Putha Sateesh Kumar, 2025, 13:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Cyber Security in India: Emerging Threats, Legal Framework, and National Response Mechanisms

Putha Sateesh Kumar[1], Dr. Akash Sexana[2]
[1]Research Scholar Shridhar University, Pilani
[2]Professor and Supervisor Department of Computer Science, Shridhar University, Pilani

Abstract- Cyber security has emerged as a critical concern for India in the backdrop of rapid digitalisation, expanding internet penetration, and increasing reliance on information and communication technologies. The country faces a wide spectrum of cyber threats ranging from financial fraud, data breaches, ransomware, and phishing attacks to sophisticated state-sponsored cyber espionage and attacks on critical information infrastructure. This paper examines the evolving cyber threat landscape in India, analyses the existing legal and policy framework governing cyber security, and evaluates the national response mechanisms established to prevent, detect, and respond to cyber incidents. It highlights the role of key institutions such as CERT-In, the Indian Cyber Crime Coordination Centre, and the National Critical Information Infrastructure Protection Centre. The study also identifies major challenges, including legal gaps, capacity constraints, and low public awareness, and underscores the need for stronger legislation, enhanced institutional coordination, and greater emphasis on cyber resilience to safeguard India's digital ecosystem.

Keywords: Cyber Security, India, Cyber Threats, Information Technology Act, CERT-In, Cyber Crime, Critical Information Infrastructure, National Cyber Security Policy, Digital India.

I. INTRODUCTION

Types of Cyber Threats

- **Phishing:** Phishing is a cyber attack in which attackers try to steal personal information like passwords, bank details, or credit card information by sending fake emails, messages, or websites.
- **Malware:** Malware is malicious software designed to damage systems or steal data. Examples include viruses, worms, and trojans.
- **Denial of Service (DoS) Attacks:** In DoS attacks, attackers overload a server or network with too many requests, making it unavailable for legitimate users.
- **Man-in-the-Middle (MITM) Attack:** In this attack, the attacker secretly intercepts and possibly alters communication between two parties without their knowledge (eavesdropping).
- **SQL Injection:** SQL Injection occurs when attackers insert malicious SQL queries into input fields to gain unauthorized access to a database.
- **Cross-Site Scripting (XSS):** XSS attacks involve injecting malicious scripts into websites, which then run in users' browsers and steal information.
- **Ransomware:** Ransomware encrypts the victim's data and demands a ransom payment to restore access.

Cyber-attacks in India

- Under the IT Act, 2000 and IT Act (Amendment), 2008, cyber crimes and cyber-attacks have been legally defined in India.
- With the rapid growth of the internet, smartphones, digital payments, and e-governance, cyber- attacks in India have increased significantly.
- Government organizations, private companies, financial institutions, and common citizens have all become targets of cyber-attacks.

Cyber Threat Evolution

Time Period	Nature of Cyber Threats
1970s–1980s	Basic viruses and simple attacks
1990s	Email-based attacks and hacking
2000s	Malware, spyware, and phishing
2010s	Advanced Persistent Threats (APTs), ransomware
Present & Future	AI-based attacks, large-scale cyber warfare

Some Examples of Recent Cyber Attacks

1. **Stuxnet Malware**
- Stuxnet was a highly sophisticated malware designed to target industrial control systems.
- It caused serious damage to nuclear facilities by attacking SCADA systems.

2. **Aadhaar Data Breach**
- In India, incidents related to leakage of Aadhaar data have raised serious concerns.
- Sensitive personal information of citizens was exposed due to weak security practices.

3. **WannaCry Ransomware Attack**
- In 2017, WannaCry ransomware affected computers worldwide, including India.
- It encrypted user data and demanded ransom in Bitcoin.
- Hospitals, companies, and government offices were badly affected.

4. **GRAVITY RAT Attack**
- In 2017, CERT-In reported the GRAVITY RAT cyber-attack.
- It targeted Indian military and defense-related organizations.
- The malware was capable of stealing confidential data.

Key Takeaway

Cyber-attacks in India are increasing in frequency, scale, and sophistication, making cyber security a critical national priority.

Need for a Strong Cyber System

As cyber threats are increasing rapidly, it is necessary to create a strong and secure cyber system.

Cyber Security Framework

- Protection of computers, networks, data, and information systems.
- Ensuring confidentiality, integrity, and availability of data.
- Establishing legal, technical, and organizational security mechanisms.
- Managing cyber risks, prevention, detection, and response.
- Promoting cooperation between government, private sector, and international agencies.

Cyber Laws in India

- **Information Technology Act, 2000 –** India's first major law related to cyber crimes and electronic governance.
- **Information Technology (Amendment) Act, 2008** – Introduced stronger provisions for cyber security and cyber offences.
- **Indian Penal Code, 1860 –** Certain cyber crimes are also punishable under IPC provisions.

Government Institutions

- CERT-In (Indian Computer Emergency Response Team)
- Works under the Ministry of Electronics and Information Technology and plays a key role in cyber security.
- National Cyber Coordination Centre (NCCC)
- Responsible for real-time monitoring and coordination of cyber threats.
- Indian Cyber Crime Coordination Centre (I4C)
- Focuses on prevention, detection, and investigation of cyber crimes.
- National Cyber Security Policy, 2013
- Aims to create a secure and resilient cyber space.

Other Important Initiatives

- **Digital India Mission –** Promotes secure digital infrastructure and services.
- **National Critical Information Infrastructure Protection Centre (NCIIPC) –** Protects critical information infrastructure.
- **Cyber Swachhta Kendra –** Detects and removes malware from computers and devices.
- **Data Protection Initiatives –** Efforts to protect citizens' personal and sensitive data.

Conclusion

Cyber security is not only a technical issue but also a national security concern.

With the increasing use of digital technologies, strong cyber laws, awareness, and institutional frameworks are essential for India's safe digital future.

- After the cyber attack, in order to effectively deal with cyber threats and attacks, the Indian Government has taken several steps.

- A special branch called Defence Cyber Agency (DCA) has been established for cyber security.
- Digital India and Cyber Swachhta Kendra are major initiatives launched by the Government of India.
- The Ministry of Home Affairs (MHA) has launched the National Cyber Security Policy (NCSP).

Cyber Security Structure in India

Pm Office/Cab Inet Secy (Pmo/Cab Sec)	Ministery Of Home Affairs (Mha)	Ministery Of External Affairs (Mea)	Ministery Of Defence (Mod)	Ministery Of Common Info Technology (Mcit)	Non Govt. Organizational
National	National	Ambassadors	Tri Service	Department Of	Cyber Security And
Cyber	Security	& Ministers	Cyber	Information	Anti Hacking
Security	Council		Commad	Technology	Organisation (Csaho)
Coordinator	Secretariat			(Dit)	
(Ncsc)	(Nscs)				
National	Directorate Of	Defence	Army (Mi)	Department Of	Cyber Society Of India
Technical	Forensic	Attaches		Telecom (Dot)	(Cysi)
Research	Science				
Organisation	(Dfs)				
(Ntro)					
National	National	Joint	Navy (Ni)	Indian Computer	Center Of Excellence
Critical Info	Disaster Mgt	Secretary		Emergency	For Cyber Security
Infrastructure	Authority			Response Team	Research &
Protection	(Ndma)			(Cert-In)	Development In India
Centre					(Cesrdi)
(Nciipc)					
Joint	Central		Air Force	Educational	Cyber Security Of India
Intelligence	Forensic		(Afi)	Research	(Csi)
	Science Lab			Network	
	(Cfsls)			(Ernet)	

Pm Office /Cabinet Secy	Ministery Of Home Affairs (Mha)	Ministery Of External Affairs (Mea)	Ministery Of Defence (Mod)	Ministery Of Common Info Technology (Mcit)	Non Govt. Organizational (Ngo)
National	Intelligence		Def. Info	Informatics	National Cyber
Crisis	Bureau (Ib)		Assurance &	Center (Nic)	Security Of India
Management			Research		(Ncs)
Committee			Agency		
(Ncmc)			(Diara)		
Research And			Defense	Center For	Cyber Attacks Crisis
Analysis			Intelligence	Development Of	Management Plan Of
Wing (Raw)			Agency (Dia)	Advanced	India (Cacmp)
				Computing C-	
				Dac	
Multi Agency			Defense	Standardisation	

Center			Research Dev.	On, Testing And	
			Authority	Quality	
			(Drdo)	Certification	
				(Stqc)	
National Information Board (Nib)					

International Initiatives:

- Budapest Convention on Cybercrime was the first international treaty adopted in 2001 and came into force in 2004.
- India has not signed this convention yet, because it was framed without India's participation.
- In September 2020, India announced that it will develop an indigenous cyber security framework.
- CERT-In is responsible for cyber incident response, prevention, and coordination.

Conclusion:

- Cyber security is a multidimensional concept that includes technical, legal, and international aspects.
- For a country like India, cyber security is very important because of the increasing use of the internet and digital services.
- Through initiatives such as Digital India, CERT-In, and cyber security policies, India is making efforts to strengthen cyber security.
- In the future, it is necessary to develop strong laws, awareness, and technical infrastructure to deal with cyber threats.

REFERENCES

1. Government of India. Information Technology Act, 2000 (as amended in 2008). Ministry of Law and Justice, New Delhi.
2. Government of India. National Cyber Security Policy, 2013. Ministry of Electronics and Information Technology (MeitY).
3. CERT-In. About CERT-In and Cyber Security Guidelines. Indian Computer Emergency Response Team, MeitY.
4. Ministry of Home Affairs. Indian Cyber Crime Coordination Centre (I4C): Framework and Objectives. Government of India.
5. NCIIPC. Critical Information Infrastructure Protection in India. National Technical Research Organisation (NTRO).
6. Kshetri, N. (2016). Cybersecurity in India. Springer International Publishing.
7. Chawla, S., & Kumar, R. (2020). "Cyber Security Challenges in India: A Review." International Journal of Computer Sciences and Engineering, 8(5), 45–50.
8. OECD. (2021). Enhancing Cybersecurity Policy and Governance. OECD Publishing.
9. United Nations Office on Drugs and Crime (UNODC). (2020). Cybercrime and Digital Security: Global Perspectives.
10. Drishti IAS. "India's Cyber Security Challenges: Threats and Strategies." Drishti Current Affairs.