ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor (RJIF): 8.4
IJAR 2025; 11(2): 217-219
www.allresearchjournal.com
Received: 05-12-2024
Accepted: 10-01-2025

Dr. Bimal Marandi
Faculty of BCA, S.P. College, Dumka, Jharkhand, India

Corresponding Author:
Dr. Bimal Marandi
Faculty of BCA, S.P. College, Dumka, Jharkhand, India

Issues & challenges of cyber security in India: A research review

Bimal Marandi

DOI: https://doi.org/10.22271/allresearch.2025.v11.i2c.12373

Abstract
In the realm of information management, cybersecurity is paramount. In contemporary society, safeguarding privacy and data has emerged as one of the most challenging endeavours. Cyber protection is a significant subject, although it is difficult to explain accurately. It has previously been conflated with phrases like as anonymity, information sharing, intelligence collecting, and monitoring. The significance of a data security framework to protect the evolving ICT infrastructure in the current information landscape is paramount. ICT infrastructure serves as the fundamental link among all essential national infrastructures. The implementation of both E-governance and Ecommerce initiatives globally need a robust cybersecurity infrastructure paradigm. This article aims to provide an overview of this trend, along with potential patterns and imperatives that emerge from this study concerning India.

Keywords: Cybersecurity, information management, e-governance, e-commerce

Introduction
Cybersecurity is defined as the protection of ICT networks and their contents. Cyber protection serves as an effective concept; nonetheless, it remains resistant to precise definitions, representing a wide and sometimes flexible notion. Terms like as anonymity, knowledge disclosure, intelligence collecting, and monitoring are often misinterpreted as synonymous. Cybersecurity may effectively function as a system for safeguarding privacy and preventing illicit surveillance, while the sharing of cybersecurity information and intelligence gathering can act as important instruments. Effective data security necessitates the significance of risk management for information networks. Three factors comprise the hazards connected with every assault: challenges (perpetrators), vulnerabilities (weaknesses), and repercussions (consequences of the attack). Although the majority of cyber-attacks little affect national security, the economy, and the well-being of individuals, a successful attack on many vital infrastructure components—predominantly in the private sector—can have significant repercussions. Mitigating such risks often involves eradicating sources of threats, addressing vulnerabilities, and diminishing consequences. Terms like as anonymity, information sharing, data collecting, and monitoring are often conflated with cybersecurity in public discourse. Privacy refers to an individual's capacity to regulate others' access to information. Effective cybersecurity may safeguard privacy in an automated environment; yet, information shared for cyber protection may sometimes include personal data that certain individuals regard as private. Cybersecurity serves as the means to safeguard an information system from unauthorized surveillance and intelligence gathering. Nonetheless, these approaches may also facilitate the promotion of cyber defence by addressing potential sources of cyber risks. Moreover, monitoring information flow inside a system may be a critical element of cybersecurity defence.

Cyber Security -An Overview
Experts and policymakers have engaged in prolonged discourse over this problem. Articulated increasing concern over the security of ICT systems against cyber-attacks, which are deliberate efforts by unauthorized persons to infiltrate ICT programs, often aimed at theft, disruption, destruction, or other illicit activities. A multitude of specialists anticipate an increase in both the frequency and magnitude of cyber-attacks in the next years. The protection of ICT systems and data is referred to as cyber security. The phrase "cyber

security" was created to denote the safeguarding of digital information. Cyber defence, sometimes seen as a nebulous concept, may serve as a useful asset in fostering diversity and inclusion.

Nonetheless, it is challenging to delineate accurately. It often pertains to one or more of the following aspects: A series of procedures and measures aimed at safeguarding servers, computer networks, related hardware, and software from intrusion, damage, or various threats, including devices and applications, as well as the data they encompass and interact with, such as software and records, along with other elements of cyberspace. The state of being protected from these risks. The extensive endeavour focused on implementing such initiatives and improving their efficacy. In policy discussions, cyber security is sometimes confounded with concepts such as anonymity, information exchange, data collecting, and monitoring. Privacy denotes an individual's right to regulate access to information pertaining to them. Consequently, while effective cyber protection may safeguard privacy in a digital environment, information shared to support cyber security initiatives may sometimes include personal data that some analysts could deem confidential. Cyber defence will safeguard against unlawful surveillance and intelligence gathering from an information system. When aimed at potential sources of cyber dangers, such efforts may be advantageous for attaining cyber security. Surveillance, in terms of regulating information flow inside a system, may be a crucial element of cyber defence.

Definition of cyber-security

As per the IT Act, 2000: Sec. 2(nb), cyber security refers to the safeguarding of information, equipment, devices, computers, computer resources, communication devices, and the information contained therein against unauthorized access, use, disclosure, interruption, alteration, or destruction. "Measures to prevent unauthorized access or attacks to secure a device or computer system (such as on the Internet)."

Cybersecurity includes preventative measures used to avert data loss, hacking, or malicious material. It necessitates an understanding of potential vulnerabilities to information, such as viruses and other dangerous software. Identity control, crisis management, and emergency management are cyber security strategies.

India's digital presence India has achieved considerable progress in the digital domain during the last ten years. The nation has one of the highest internet user populations globally, over 700 million individuals online. The Indian government's Digital India effort has significantly advanced digital literacy and facilitated the expansion of e-commerce, online banking, and e-governance. Nevertheless, as internet access expands, the prevalence of cyber dangers has increased markedly.

Research Methodology

A study design delineates the framework for the inquiry questions to be examined. It presents a coherent correlation of the evaluation techniques, testing protocol, analytical framework, and duration. This study used a descriptive research technique, since this approach is appropriate for problems necessitating comprehensive and detailed elucidation.

Methods of data collection

The method used for data collection is secondary. To enhance the overall efficacy of the study, existing data is aggregated and synthesized. Data may be gathered using either primary or secondary methods. This research used a secondary technique.

The cyber space of India

The exponential expansion of the Internet in the last decade seems to have contributed to an increase in the incidence of online assaults. The National Informatics Centers were established in 1975 in India to provide diverse IT solutions to the government. Three primary networks had been developed at that time.

a) **INDONET:** This network connects India's computer infrastructure, including IBM mainframes.
b) **Nic NET:** This is a public-sector network that connects the federal government with state and local governments.
c) **ERNET:** ERNET is an Education Research Network that caters to the university and research communities, as well as addressing cyber-attacks perpetrated by terrorists as a form of non-state or state-sponsored warfare.

National Cybersecurity Policy-2013

The National Cyber Security Policy, 2013, is a significant endeavour by the Indian government to safeguard the nation's cyber security environment; yet, it has several deficiencies that must be rectified to enhance its efficacy in addressing future challenges. The Government of India created the National Cyber Security Strategy 2020 for this objective. The National Cyber Security Strategy 2020 seeks to safeguard company data, a critical information asset that might impact national security and the economy. The first component ensures extensive digitalization of public services, the security of supply chains, the protection of important information infrastructure, and the security of digital payments. The second aspect fortifies structures, character, institutions and governance, budget allocation, research, innovation and technology development, capacity and skill enhancement, audit and assurance, and data security. The third part integrates internet infrastructure, standard development, cyber insurance, Brand India, cyber diplomacy, and cyber-crime investigation.

Challenges encountered by India's cyber security

- **Insufficient understanding:** A major difficulty in cybersecurity in India is the public's lack of understanding. A significant number of individuals are oblivious to the dangers posed by cyberattacks and fail to implement essential measures to safeguard their digital assets.
- **Inadequate financing:** A significant concern is the deficiency of enough financing for cybersecurity activities. Numerous firms in India fail to commit sufficient resources to cybersecurity, leaving them susceptible to assaults.
- **Deficiency of Skilled Professionals:** India is experiencing a significant scarcity of proficient cybersecurity experts. The need for cybersecurity specialists is rising swiftly, however there is a shortage of qualified people to meet this need.

- **Inadequate Legislation and Regulations:** India has insufficient rules and regulations pertaining to cybersecurity. The legislative framework for cybersecurity is antiquated and insufficiently addresses the contemporary digital environment, complicating the prosecution of hackers.
- **Cyber Espionage:** India is a key target for cyber espionage because to its large population, burgeoning economy, and vital geopolitical significance. Cyber espionage poses a substantial risk to national security, necessitating that India implement appropriate countermeasures.

Prospects for India's cyber security

- **Significant Market Potential:** The need for cybersecurity solutions and services is rising swiftly in India. The Indian cybersecurity industry is projected to reach USD 13.6 billion by 2025, presenting a significant potential for cybersecurity firms to enhance their operations.
- **Government measures:** The Indian government has implemented many measures to enhance cybersecurity throughout the nation. The National Cyber Security Policy 2013 and the Cyber Swachhta Kendra exemplify governmental measures designed to bolster cybersecurity in India.
- **Proficient Workforce**: India has a substantial reservoir of IT workers, which may be used to cultivate a proficient workforce in cybersecurity. With appropriate training and instruction, these individuals may be developed into cybersecurity specialists.
- **Collaboration and Partnerships:** India has the potential to engage with other nations and organizations to enhance its cybersecurity. Partnerships with nations such as the United States, Israel, and Japan may provide India with access to sophisticated technology and proficiency in cybersecurity.
- **Innovation and Entrepreneurship:** India has a robust startup environment, with several businesses developing novel solutions to tackle cybersecurity concerns. This offers a prospect for entrepreneurship within the cybersecurity sector, perhaps fostering innovation and generating new employment prospects.

India's cybersecurity business is seeing a notable increase in demand. The cybersecurity industry in the nation is projected to expand at a compound annual growth rate (CAGR) of 15.6% from 2020 to 2025, as per a research by Research and Markets. This offers a significant opportunity for the nation to establish a robust cybersecurity ecosystem. The Indian government has implemented several measures to tackle the cybersecurity threat. The Ministry of Electronics and Information Technology (MeitY) has initiated many programs, including the Cyber Swachhta Kendra, the National Cyber Coordination Centre (NCCC), and the Cyber Surakshit Bharat project, to enhance awareness and fortify cybersecurity in the nation.

Conclusion

India's digital revolution has generated significant prospects for economic advancement and social development. Nonetheless, it has also introduced considerable cybersecurity issues. The nation must adopt a thorough and cooperative strategy to tackle these difficulties. This entails raising awareness, enhancing capability, fortifying legal frameworks, and promoting innovation. Cybersecurity is an important concern that India must tackle in its pursuit of becoming a digital giant. The complexities and nuances of cybersecurity in India provide both challenges and opportunity.

Despite problems such as little knowledge, inadequate financing, and ineffective rules and regulations, there are possibilities including substantial market potential, governmental efforts, a competent workforce, collaborative collaborations, and avenues for innovation and entrepreneurship. Confronting these problems and capitalizing on these possibilities would be essential for India to enhance its cybersecurity framework and attain its digital objectives.

References

1. Times of India. Amid spying saga, India unveils cyber security policy. INDIA. 3 July 2013.
2. Data Security Council of India. Analysis of National Cyber Security Policy (NCSP-2013). 6 May 2021.
3. Centre Of Excellence for Cyber Security Research and Development in India (CECSRDI). Analysis of National Cyber Security Policy of India 2013 (NCSP-2013) and Indian Cyber Security Infrastructure. 21 November 2014.
4. Gupta BB, Joshi RC, Misra M. ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack. Int J Netw Secur. 2012;14(1):36-45.
5. Stanford Journal of International Law. Beyond the New 'Digital Divide': Analysing the Evolving Role of National Governments in Internet Governance and Enhancing Cyber security. Stanford J Int Law. 2014;50:119. Indiana Legal Studies Research Paper No. 290. 15 July 2014.
6. Perry4Law Organization. Cyber Security Breaches Are Increasing World Over and India Must Be Cyber Prepared. 22 May 2014.
7. Centre Of Excellence for Cyber Security Research and Development in India (CECSRDI). Cyber Security Challenges in India Would Increase. 18 November 2014.
8. The Economic Times. For a unified cyber and telecom security policy. 24 Sep 2013.
9. Department of Electronics & Information Technology, Government of India. National Cyber Security Policy-2013. 1 July 2013.