developed the State System called RUnet for detection, prevention and elimination of all the consequences of cyber attacks on the Russian Federation's Information Resources (GosSOPKA).[43] The main aim of GosSOPKA is detecting and preventing cyber attacks targeting the Russian information resources.

All these countries have their varied mechanisms of dealing with cyber crimes particulary in the power sector. With the best practices of each, India can certainly learn to make its cyber space more secure. Also with implementation of the recent CEA guidelines India would soon be in a position to teach other countries about the nitty gritties of cybersecurity as well.

IV Vulnerabilities in the Indian power sector

According to a report by McKinsey Global Institute, India is the second-fastest digital adopter among the seventeen most digital economies of the world.[44] India's core digital sectors accounted approximately for about $170 billion which is around seven

40 Janne Hakala and Jazlyn Melnychuk, NATO Strategic Communications Centre of Excellence, NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), "Russia's Strategy in Cyberspace" at 4, *available at* chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_15-06-2021.pdf (last visited on Jan. 30, 2024).

41 Natalia Gulyaeva *et.al.*, "Russia: Cybersecurity", Sep. 2022, *available at* :https://www.dataguidance.com/opinion/russia-cybersecurity (last visited on Jan. 21, 2024).

42 Center for Strategic and International Studies (CSIS), 'Significant Cyber Incidents', available at https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents (last visited on Jan. 30, 2024).

43 Ilona Stadnik, Internet Governance Project, "Sovereign Runet: What Does it Mean?", *available at:* https://www.internetgovernance.org/wp-content/uploads/IGPWhitePaper_STADNIK_RUNET-1.pdf (last visited on Jan. 2, 2024).

44 Noshir Kaka *et. al,* "Digital India: Technology to Transform a Connected Nation", *McKinsey Global Institute*(Mar. 27, 2019), *available at*: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-india-technology-to-transform-a-connected-nation (last visited on Jan. 4, 2024).

percent of GDP in 2017–18. This is further expected to grow eight to ten percent of the GDP by 2025.[45] The power sector faces a range of unique cybersecurity challenges due to its reliance on interconnected systems, industrial control systems (ICS) and smart grid technologies. These challenges stem from the increasing digitization and interconnectivity of power systems, which have opened up new avenues for potential cyber-attacks. Understanding these challenges is crucial for developing effective cybersecurity strategies and implementing appropriate countermeasures. This section in detail discusses various types of vulnerabilities which are as follows:

(i) *Industrial Control Systems* (ICS): ICS are critical components of power systems which are responsible for monitoring and controlling of various processes. They are a very crucial part of the critical infrastructure. ICS in the power sector comprises control systems that automate and regulate generation and distribution of power. These systems include components such as Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), and Supervisory Control and Data Acquisition (SCADA).

Originally, ICS implementations were susceptible primarily to local threats because many of their components were in physically secured areas and the components were not connected to IT networks or systems.[46] While designing these systems, emphasis was more on functionality rather than on security. However, integration of the ICS systems with IT networks provided comparatively less isolation to ICS from the outside world and created a greater need to secure these systems from remote, external threats.

Hence these are more vulnerable to cyber-attacks. Cybercriminals exploit these susceptibilities in ICS for gaining unauthorized access, manipulating control settings and disrupting the operation of power infrastructure. Attacks on ICS is blurring the lines between cyber and physical attacks, prompting national security concerns in many countries.[47]

(ii) *Interconnected Systems:* The power sector relies on a complex network of interconnected systems for the generation, transmission, and distribution of electricity. These systems, including supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS) are often connected to the internet and vulnerable to cyber threats.[48] As SCADA is a combination of hardware and software which enables real-time data collection, visualization,

45 *Supra* note 31.

46 *Ibid.*

47 Steve Livingston *et.al.*, "Managing Cyber Risk in the Electric Power Sector"(Jan, 31, 2019), *available at:* https://www.deloitte.com/global/en/our-thinking/insights/industry/power-utilities-renewables/cyber-risk-electric-power-sector.html (last visited on Feb. 16, 2024).

48 T. Halder, 'A cybersecurity for a smart grid,' 2014 6th IEEE *Power India International Conference (PIICON)*, Delhi, India, 1-6 (2014), *available at*: 10.1109/POWERI.2014.7117705. (last visited on Mar. 15, 2024).

as well as control of the power processes, its manipulation can severely affect the power generation. There are basically three main components of SCADA namely,

i. Supervisory Control,

ii. Data Acquisition and

iii. Human-Machine interface.

Attackers might strike at any of the component and cause massive damage to the entire system. Any compromise in one part of the system can potentially propagate across the network which may lead to cascading effects and widespread disruptions eventually.

Even DCS plays a crucial role in managing and controlling the generation, transmission, and distribution of electrical power. It integrates different control functions and allows operators to monitor and regulate various equipment and processes in real-time. DCS systems log and store historical data. This data can be further analysed for trouble shooting, maintenance planning, evaluation of various performances as well as for regulatory compliance purposes.[49] Manipulation with DCS would does hamper the efficient working of the entire power system.

(iii) *Legacy Systems and Infrastructure*: Legacy systems and infrastructure refer to outdated or obsolete technologies, software, and hardware that are still in use within an organization or industry. Once considered as state-of-the-art, these systems fall an easy prey for cyber-attacks. They pose several challenges like security vulnerabilities, compatibility issues, limited functionality, maintenance and support challenges. The main challenge lies in securing these legacy systems while ensuring their compatibility with newer technologies and security protocols. Vulnerabilities in legacy systems can provide entry points for attackers to gain unauthorized access, disrupt operations, or manipulate critical infrastructure.

(iv) *Advanced Persistent Threats (APTs)*: As the name suggests, Advanced Persistent Threats (APTs) are a type of sophisticated and stealthy cyber-attack which focuses on specific organizations or sectors over an extended period. They differ from typical cyber-attacks as they are persistent and targeted. instead of a one-time attack, APTs aim to gain prolonged access to a target's systems, often remaining undetected for extended periods, at times even months or years. APT actors use highly advanced techniques and at times compromise at initial levels for bigger gain in the future.

---

49 Mangesh M. Ghonge (ed), "Security Improvement Technique for Distributed Control System (DCS) and Supervisory Control-Data Acquisition (SCADA) Using Blockchain at Dark Web Platform", *Cybersecurity and Digital Forensics* 317-333, (Scrivener Publishing LLC, Jan. 2022), *available at*: https://doi.org/10.1002/9781119795667.ch14 (last visited on Jan. 20, 2024).

APTs often employ advanced techniques like zero-day exploits, custom malware, and social engineering tactics to evade detection and gain prolonged access to systems.[50] According to report by IDSA, thirty- eight percent of the APT vectors like APT40, APT3, APT10 and APT17 have been reported to be developed and deployed by China for espionage, stealing of data and IP.[51] These vectors might cause massive upveals not only in the power sector but can affect entire Indian economy. Some APTs are general purpose tools but others are customised for specific countries and purposes. The Indo-Chinese rivalry ranges from geographic to economic and now to digital field as well. The techniques and tools like APT1, APT3, APT10, APT15, APT17, APT26, etc. have been deployed against India as well.[52]

(v). *Ransomware Attacks*: Ransomware attacks have become a significant concern for the power sector. Attackers use malicious software to encrypt critical data or systems and demand ransom payments in exchange for restoring access. These attacks can lead to operational disruptions, financial losses, and potential safety risks if they affect control systems responsible for power generation or distribution. There are different types of ransomware, including encrypting ransomware and locker ransomware. Encrypting ransomware does the job of encrypts files, while locker ransomware locks the victim out of their system in totality, thus preventing access to the operating system or important files. Ransomware attacks are usually launched by criminal organizations for seeking financial gain or by nation-state actors to disrupt infrastructure.

Recently a malware was detected in Nuclear Power Corp of India Limited (NPCIL) system but the government owned body claimed that none of the information was compromised.[53] NPCIL designs, constructs and runs nuclear power reactors in the country. The installed capacity is around 6,780 megawatts.[54] The malware was detected in the Russian built reactors in

50 Amit Sharma *et.al* , "Advanced Persistent Threats (APT): Evolution, Anatomy, Attribution and Countermeasures", *Journal of Ambient Intelligence and Humanized Computing pages 9355–9381 (2023)* (May 6, 2023), *available at:* https://link.springer.com/article/10.1007/s12652-023-04603-y(last visited on May 30, 2023).

51 Krutika Patil, "Chinese Targeted Cyber Operations against Taiwan: Key Takeaways for India", *Manohar Parikkar Institute for Defense Studies and Analysis, available at:* https://www.idsa.in/issuebrief/Targeted-Cyber-Operations-280922 (last visited on May 20, 2024).

52 Editor, "India needs to review its 2013 Cybersecurity Policy", *The Times of India,* (June 22, 2020). *Available at* https://timesofindia.indiatimes.com/india/india-needs-to-review-its-2013-cyber-security-policy/articleshow/76502600.cms (last visited on Jan. 25, 2024).

53 Reuters, "Nuclear Power Corp of India says detected malware in it System", *Livemint* (Oct. 30, 2019), *available at:* https://www.livemint.com/news/india/nuclear-power-corp-of-india-says-detected-malware-in-its-systems-11572437521678.html, (last visited on Feb. 15, 2024).

54 National Power Corporation of India Limited, *available at:* https://www.npcil.nic.in/index.aspx (last visited on May 5, 2024).

Kudunkulam. Being a state-run entity, which oversees working of around 22 nuclear power plants, this is quite threatening. According to CERT-In, these attacks have jumped 51% in the current year.[55] The recent attack in Madhya Pradesh Power Management Company Limited (MPPMCL) was also a ransomeware attack. The hackers though did not demand any cash but had given their email id's to the officials for further contact.[56] As per the government guidelines the officials were scanning the servers to restore them with precaution.

(vi) *Supply Chain Risks*: Power sector relies on a vast network of System Integrators, Equipment Manufacturers, Suppliers/Vendors, Service Providers, IT Hardware and Software Original Equipment Manufacturers (OEM's) and other contractors engaged in the Indian Power Supply System This complex supply chain adds more cyberthreats as malicious actors may exploit vulnerabilities in the supply chain to gain unauthorized access or introduce compromised components into the power infrastructure. Establishing robust supply chain security measures and conducting regular audits are essential for mitigating these risks.

(vii) *Insufficient Security Measures*: Many power sector businesses have insufficient security measures to protect their networks and systems. This includes weak or outdated firewalls, access controls, intrusion detection systems and encryption protocols. Without robust security measures, cyber attackers have a fair advantage of infiltrating networks, stealing sensitive data and causing disruptions to power outlets at generation and distribution sites. Security measures are needed both at Information Technology (IT) and Operational Technology (OT) systems. Lack of security measures make the system easy target for cyber attackers. With a little help of social engineering techniques even the most crucial and sensitive data can be stolen if the system is not updated with apt security measures.

(viii) Third-Party Dependencies: Third party vendors and System Integrators, Equipment Manufacturers, Suppliers/Vendors, Service Providers, IT Hardware and Software OEMs engaged in the Indian Power Supply System for protection of Control Systems for System Operation and Operation Management, Communication System and Secondary Automation and Tele

55 Nabeel Ahmed, "Ransomware Attacks jump 51% this year CERT-In", *The Hindu,* (Aug. 5, 2022), *available at:* https://www.thehindu.com/sci-tech/technology/ransomware-attacks-jump-51-this-year-cert-in/article65731847.ece (last visited on Feb. 26, 2024).

56 PTI, "MP: State-run Power Management Firm's IT System Hit by Ransomware Attack", *Deccan Herald* (May 28, 2023, Jabalpur), *available at:* https://www.deccanherald.com/national/north-and-central/mp-state-run-power-management-firms-it-system-hit-by-ransomware-attack-1222761.html(last visited on Feb. 2, 2024).

control technologies have been tagged as responsible entities in the CEA Guidelines 2021. If these responsible entities do not prioritize cybersecurity, it can introduce vulnerabilities into the power sector's infrastructure. For example, if a vendor's software or equipment has security flaws or backdoors, attackers can exploit it for gaining unauthorized access to the sector's networks or systems.

(ix) *Phishing and Social Engineering*: Phishing emails and social engineering techniques are commonly used by cyber attackers to trick employees into revealing sensitive information or providing unauthorized access to systems.[57] In the power sector, employees may receive emails that appear legitimate but contain malicious attachments or links. Social engineering tactics may manipulate employees into divulging their login credentials or other sensitive information. Without proper training and awareness, employees may unknowingly fall victim to these plots of the attackers thus, compromising the security of the entire network.

(x) *Lack of Awareness and Training:* Insufficient cybersecurity awareness and training among power sector employees can increase the likelihood of successful cyber-attacks. Without a strong understanding of best practices, employees may unintentionally engage in risky behavior, like clicking on fraudulent links, using weak passwords or similar passwords, or connecting unauthorized devices to the network. Regular training programs and awareness campaigns are crucial for educating employees about common cyber threats, identifying potential risks, and promoting good cybersecurity hygiene. Periodic review of policies and procedures is essential while introducing new technologies.

V Robust measures for enhancing cybersecurity in the power sector

Robust measures include a range of initiatives like regulatory frameworks, cybersecurity standards, capacity building, incident response mechanisms, information sharing and collaboration as well as public-private partnerships. These measures establish a comprehensive defence against cyberattacks, identify the pertaining vulnerabilities, respond to the incidents and build a resilient power sector. Few of the measures are as follows:

(i) *Authentication*: It is often said that the first line of defence are employees themselves. Social engineering, phishing are common tools which make humans

57 Ahmed Alzahrani, "Coronavirus Social Engineering Attacks: Issues and Recommendations" *International Journal of Advanced Computer Science and Applications (IJACSA),* 11(5), 2020), *available at:* https://pdfs.semanticscholar.org/3abffa2b63727dbcee307493fca1004e58bebfd6.pdf (last visited on Jan. 20, 2023).

the weakest link in the cybersecurity.[58] One of the most underestimated methods for cyber-resilience is authentication. It is the process of verifying the identity of users or devices who try to access critical systems in the power sector. Unique usernames, strong passwords, multifactor authentication (MFA), or even biometric authentication are few basic measures which can have huge effect in upveiling the security of the organization. These measures ensure that only authorized individuals or devices can access sensitive information and control systems and thus reduce the risk of unauthorized access or data breaches.[59] This is essential especially in a country like India, where the power infrastructure is distributed across varied geographic areas and accessed by various stakeholders

(ii) *Authorization*: After a successful authentication, authorization determines the level of access and actions that a device or a user is permitted to perform. In the power sector, implementing proper authorization controls is essential for preventing unauthorized modifications or disruptions to critical systems.[60] Importance of SCADA and DCS has already been mentioned in another section of this article. Their vulnerability can be checked if only authorized officials have access to main data. This can be done by defining user roles and permissions, regularly reviewing and updating access rights based on job roles and responsibilities and applying the principle of least privilege.[61]

(iii) *Network Segmentation:* Segmenting networks would help to isolate the critical systems from non-critical ones. This would also enhance the confidentiality of data, separating sensitive information from unauthorised access or disclosure. Power sector deals with large amount of sensitive data such as infrastructure designs, customer information, system configurations, operational data, financial records, and regulatory compliance data.

58 Chetioui *et. al*, "Overview of Social Engineering Attacks on Social Networks", *Procedia Computer Science* (198 (2022) 656-661).*available at*: https://www.sciencedirect.com/science/article/pii/S1877050921025412 (last visited on May 30, 2023).

59 National Centre for Education Statistics, "Protecting Your System: User Access Security", *Safeguarding your Technology (*CHAPTER 8) available at https://nces.ed.gov/pubs98/safetech/chapter8.asp (last visited on June 10, 2023).

60 IT and Cybersecurity Division, Ministry of Power, Government of India, Central Electricity Authority (CEA)Guidelines, "CEA (Cybersecurity in Power Sector Guidelines)", (October, 2021)available at chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://cea.nic.in/wp-content/uploads/notification/2021/10/Guidelines_on_Cyber_Security_in_Power_Sector_2021-2.pdf (last visited on May 10, 2023).

61 Techtarget, "What Is Least Privilege & Why Do You Need It?" (June 13, 2023), *available at*: https://www.beyondtrust.com/blog/entry/what-is-least-privilege *available at: https://www.techtarget.com/searchsecurity/definition/principle-of-least-privilege-POLP*(last visited on May 05, 2023).

Segmentation would lead to multiple layering thereby preventing complete mishaps by giving up entire data set in one go. Measures such as data classification, encryption, access controls, data loss prevention (DLP) can be implemented for same. This helps contain potential cyberattacks, limiting their impact and reducing the risk of cascading disruptions. DLP solutions typically involve a combination of software tools, policies, and procedures.[62]

(iv) *Risk/Vulnerability Assessment*: Conducting regular risk assessments to identify specific vulnerabilities and threats. Periodic assessments would lead to data integrity.[63] This would ensure that the data remains accurate, complete, and unaltered throughout its lifecycle. It is essential for maintaining the reliability and trustworthiness of data used for power generation, transmission, and distribution. This can be achieved by implementing data validation checks, using cryptographic techniques such as hashing and digital signatures, and employing secure data transmission protocols like Secure Sockets Layer (SSL) and Transport Layer Security (TLS) for preventing unauthorized modifications, tampering, or corruption of critical data.[64]

(v) *Compliance with industry standards*:Implementing internationally recognized standards such as ISO/IEC 27001:2021 and the NIST Cybersecurity Framework would establish a strong baseline for cybersecurity in the power sector. These standards offer systematic approaches for managing information security risks, implementing effective security controls, thus responding to severe cyber threats. Compliance involves conducting risk assessments, safeguarding critical assets, detecting and responding to incidents while ensuring timely recovery.[65] Genuine implementation of these standards would enhance the power sector's ability to protect infrastructure, data, and customer information from cyber-attacks.As these standards provide internationally recognized benchmarks for managing and mitigating cybersecurity risks; allying

62 Asaf Shabtai *et. al.*, *A Survey of Data Leakage Detection and Prevention Solutions* (Springer New York, 2012).

63 Shaocheng Wu *et.al.*, "Data Integrity Research of Power Metering Automation System" 16th International Symposium on Communications and Information Technologies (ISCIT) Conference (Sep. 2016) DOI:10.1109/ISCIT.2016.7751717, *available at:* https://www.researchgate.net/publication/310809261_Data_integrity_research_of_power_metering_automation_system (last visited on May 07, 2023).

64 IBM, "How SSL and TLS provide identification, authentication, confidentiality, and integrity, *available at:* https://www.ibm.com/docs/en/ibm-mq/7.5?topic=ssl-how-tls-provide-authentication-confidentiality-integrity (last visited on Mar. 3, 2024)

65 Douglas Landoll, *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments (*3rd edn., CRC Press, 2021).

with these will not only be beneficial for the Indian power sector but would also bring them at par with the global practices.

(vi) *Collaboration between all the stakeholders:* Effective cybersecurity strategies would require collaboration between government agencies, power sector organizations, and cybersecurity experts. This collaboration would foster information sharing on real time basis, exchange of threat intelligence and would develop coordinated incident response mechanisms for mitigating cyber-attacks. Regular training and awareness programs for power sector personnel would also play a significant role in promoting a secured environment. By working together, these stakeholders can enhance the resilience of the power sector and effectively address the evolving challenges posed by cyber threats. Industry Ransomware as a Service (RAAS) is also threatening the Indian cyberspace, proper care must be taken or else it wouldn't be long that Indian power sector might succumb to the whims and fancies of these money/ power hungry minded criminals. As mentioned earlier, Chinese hackers are targeting Indian power sector[66]. Unlike the past instances, now he state-backed hacker group Red Echo is targeting the national energy sector. Hence there is a dire need to implement all the measures at the earliest and have a stable and full-fledged cybersecurity policy for the Indian power sector.

VI Conclusion

The research paper thus provides a critical analysis of the power sector in India and its susceptibility to day by day increasing cyber-attacks. The paper emphasizes on the urgent need of implementing robust cybersecurity measures. The study found that the Indian power sector relies heavily on digital infrastructure, making it vulnerable to cyber-attacks which can have far-reaching consequences on the country's economy and national security. Recent examples were highlighted in different sections of the paper. Several challenges faced by the power sector in terms of cybersecurity, including outdated systems, a lack of awareness, inadequate regulatory frameworks, and a shortage of skilled professionals needs attention of all the involved stakeholders. As these challenges are further exacerbated by the increasing complexity and frequency of cyber-attacks there is an urgent need to oversee the structures, personnel, processes and capabilities from cyber perspective.

The encompassing ransomware attacks, APT attacks, insider threats can potentially result in power disruptions, data breaches, and disruption of critical services as has been done on foreign land. India needs to learn it from the international scenario, both the harsh effect of cyber threats as well as mechanisms to deal with it. Addressing

66 Aashish Aryan , Prabha Raghavan, ed. Explained Desk,"Explained: China's Cyber Eye and India", *Indian Express* (Mar. 4, 2021), *available at:* https://indianexpress.com/article/explained/explained-chinas-cyber-eye-and-india-7211655/ (last visited on Jan. 22, 2024).

these challenges necessitates the prioritization of cybersecurity by all stakeholders involved in the power sector (government agencies, power utilities, and regulatory bodies). As mentioned in the CEA Guidelines on cybersecurity (2021), investing in resilient security infrastructure, conducting comprehensive risk assessments, updating systems regularly and establishing effective incident response mechanisms would be the first step for a secured Indian cyberspace. Collaboration with cybersecurity experts, private sector industry partners would also lead to a secured system. The national Cybersecurity Policy submitted by Data Security Council of India (a NASSCOM initiative) shows the interest of private sector as well. Fostering knowledge-sharing platforms would contribute to enhanced ability of the sector to withstand cyber threats.

Promoting cybersecurity awareness among employees and end-users also needs to be done. Achieving this requires the implementation of various training programs, international and national workshops, campaigns all aimed to cultivate a culture of cyber hygiene and vigilance. Finally, safeguarding India's power sector against cyber threats demands a multifaceted approach that needs technological advancements, regulatory reforms, and collaborative endeavors. Adhering and updating according to the industry standards such as Indian Standard on Information Security Management Systems (ISMS)ISO/IEC 27001:2021 and the NIST Cybersecurity Framework would also ensure baseline cybersecurity. These measures would not only make India more cyber secure but would also bring it at par with other global leaders on cybersecurity. By implementing comprehensive cybersecurity measures, India can ensure the uninterrupted and secure operation of its power infrastructure, fostering sustainable economic growth and protecting national interests in an increasingly interconnected digital landscape. In this digital age, a strong cybersecurity system is only way to save from new emerging cybercrimes. Power sector holds immense significance in the life of every human being on this planet, hence cybersecurity in this sector is need of the hour

Manish Yadav[*]
Pooja Kiyawat[**]

.

* Associate Professor at National Law Institute University, Bhopal.
** Assistant Professor at National Law Institute University, Bhopal.