Research paper on Cyber Security in India

Mr. Shreesha R Huddar[1], Mr. Ramkishore M R[2]
[1]Assistant Professor, Department of Commerce BMS College of Commerce and Management
[2]Assistant Professor, Department of English BMS College of Commerce and Management

***Abstract*—In the world of information management, cyber security plays a critical role. In today's world, protecting privacy and data has been one of the most difficult tasks. Cyber protection is a valuable concept, but it is difficult to define precisely. It is also been mixed up with other terms like anonymity, knowledge sharing, intelligence collection, and monitoring in the past. The importance of a data security framework to safeguard the emerging ICT infrastructure in today's information environment cannot be overstated. ICT infrastructure is the common thread that connects all vital national infrastructures. The presence of a both E-governance and Ecommerce projects being undertaken around the world include a reliable cyber security infrastructure model. In this article, an attempt is made to present a snapshot of this development, as well as possible patterns and imperatives that arise from this analysis in the sense of India. Keywords: ICT technology vulnerability, Cyber security structure, electronic security practices, Next Generation Networks, e-governance, and e-commerce.**

I. INTRODUCTION

Cyber security has been recognized as the act of securing ICT networks and their content. Cyber protection can be an effective language, but it continues to defy precision definitions, a broad and perhaps somehow fluid idea. Other terms like anonymity, knowledge disclosure, intelligence collection, and monitoring are often wrongly conflated. Cyber security can nevertheless serve as an effective mechanism for privacy protection and illegal monitoring prevention and cyber security knowledge exchange and intelligence collections can be valuable tools. In order to achieve successful data security, risk management for information networks is seen as important. Three considerations are included in the risks associated with any assault: challenges (attackers), vulnerabilities (weakness) and impacts (what the attack does). While most cyber attacks have little impact on the national security system, the economy, livelihood and security of individual people, a successful assault on a number of critical infrastructure (CIs) components – most of which are private-sector. Reducing those risks usually means eliminating causes of threats, resolving vulnerabilities and reducing impacts. Other terms such as anonymity, knowledge sharing, data collection and monitoring are often mistakenly combined with cyber security in public debate. Privacy is related to an individual's ability to control other people's access to information. Good cyber security can thus help secure privacy in an automated world, but information exchanged for the purposes of cyber protection can sometimes include personal data that some people at least consider private.

II. CONCEPT OF CYBER SECURITY

Experts and policymakers have been debating this issue for many years. expressed growing concern about the security of ICT systems from cyber attacks intentional attempts by unauthorized individuals to gain access to ICT programmes, typically with the intent of stealing, disrupting, or destroying them damage, or any other illegal activity. Many analysts believe that the number and scale of cyber attacks are expected to rise in the coming years. The act of safeguarding ICT systems and data is known as cyber security. The term "cyber security" was coined to describe the protection of digital information. A diverse and inclusive after being a very hazy term, cyber defense may be a valuable tool.

In policy debates, cyber security is often conflated with other terms such as anonymity, knowledge sharing, data collection, and surveillance. Privacy refers to a person's right to monitor who has access to knowledge about them. As a result, while good cyber protection may help protect privacy in an electronic world, information exchanged to aid cyber security efforts could occasionally include personal information that at least some analysts may consider

private. Cyber protection will guard against unauthorized monitoring and intelligence collection from an information system. When directed at possible sources of cyber threats, however, such actions may be beneficial in achieving cyber security. Surveillance in the sense of information flow control within a system may also be an essential component of cyber defense.

1. Current Cybersecurity Landscape in India

Digital Growth

- India is among the top countries in terms of internet users (over 850 million).
- Massive digitalization through programs like Digital India has led to increased online services in banking, governance, education, and healthcare.

Key Threats

- Phishing & Ransom ware: Common attacks targeting both individuals and organizations.
- Data Breaches: Increasing incidents of sensitive data leaks.
- Cyber Espionage & Nation-State Attacks: Targeting defense, infrastructure, and strategic sectors.
- Social Engineering: Scams exploiting human psychology via calls, emails, or social media.

2. Major Cybersecurity Incidents in India

- 2020: Power grid in Mumbai faced a suspected cyberattack linked to foreign actors.
- 2021-22: Data breaches in organizations like Domino's India, Air India, and the COVID vaccine registration portal (CoWIN).
- 2023-24: Surge in ransomware attacks on Indian hospitals, educational institutions, and SMEs.

3. Government Initiatives and Frameworks

a. National Cyber Security Policy (2013)

- First major cybersecurity policy.
- Aimed to protect public and private infrastructure and create a cyber-secure ecosystem.

b. CERT-In (Indian Computer Emergency Response Team)

- Nodal agency for handling cybersecurity threats.
- Mandatory reporting of cyber incidents under revised rules (2022).

c. Data Protection Laws

- Digital Personal Data Protection Act, 2023 (DPDP Act): Enforces data privacy rights and obligations for organizations processing personal data.

d. Indian Cyber Crime Coordination Centre (I4C)

- Established to coordinate efforts against cybercrime across states.

4. Key Players in the Indian Cybersecurity Ecosystem

- Public Sector: NIC, DRDO, CERT-In, NCIIPC (Critical Infrastructure Protection).
- Private Sector: Infosys, Wipro, TCS, Quick Heal, K7, TAC Security.
- Startups: A growing number of cybersecurity startups focusing on AI, blockchain security, and zero-trust frameworks.

MEANING OF CYBER SECURITY

According to the IT Act,2000: Sec.2(nb) cyber security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction. "Anti-authorized access or assault measures to secure a device or computer system (as on the Internet)." "Cyber security refers to preventive approaches used to avoid lost, hacked or aggressive content. It calls for an awareness of possible vulnerabilities to information like viruses and other malicious programming. Identity control, crisis management and emergency management are the cyber security techniques."

WHAT THREATS ARE THERE?

Criminals' intent on monetary gain from crimes such as theft or extortion; spies intent on stealing classified or proprietary information used by government or private entities; nation-state warriors who develop capabilities and hacktivists who carry out cyber attacks in support of a country's strategic objectives.

WHAT ARE THE IMPACTS OF THIS PROBLEM?

An ICT system's security, transparency, and availability, as well as the information it manages, may be jeopardized if an attack is successful. Cyber fraud or cyber spying can lead to the theft of financial, confidential, or personal information that the perpetrator can profit from, often without the victim's knowledge. Industrial control systems can be attacked and the machinery they control, such as engines, motors, and centrifuges, can be destroyed.

ROLE OF GOVERNMENT

In terms of cyber security, the government's position includes both defending government infrastructure

and aiding in the protection of non-government networks. All government agencies now have data security responsibility for their own networks, and many have sector-specific responsibilities for CI under existing legislation. The Department of Electronics and Information Technology (Deity), Ministry of Communication and Information Technology, Government of India, has established a legislative structure called the National Cyber Security Policy.

Its aim is to keep public and private networks safe from cyber-attacks. According to the regulation, personal information (of web users), financial and banking information, and sovereign data, are also intends to safeguarded. This was especially important in light of recent NSA leaks indicating that US government agencies are spying on Indian consumers, who have no legal or technological protections against it.

Cyberspace, according to India's Ministry of Communications and Information Technology, is a diverse ecosystem comprised of human activities, software services, and the worldwide dissemination of information and communication technology. According to numerous reports and researches, India's National Cyber Security Policy of 2013 has a number of flaws and weaknesses. Despite the policy's announcement, India is still not cyber-ready. In addition, the proposal was not adopted until November of 2014. (till 21 November 2014). India's data security problems are only going to get worse, so decisive action is expected.

India's proposed programmes, such as the National Cyber Coordination Centre and the National Critical Information Infrastructure Protection Centre (NCIIPC), could help the country's cyber security and critical infrastructure protection. Now it will see how Cyber Security Strategy 2020 protects the cyber space.

Government Policy and Regulatory Framework

National Cyber Security Policy, 2013

- India’s foundational document on cybersecurity.
- Emphasizes infrastructure protection, capacity building, and creating a secure cyber ecosystem.

CERT-In (Indian Computer Emergency Response Team)

- Central agency for cyber incident response and coordination.
- Under revised guidelines (2022), mandatory reporting of all cybersecurity incidents within 6 hours.

Digital Personal Data Protection (DPDP) Act, 2023

- A landmark legislation focusing on user consent, data minimization, and accountability of data fiduciaries.
- Establishes a Data Protection Board for enforcement.

NCIIPC and I4C

- NCIIPC (National Critical Information Infrastructure Protection Centre): Focuses on protecting critical infrastructure like power grids and telecom networks.
- I4C (Indian Cyber Crime Coordination Centre): Aims to standardize and centralize response to cybercrimes across states.

III. THE CYBER SPACE OF INDIA

The exponential growth of the Internet over the last decade seems to have aided a spike in the number of cases of online attacks. National Informatics Centers were founded in 1975 in India to provide the government with various IT-related solutions. At the time, three main networks had been established. (a) INDONET: This network links India's computing system, which consists of IBM mainframes. (b) NIC NET: It is a public-sector NIC network that links the federal government with state and local governments. (c) ERNET: ERNET is an Education Research Network that serves the university and research communities and terrorists that use cyber attacks as a means of non-state or state-sponsored warfare.

NATIONAL CYBER SECURITY POLICY 2013

The National Cyber Security Policy, 2013, is a major initiative on the part of the Indian government to protect our country's cyber security climate, but it has certain flaws that need to be addressed in order to make it more effective for future complexities. So for this purpose GoI launched new NATIONAL CYBER SECURITY STRATEGY 2020. The National Cyber Security Strategy 2020 aims to protect enterprise records, a sensitive information resource that has the potential to affect national security and the economy. It has the following objectives:

1) Secure (National Cyber Space)

2) Strengthen (Structure, People, Processes, Capabilities)
3) Synergize (Resources including Cooperation and Collaboration)

IV. CHALLENGES OF LONG TERM

Preventing cyber-based hazards and espionage, reducing the impacts of successful threats, strengthening multiand intra-sector cooperation, clarifying federal agency functions and duties, and combating cyber crime are all among the executive branch activities and pending legislation. These requirements remain, however, in the light of more difficult long-term problems including design, incentives, consensus, and the environment (DICE):

Design: Experts often state that good protection must be a part of every ICT design. For economic reasons, developers have historically prioritised features over stability. Furthermore, certain potential security requirements are impossible to foresee, creating a difficult challenge for designers.

Environment: In size and properties, cyberspace is considered the most rapidly developing technological space in human history. New and emerging properties and applications—particularly social media, mobile computing, Big Data, cloud computing, internet—complicate the changing threat landscape, but could potentially improve cyber security by, for example, economies in scope of cloud computing and big data analytics.

THE POSITION OF THE UNION GOVERNMENT

India does not currently have a clear law that is primarily enforced for the security of data and the privacy of the citizen of India. The Indian Data Security and Privacy Regulatory mechanism is composed of the Information Technology Act, 2000 (the IT Act) and its related Information Technology Rules, 2011 (the IT Rules). Furthermore, under Article 21 of the Indian Constitution which guarantees the right to privacy as a fundamental right of every citizen, Personal Data is also covered. In a number of cases, the Supreme Court has ruled that information about a person and the right of the individual to access the information is also protected by the privacy privilege.

V. CONCLUSION

Although the government's objective is to ambitiously expand cyber connectivity. E-commerce is booming, and a number of e-governance practices now take place on the Internet. If we become more dependent on the internet for our everyday lives, we are even more vulnerable to cyberspace disruptions. The speed at which this industry has expanded has led policymakers and private businesses to strive to understand both the complexity and importance of cyber security and how accountability is shared. Cyberspace occupies the fifth position in the common space and it is essential that all nations work on cyberspace together and cooperate.

There is an increasing need for cyberspace and its use. In order for many terrorists to target key intelligence facilities, cyberspace is becoming a major field. The current legislation is unable to curb cyber attacks and thus calls for a change in the existing legislation to allow these practices to be checked. International coordination amongst nations is needed to tackle cybercrime effectiveness so that the evolution of cybercrime on the Internet is not restricted to countries without borders, such that universal partnership amongst countries is needed in order to operate together to and the increasing risks and danger to a manageable level.

REFERENCES

[1] "Amid spying saga, India unveils cyber security policy". Times of India. INDIA. 3 July 2013.
[2] "Analysis of National Cyber Security Policy (NCSP–2013)". Data Security Council of India. 6 May 2021.
[3] "Analysis Of National Cyber Security Policy of India 2013 (NCSP-2013) And Indian Cyber Security Infrastructure". Centre Of Excellence for Cyber Security Research and Development in India (CECSRDI). 21 November 2014.
[4] B. B. Gupta, R. C. Joshi, ManojMisra, ―ANN Based Scheme to Predict Number of Zombies involved in a DDoS Attack, International Journal of Network Security (IJNS), vol. 14, no. 1, pp. 36-45, 2012.

WEB SITES

[1] https://www.meity.gov.in/content/national-cyber-security-policy-2013

[2] https://www.scribd.com/document/474175656/Majhi-Santosh-Kumar-2015-Cybersecurity-Issues-andChallenges-A-View-Indian-Insitute-of-Technology-Journal-of-Global-Reasearch-in-Computer-Science.
[3] https://indiacode.nic.in/bitstream/123456789/1999/3