BOHR International Journal of Computer Science
2023, Vol. 2, No. 1, pp. 1–6
DOI: 10.54646/bijcs.2023.11
www.bohrpub.com

METHODS

Proposed arrangements and cyber security challenges in nuclear domain: An explanatory study of India

Showkat Ahmad Dar[1]* and Aadil Ahmad Shairgojri[2]

[1]Department of Public Administration Annamalai University, Chidambaram, Tamil Nadu, India
[2]Department of Political Science Annamalai University, Chidambaram, Tamil Nadu, India

***Correspondence:**
Showkat Ahmad Dar,
showkatdar0404@gmail.com

Received: 05 January 2023; **Accepted:** 18 January 2023; **Published:** 03 February 2023

The goal of cyber security is to protect the internet against online attacks. One of the most frequently used terminologies in cybersecurity is "cyber-threats," which refers to the use of information and communication technology (ICT) for hostile purposes by a range of criminals. The complexity of cyber security architecture makes higher safety measures necessary to guard against system flaws and potential global catastrophes. One of the most important security issues today is cyberattack. A cyber breach could make nuclear systems safety and security safeguards ineffective, which is especially important for nuclear systems. India, which has a sizable and developing nuclear programme, has a similar situation. Over the past few decades, governments, including India, have invested a significant amount of time and money in building effective physical safeguards for nuclear installations, which has raised the risk of a cyber or hybrid attack. The risk of hacking, disruption, or sabotage rises as nuclear infrastructure becomes more and more reliant on cyber technology. Any cyberattack's antagonistic goal is to take advantage of a system's weaknesses in order to take over, operate, and keep a presence on the target system. Designing standards that can accommodate both immediate and long-term needs is crucial due to the sensitivity of nuclear materials and infrastructure. The study's objective is to discuss the proposed arrangement of cyber security in nuclear domain in India.

Keywords: cyber, security, nuclear, malware, framework and lucanas

Introduction

India surpassed China at No. 33 and Pakistan at No. 79 in a worldwide cybersecurity rating of countries, rising to No. 10 overall. India climbed from 47th to 10th rank in the Global Cybersecurity Agenda of the International Telecommunication Union of the United Nations (GCA). A strong cybersecurity plan is required to safeguard India's citizens, government systems, and economic ecosystem. This will help protect people from cyberthreats while also boosting investor (confidence in the economy. One benefit is that it will result in more employment openings in this industry. According to a study conducted by PwC India and The DSCI, or the Data Security Council of India, the cybersecurity market in India is expected to grow significantly and reach USD 3.05 billion by 2022. The compound annual growth rate, or CAGR, would be 15.6%. Keeping data, networks, programmes, and other types of information safe from unauthorized access, erasure, and change is the aim of cybersecurity. Due to security issues and cyberattacks, cybersecurity has grown to be a major concern in the modern world. Numerous businesses (1) produce software for data protection. With the help of this software, the data will be protected.

Cybersecurity makes it simpler to defend against viral attacks on our computer system and data. India and China have more people using the internet than any other country on the planet. A good cybersecurity plan that employs (2) a defense-in-depth approach to defend systems, networks, and data can help businesses lessen their vulnerability

CC BY NC ND

to cybercrime, even though preventing it and ensuring complete internet security may not be possible. Defense-in-depth techniques are used to protect nuclear power plants from intrusions by layering security measures across the network. A hardware device that only permits data to move from high-security zones to low-security areas is one part of this strategy.

Research objectives

In order to protect against increasingly sophisticated online attacks in a digitally dependent and networked environment, cyber security must be a key component of nuclear security. The prevention, detection, and response to theft, sabotage, unauthorized entrance, illegal transfer, and other malicious acts involving nuclear material and other radioactive compounds and the facilities that store them are the focus of nuclear security. The top security experts in our nation are increasingly recognizing nuclear energy as a pillar of national security. Cybersecurity supports nuclear security. The study aims out to explore the planned arrangements and cyber security concerns in India's nuclear domain after performing a thorough review of the literature. The study also demonstrates India's cyber security tactics.

Materials and methods

Most of the content in this research study is based on information that was obtained from official government websites, such as articles, books, and official documents. An empirical approach has been used to thoroughly investigate and explain the data and the connections between them. In order to reach a fair judgment, we gathered and analyzed qualitative data. As part of this study, researchers employed direct approaches such as scientific observation and expert interviewing. Experimentation, critical analysis, and observation were used to contextualize the study's subject. These strategies have contributed new, logical information to the body of literature, which is backed up by empirical evidence. They have been used.

Discussion and outcome

In order to prevent system faults or future crises, the architecture of cybersecurity is growing more complex. Cybersecurity issues are becoming more and more prevalent. Nuclear safety and security protocols can be rendered meaningless by cyberattacks. With a developing nuclear arsenal, India, too, is no exception. India, for example, has invested extensively in nuclear physical defenses as a result of rapid technology advancements that have made cyber or hybrid attacks more likely. The likelihood of a nuclear site being hacked, disrupted, or sabotaged rises as cyber integration expands. The vulnerabilities of a system are exploited by cyberattacks in order to seize control, function, and persist. It's possible for hostile forces or cyberattackers to acquire or release nuclear or radioactive materials, as well as crucial information regarding nuclear plants and reactor designs. In light of the fact that cyberattacks might give an adversary direct physical access to a nuclear plant, their interconnectedness creates new issues. They use different levels of secrecy for military and civilian nuclear programmes in India. Given the sensitivity of nuclear materials, the nation's nuclear security system must include cybersecurity. Reviewing India's current regulatory framework and identifying any potential weaknesses in nuclear plant protection mechanisms is essential to solving the country's nuclear security issues. Historically successful cyberattacks on nuclear installations could teach India lessons for the future. Two developed countries, the United States and Japan, may share their best practices with India. Idea publications should also be consulted to improve nuclear system security. In order to prevent cyberattacks on India's nuclear facilities, there must be multiple layers of defense. policymakers and industry in India must work together to improve cyber-nuclear security measures and establish a more comprehensive national cyber-nuclear security framework as the country's nuclear infrastructure embraces cyber technologies.

Cyber-nuclear security in India

In June 2013, after the Snowden revelations, cybersecurity became increasingly crucial. After snow den's leaks, India improved its cybersecurity. India's nuclear security architecture includes cybersecurity, although the required infrastructure might not be sufficient. Hacking and infiltration are ignored by India's cybersecurity strategy. India gained notoriety in 2021 after Mumbai power disruptions were linked to a possible Chinese intrusion into its electrical system during the Ladakh conflict. India's cyberattacks increased in volume in 2020.

In 2013, India adopted its first cyber policy. Since 2008, no updates have been made. In 2020, according to Modi, a new national policy framework would be launched. Given that they are top-secret, neither the nuclear sector nor India's security architecture is mentioned in the 2013 strategy. Cybersecurity protocols are rarely discussed, much like nuclear policies. It is untrue that there are no cybersecurity precautions in India's nuclear programme. NTRO and DCA handle cyber security. Together with the (3) National critical information infrastructure protection center and the national disaster management authority, India's computer emergency response teams contribute to the security of important cyber infrastructures. NCCC coordinates information gathering

and keeps an eye on communications. CISAG "conducts routine assessments of information systems and provides guidance on avoiding cyberattacks." Analysis of the current policy framework and any potential gaps is necessary to address India's nuclear cybersecurity problems.

Cybersecurity businesses exist in India. The effectiveness of the nuclear security framework's cybersecurity laws depends on how efficiently cybersecurity, cyber infrastructure, and operating agencies are integrated. Interagency coordination is required for cybersecurity. Government organizations must update cybersecurity laws and procedures to keep up with a rapidly evolving threat environment roles, responsibilities, and backup plans for short- and long-term implementation (3) and adaptability to shifting conditions and technology are all components of effective cybersecurity policy cyber risks and cybersecurity are significant issues in India, establishing agency roles and duties, managing cyber risks and vulnerabilities, and facilitating thorough contingency planning are all requirements of a cyber-nuclear strategy.

Cyberattacks' nuclear risks

The 2021 Natanz plant attack, which disrupted centrifuge power, demonstrated the strength and intelligence of cyberspace. Such hacks are concerning even without political repercussions. The country's security measures should be strengthened, and outdated and vulnerable cybersecurity technologies, such as administrative computer networks (as in the Kudankulam incident) or nuclear facility security measures that use risky technologies, should be improved or replaced. India should also actively address upcoming risks. The nuclear aspirations of India present cyberthreats 2019 cyber assaults against ISRO in Karnataka and Kudankulam in Tamil Nadu revealed these flaws. The hack made use of a d-track variant developed by the Lazarus gang, which has ties to North Korea. This episode demonstrates the need for national cyber-nuclear security (3).

The only systems impacted were administrative ones. Malware is kept out of plant instrumentation and control using air gaps. "Computers or networks not connected to the internet" are "air gaps." according to experts, air gaps, antivirus software, and firewalls are insufficient to thwart today's dynamic attacks. A breach at Kudankulam was prevented by air gaps. Following the incident, CISAG suggested many quick and near-term steps, such as "hardening internet and administrative intranet connectivity, limiting removable media, blocking hazardous websites & Ips, etc."

Although the fact that it did not penetrate the nuclear system is positive, it raises concerns about its inadequacies and could erode public confidence in nuclear energy. In order to boost cybersecurity, long-term policy changes are required. These significant CISAG programmes are reactive. By modernizing air gaps and firewalls, national cyber-nuclear strategy can increase the resilience of nuclear facilities (3).

Lessons from the global context for cyber-nuclear security and recommendations for India

Global cybersecurity we need global solutions. To counteract cyberattacks, like-minded nations must band together. Nuclear cybersecurity protocols were devised by the US and Japan. These countries create emergency plans and online resilience strategies. India may pick up best practices for cybernuclear warfare from international allies.

Along with the UK and Russia, India might potentially develop its cyber-nuclear infrastructure. The topics include information (4) exchange, reactor design, nuclear safety, etc. India should increase cyber-nuclear collaboration given the growing importance of cybersecurity in the global nuclear ecosystem. Cooperation in technology, expert exchange, information-sharing agreements, collaborative exercises, workshops, and enhanced infrastructure for nuclear systems' security.

India ought to work with online businesses. India prohibits nuclear energy. India's nuclear fuel cycle and weapon development are under government control. Governments are in charge of nuclear security and safety. Cyber nuclear security can be educated through cybersecurity. Private actors who act dishonestly and maliciously always jeopardize cybersecurity. Industry professionals from the UK should be incorporated into India's cybersecurity policies. The cybersecurity safeguards for India's nuclear facilities must be regularly checked.[1]

Consequences of cyberattacks and their implications on nuclear security

Cyberattack severity depends on access. Enemy access to NC3 systems has complex repercussions on nuclear weapons. If an attacker breaches a nuclear weapons systems command and control infrastructure, they could launch nuclear warheads or missiles without authorization. Cyberattacks endanger nuclear weapons. Malware and viruses can enter systems across the production and supply chain. Putting codes in conventional and nuclear weapons could reduce their effectiveness. By utilizing disruptive cyberattacks, enemy can cease nuclear weapons system communication. This can impede information flow, allow them access to private information, stop dual-use communications, overwhelm vital communication networks, and prevent individuals from using communication channels to calm a situation.

Cyberattacks hurt the government in three ways: financially, in how it works, and in its reputation. Given the way nuclear systems are bought and kept up, a breach must be taken into account. A cyberattack on one part of a system shows weaknesses in the rest of the system. This means that the security methods and infrastructure need

[1] Brent Kessler, "The Vulnerabilities of Nuclear Facilities to Cyber Attack," Stanford Strategic Insights, (Spring 2011), 20.

to be reviewed in their entirety. Any safety problem makes people doubt the systems, hurts relationships with friends and foes, and makes people wonder how reliable a country's nuclear power is. Cyberthreats to nuclear systems must take into account how people might react. Nuclear systems depend on people to make decisions, so they are "prone to human fallibility." Warnings can be wrong if a person makes a mistake, either by accident or on purpose. There is also insider threat. People with different levels of security clearance run and run nuclear systems, which make them vulnerable to cyberattacks. Insider threats include making software flaws and taking advantage of them, spreading viruses, and giving important information to enemies. For nuclear security, insider threats mean that cyber security measures are also needed. Along the whole supply chain, cyber risks can affect nuclear systems, so both technology and people are needed.[2]

Context Indian

Context for India's nuclear architecture to work, it needs to have cyber security. India was named by Symantec as one of the top five countries with the most cyber risks and attacks in 2018. The Department of Electronics and IT made its first cyber security policy framework in 2013. The policy document says what the goals of a (5) cyberattack are After Snowden said that the NSA spied on Indian people because of a lack of cyber security, this policy was made. Risks and weaknesses in cyberspace are an important part of both public and private infrastructure.

The government has set up a "Defense Cyber Agency" to deal with Cyberwarfare and cyber infiltration in India's defense networks. The National Technological Research Organization (NTRO) of India is in charge of cyber intelligence and counterintelligence. The technical parts of the agency work on their own. The policy for 2013 includes best practices, setting up information standards and protocols, identifying and categorizing risk perceptions, and validating and testing cyber security measures on a regular basis. It was put in place without much thought, and there isn't much talk about how to spread it across India. The 2013 policy does not cover everything. It hasn't been changed in seven years to keep up with the growth of cybertech. CERT-In was started in 2004 and is in charge of coordinating "cyber security emergency response and crisis management." CERT-In works with other organizations around the world to improve India's cyber security.[3]

Cyber and nuclear security are missing. Cybersecurity goals and approaches are outlined. Agencies must collaborate to address SOP problems and failures. The September 2019 cyber-attack on India's Kudankulam Nuclear Power Plant revealed the need to increase cyber-nuclear security. Malware affected the administration system, but not plant control or instrumentation. Researchers said the attack was caused by a North Korean-linked virus, although Indian officials have not confirmed this. ISRO found malware in Kudankulam. The hack only affected administrative systems, but it showed that there were holes in nuclear security. Air-gaps are not well taken care of and don't offer much protection. A lot of administrative network data was taken, which could mean that more important systems could be attacked. Cyberattacks are stopped by firewalls, anti-virus software, air gaps, and one-way gateways. In 2020, there will be a new cyber policy. Any new plan must close the holes in the old ones. If it doesn't, India may have trouble with nuclear cyber security.

Cyber-nuclear security framework for India

India's cyber security infrastructure is inadequate, and its nuclear security architecture is kept a secret. Support a thorough and well-considered strategy for fending off cyberattacks. The Kudankulam attack exposed India's obsolete cyber defenses. Although India does have a cybersecurity policy, it lacks a lot of assurance. First off, there is no means to alert the public when nuclear or cyber infrastructure is malfunctioning. The Kudankulam incident is ambiguous and leaves out any mention of cyber security at nuclear facilities. This indicates that there are still issues with India's (6) cyber-nuclear security infrastructure that are "unresolved, underdeveloped, and to some extent unknown." Finding actionable channels in the nuclear security setup will be made easier by developing a flexible, dependable, and powerful cyber threat analysis system. The cyber-nuclear security system might be strengthened and made less likely to fail with a few more measures. India should study other nations' efforts to safeguard their nuclear facilities online and take note of their mistakes. The United States, United Kingdom, and Japan have developed robust cyber-security solutions to safeguard their nuclear infrastructure. Indian officials must participate in negotiations with other nations to create institutions, structures, and standards for nuclear and cyber security. India should cooperate more closely and exchange best practices on a bilateral basis with Japan and Australia.

CERT-In discusses how India collaborates with other nations to strengthen cyber security in its annual reports. Cyber-nuclear security can be added to nuclear facilities that are used for good things. India could work with experts to build its own cyber-nuclear security infrastructure and use it to protect other parts of its nuclear programme without giving away too much sensitive information or technology. The global supply chain is where India gets a lot of the tools and equipment it needs for its infrastructure (7).

[2] Debak Das, "An Indian nuclear power plant suffered a cyberattack. Here's what you need to know," The Washington Post, November 4, 2019, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/

[3] Annual ORG, C. I. (2017). Cyber Security & the CERT-In a Report on the Indian Computer Emergency Response Team's Proactive Mandate in the Indian Cyber Security Eco system. Cis India.Org. Retrieved June 11, 2022, from https://cisindia.org/internetgovernance/files/cert-ins-proactivemandate.pdf

Malware can enter the system at any stage in the supply chain. It is simple to neglect equipment or systems because it might remain dormant in any area for a very long time. Verify the supply chain's ability to manage cyber risks. For sourcing, vendor management, supply chain quality and continuity, as well as transportation security, strict standards are required. The nuclear establishment has to be educated about cyber threats, normalize the practice of managing cyber threats and ensure that everyone understands its significance. This improves safety precautions against insider threats. When authorities don't cooperate and exchange information, India's security apparatus is more susceptible to cyber assaults. Adjust this. If there were clear responsibilities for preparation, accountability, and testing, cyber-nuclear security would be better for India. A robust, accountable system that recognizes and rewards nuclear cyber-security practices, actions, and policies is essential.

Conclusion

India's nuclear infrastructure could be attacked online if there aren't clear rules. India doesn't have a cyber-nuclear policy, which leaves it open to cyberattacks, less educated, less knowledgeable, less able to work together, and slower to respond. Since cyberspace is always changing, nuclear security architecture must give cybersecurity top priority. Insider risks and the safety of nuclear facilities are very important.

After Kudankulam, plans for emergencies were made. Change your plans for cyber security to deal with cyber threats. India doesn't have a good set of policies to protect its cyber-nuclear system from cyberattacks. Security rules for India's nuclear infrastructure should be looked at every so often. Because nuclear materials and infrastructure are unstable, policy must offer both short-term and long-term solutions and think about the environment. India can build and improve its defenses by working with other countries. This gives India a way to deal with new threats and worries. Cyber security should be a top priority when updating nuclear systems and facilities. Quickly, new technologies are made and used. Government agencies should stay on top of changes in technology and make plans for a wide range of procedures and situations and get the private sector to take part.

It would be foolish to overlook the dangers that emerging threats to infrastructure represent. A government's ability to put in place comprehensive cyber security measures that defend against current threats and allow for modifications in the future is critical to reducing these risks." Because nuclear systems are notoriously difficult to keep up to date and because new threats from both states and non-state actors are always emerging, cyber security should be a constant topic of conversation among a wider audience. As well as harming the economy and public safety, cyberattacks on India's critical infrastructure could also cause havoc in the fields of nucleic and nuclear power generation, energy, finance, and telecommunications. When compared to other digital nations, the protection of the nation's critical information infrastructure has been elevated to a high level of importance DSCI (8). Developing a national security plan that includes cybersecurity as a major component is not something Indians should wait to accomplish, as other countries have done. This has been done successfully by other countries.

Acknowledgments

We would like to express our gratitude to everyone who provided input for this article. We would like to extend our thanks to everyone whose comments and ideas served as a source of inspiration while we were working on this article. We owe a debt of gratitude to the authors and experts who have already penned works on topics analogous to those that we covered, as it is their citations that allowed us to appropriately wrap up our work.

References

1. Pornima B. Cyber Threats and Nuclear Security in India. *J Asian Secur Int Affairs.* (2022) 9:183–206. doi: 10.1177/23477970221099748
2. Bommakanti K. *The Impact of cyber warfare on nuclear deterrence: A conceptual and empirical overview*. Mumbai: Observer Research Foundation (2018).
3. Mohan P. *Ensuring Cyber Security in India's Nuclear Systems*. Mumbai: Observer Research Foundation (2020).
4. Kessler B. *The Vulnerabilities of Nuclear Facilities to Cyber Attack. Stanford Strategic Insights*. Stanford, CA: Stanford University (2011).
5. Nye JS. Nuclear lessons for cyber security? *Strat Stud Q.* (2011) 5:18–38. doi: 10.21236/ADA553620
6. De Groot J. *What is Cyber Security? Definition, Best Practices & More, Data Insider*. Waltham, MA: Digital Guardian (2023).
7. Centre for Internet & Society. *Cyber Security & the CERT-In a Report on the Indian Computer Emergency Response Team's Proactive Mandate in the Indian Cyber Security Eco system*. Karnataka: Centre for Internet & Society (2017).
8. DSCI. (2013)
9. Hindustan Times. *Cyber attack at Kudankulam; critical system safe*. New Delhi: Hindustan Times (2019).
10. Choi JS, Gallagher N, Harry C. *An Effect-Centric Approach to Assessing the Risks of Cyber Attacks against the Digital Instrumentation and Control Systems at Nuclear Power Plants*. Baltimore, MD: Center for International & Security Studies (2020).
11. Kushner D. *The Real Story of Stuxnet*. New York, NY: IEEE Spectrum (2013). doi: 10.1109/MSPEC.2013.6471059
12. Das D. *An Indian nuclear power plant suffered a cyberattack. Here's what you need to know*. Washington, DC: Nash Holdings (2019).
13. Futter A. *Nuclear Weapons in the Cyber Age: New Challenges for Security, Strategy and Stability. Valdai Club*. Moscow: Valdai Paper (2016).
14. Futter A. *Managing the Cyber-Nuclear Nexus*. London: European Leadership Network (2019).
15. Giaurov V. *The Cyber-Nuclear Security Threat: Managing the Risks. Vienna Center for Disarmament and Non-Proliferation*. Stanford, CA: Stanford University (2017).

16. Jang KB, Baek CH, Woo TH. Analysis of cyber nuclear terrorism by DTrack consequences in the civilian nuclear power plant. *J Nuclear Sci Technol.* (2022) 59:207–15. doi: 10.1080/00223131.2021.1961634
17. Kazi R. The Roadmap for India's Nuclear Security. *Strat Anal.* (2016) 40:371–8. doi: 10.1080/09700161.2016.1209912
18. Kazi R, Kumar N. Thinking the Unthinkable: Cyber Attacks on India's Nuclear Assets. *Liberal Stud.* (2019) 4:107.
19. Linnosmaa J, Papakonstantinou N, Malm T, Kotelba A, Parssinen J. Survey of cybersecurity standards for nuclear instrumentation and control systems. *Proceedings of the International Symposium on Future I&C for Nuclear Power Plants, ISOFIC 2021: Online*. Kita Ward (2021). doi: 10.1109/ETFA52439.2022.9921502
20. Masood R. *Assessment of cyber security challenges in nuclear power plants security incidents, threats, and initiatives. Cybersecurity and Privacy Research Institute the George Washington University*. Washington, DC: George Washington University (2016).
21. Mishra S, Jacob H. *Nuclear Security Governance in India: Institutions Instruments and Culture (2019) (No. SAND 2020 10916). Sandia National Lab.(SNL-NM)*. Albuquerque, NM: Pandit Deendayal Petroleum University (2020). doi: 10.2172/1678824
22. Mohan P. *Can India Address the Growing Cybersecurity Challenges in the Nuclear Domain?* New Delhi: ORF (2021).
23. Sarkar J. Managing nuclear risk in South Asia: An Indian response. *Bull Atomic Sci.* (2017) 73:59–61. doi: 10.1080/00963402.2016.1264215
24. Shoaib M. *The Cyber-Nuclear Nexus and Threats to Strategic Stability*. San Francisco, CA: Academia.edu (2018).
25. Steitz C, Auchard E. *German nuclear plant infected with computer viruses, operator says*. London: Reuters (2016).
26. Economic Times. *India ranks 3rd among nations facing most cyber threats: Symantec.Economictimes.Indiatimes.Com*. Mumbai: Economic Times (2018).
27. Economic Times. *ISRO warned of a possible cyberattack when Track came calling" Economictimes.Indiatimes.Com*. Mumbai: Economic Times (2019).
28. Meity Gov. *National Cyber Security Policy 2013 MeitY*. New Delhi: Meity Gov (2013).
29. NSIAEA. *Nuclear Security Series Glossary Version 1.3*. Vienna: NSIAEA (2015).