47

Reframing India's Cybersecurity Terrain: Hurdles, Developments and Prospective strategies[1]

Ms. Shubhajeet Shome*

Abstract

India holds the second position worldwide in terms of internet users, and this figure is growing rapidly. The country is making significant progress towards achieving its digitalization goals. The Indian government is also prioritizing this issue to ensure that all sectors in the country embrace maximum digitalization. However, the number of cybercrimes in India is also on the rise. Various forms of cybercrimes such as hacking, phishing, cyber bullying, online scams, and cyber extortion are victimizing individuals, private organizations, and even government agencies in India. This study aims to explore the different techniques of cybercrimes prevalent in India and around the world. This paper analyses the current cybercrime scenario in India and proposes measures to combat these crimes. Finally, the study concludes with relevant remarks and suggests areas for further research.

Keywords: Cyber extortion, phishing, Crypto jacking, National Cyber Policy, NCIIPC

Cybersecurity is a complex set of technologies, processes, and tools designed to protect our information, networks, and systems from malicious actors. In a world where information flows everywhere, cybersecurity acts as the sentinel. From hackers trying to gain unauthorized access to advanced malware designed to destroy, steal, or exploit sensitive information, cybersecurity is the custodian of our digital assets. Cybersecurity is the discipline that combines innovation and vigilance. It adapts to the ever-evolving landscape of digital risks to protect the integrity, confidentiality, and availabilityof your digital assets. Cyber warfare refers to the use of cyber space by state or non-state actors to carry out actions that pose a significant threat. It

*1 Shubhajeet Shome, Assistant Professor, Department of Law, University of North Bengal
* Assistant Professor, Department of Law, University of North Bengal

 E-ISBN: 978-93-6252-893-3

is a form of conflict that takes place primarily on the internet and involves politically motivated attacks on information or information system (Schatz and Wall). Cyber-attack can lead to severe consequences, such as disabling official networks and activities, disrupting essential services, alteration or stealing of any data and crippling financial system of the world.

The global economy has been completely transformed by information, technology connecting people and market in unimaginable ways. This has led nations worldwide to explore innovative ideas for economic growth and inclusivity. However, it has brought about new vulnerabilities and opportunities for disruption. Cyber security threats can come from different sources that result in disruptive activities and target individuals, businesses, national infrastructure and even governments (Devi). The consequences of these threats pose significant risks to public safety, national security and the stability of global economy. It can be challenging to determine the origin, identity or motivation behind such disruptions as they can occur form anywhere. As a result cyber security threats have become one of the most critical challenges for national security and economy (Gerecke).

1. Patterns of Cyber Attacks

Identity theft: In the digital era, identity theft via cybercrime is a major threat. It entails the unlawful use of another person's name, Social Security number, credit card information, or other identifying information for fraudulent reasons. Cybercriminals employ a variety of techniques, such as social engineering, malware, database hacking, and phishing emails, to get this information.

Ransomware: Ransomware is a type of malicious software designed to block access to a computer system or files until a sum of money, or "ransom," is paid. It's a serious cybercrime that has impacted people all across the world, includingcorporations, governments, and private citizens (Most cyber-attacks in India). After gaining access to a system, ransomware encrypts files or locks the system,rendering data unreadable. The responsible hackers then request money, sometimes in bitcoin, in order to unlock the system or provide a decryption key. With certain ransomware gangs now threatening to release confidential data in the event that the ransom is not paid, this type of cybercrime has taken on new dimensions that make it a dual danger to privacy and data security.

Phishing and cyber bullying: Phishing is the practise of making false efforts to get private data, including credit card numbers, usernames, passwords, and other sensitive information. Usually, to do this, one must seem to be a reliable source while communicating online. Phishing efforts might take the shape of texts, emails, or phoney websites that look authentic, deceiving people

 E-ISBN: 978-93-6252-893-3

into sending their personal information. Cyberbullying is when someone or a group is harassed, threatened, or harmed by the use of digital communication means. It can manifest itself in a number of ways, including disseminating gossip, humiliating details, threatening others, or sending disparaging remarks by SMS, social media, or other internet channels. Cyberbullying victims may have significant emotional and psychological impacts, such as sadness, anxiety, or even self-harm (Alpana and Malhotra).

Hacking and online scam: Hacking is all about gaining unauthorised access to computer system or networks. It can involve anything from basic activities like guessing passwords or using malware to more advanced attacks that takes advantage of software vulnerabilities. Hackers have different motives for their actions, which can include stealing sensitive information, disrupting systems or spreading malware. Cyber scams especially online scams are any of a broad variety of dishonest internet activities intended to fool people or businesses into divulging private information or money (Prasanthi and Ishwarya). Phishing and social engineering are two prevalent forms of cyber frauds that involve tricking victims into divulging personal information or granting access through emails or websites that appear authentic. Various fraudulent schemes, including fake websites, investment scams, lottery scams, and romance scams, aimed at deceiving individuals for financial gain (Verma and Sharma).

Cyber espionage: cyber espionage is the act of using digital methods to gain access to confidential information or data from individuals or organizations or government without permission. This involves secretly infiltrating computer networks, systems or devices to steal sensitive information, intellectual properties, or classifies data for political, financial advantage. Cyber espionage can be carried out by state –sponsored groups, criminal organizations and even individual who use various tactics such as malware, phishing, social engineering and other sophisticated methods to breach networks and extract information (Kandpal). The reasons behind cyber espionage can vary from political oreconomic gain to gaining a competitive edge in different sectors.

Crypto jacking: Crypto jacking refers to the sneaky practice of using someone else's computer without their permission to mine cryptocurrency. This devious act involves hackers infiltrating a device, often by planting malware or malicious code on websites, in order to exploit its processing power for mining cryptocurrencies like Bitcoin, Monero, or Ethereum. As a result, the affected device can experience significant slowdowns and increased energy consumption. Users may notice their device running sluggishly or the fan working overtime due to the excessive workload on the processor.

 E-ISBN: 978-93-6252-893-3

Denial-of-Service Attacks: DoS attacks aim to block users from using a service in a lawful manner. Attackers do this by sending more traffic over a network than it can manage. Accessing excessive amounts of network resources, which stops consumers from accessing the resources. DoS attacks send a massive volume of protocol packets via a distant network. Trying to route or process every packet eventually overloads servers and routers. In a few of minutes, network activity surges rapidly and the network ceases to react to regular traffic and client service requests. This type of attack is also referred to as a network saturation attack or bandwidth consumption attack.

2. Cyber security situation in India

India is ranked third globally among the top 20 countries where cybercrimes occur, according to the United States Internet Crime Complaint Centre (IC3) of the Federal Bureau of Investigation's 2019 Internet Crime Report. With 93,796 victims of cybercrimes, the United Kingdom led the list, followed by Canada (3,721) and India (2,901), with the USA not included in the list (Unites states Internet Crime Complaint Centre , 2019). The NCRB's "Crime in India, 2020" report has provided data for the year 2020. According to the report, there were 50,035 cases of cybercrimes registered in 2020, which is an increase of 11.8% from the previous year's 44,735 cases. The crime rate for cybercrimes also increased from 3.3 in 2019 to 3.7 in 2020. Out of the total cases registered, 60.2% were related to fraud, which amounts to 30,142 cases (NCRB).

In 2021, India witnessed a total of 52,974 cybercrime incidents, marking a nearly six percent increase compared to the previous year. Telangana emerged as the leading state, accounting for over 19 percent of these cases. Uttar Pradesh, on the other hand, reported a decline in cybercrime cases, with 8,829 incidents in 2021 compared to 11,097 in 2020. Similarly, Karnataka also experienced a decrease in cases, going from 10,741 in 2020 to 8,136 in 2021. Among cities, Bengaluru, India's IT hub, recorded the highest number of cybercrimes. However, the city has observed a downward trend in reported cases over the past three years. In 2021, Bengaluru reported 6,423 cybercrime cases, a decrease from 8,892 in 2020 and 10,555 in 2019 (Kant).

This is also very shocking that 80% of total crimes are reported from 10 districts in India. A new study conducted by an IIT Kanpur-incubated start-up has revealed that Rajasthan's Bharatpur and Uttar Pradesh's Mathura have takenover as the leading hotspots for cybercrime in India, replacing Jharkhand's Jamtara and Haryana's Nuh. The study also found that the top 10 districts in the country are responsible for 80% of all cybercrimes. The Future Crime Research Foundation (FCRF) has published these findings in their latest white paper titled 'A Deep Dive into Cybercrime Trends'. According to the FCRF,

 E-ISBN: 978-93-6252-893-3

Bharatpur (18%), Mathura (12%), Nuh (11%), Deoghar (10%), Jamtara (9.6%), Gurugram (8.1%), Alwar (5.1%), Bokaro (2.4%), Karma Tand (2.4%) and Giridih (2.3%) are the top contributors to cybercrime cases in India (80% of cyber crimes from 10 districts).

According to data (Davidpur) India is listed among the top five vulneravble countries which are most likely to have high percentage of cyber-attacks. Indiais ranked 4th with 5.33% of cyber-attacks percentage. It shows that though current centre government is endeavouring to promote digitalization in almost every sector in the nation. But there are high requirement to ensure a robust cyber security system in the nation.

Chart 1

Top Five Countries with High percentage of Cyber Attacks	
Countries	Percentage
China	18.83%
US	17.05%
Brazil	5.63%
India	5.33%
Germany	5.10%

Source: Cyber Proof

India is ranked 1st in terms of getting attacked by ransomware encryptovirological malware which causes heavy damage and block the personal data unless ransom is paid. It is a threat given by hackers to the internet users to pay high costs to save their personal data or information. Many users in India have been harassed through this process. It shows that digitalization is not fully possible if these fringe elements are not kept in control. India is ranked second in terms of internet users in the world. This country has been experiencing a rapid growth of digitalization in different sectors especially since last decade. Banking sector, finance sector, trade and commerce sector and other sectors are now adopting the digitalization process in a very rapid form. So internet users are now targeted from several ways by the cyber miscreants.

There are different tools that can be used for attacking computer systems. Malware is the term used to describe these tools. Examples of malware include viruses and worms. These are computer programs that can replicate themselves and have various effects, ranging from causing inconvenience to compromising the security of information (Buzan). Another type of malware is Trojan horses, which are destructive programs that disguise themselves as harmless

 E-ISBN: 978-93-6252-893-3

applications but actually create a backdoor for hackers to enter the system later. The main objective of system intrusion is often to gain full control or "root" access to the system, which allows the intruder unrestricted access to its inner workings. Because of the nature of digitally stored data, individuals with criminal intentions may choose to postpone, interrupt, manipulate, exploit, obliterate, pilfer, or alter the information. The significance of the data or the importance of the application will determine the extent to which these actions will impact, resulting in varying levels of severity.

Chart 2

Top 5 **countries where most users were attacked by Ransomware**	
Countries	Percentage
India	9.6%
Russia	6.41%
Kazakhstan	5.75%
Italy	5.25%
Germany	4.26%

Source: Cyber security

3. Government initiatives to prevent cybercrimes in India National Cyber Security Policy

The National Cyber Security Policy is a comprehensive framework created by the Department of Electronics and Information Technology. Its main goal is to safeguard both public and private infrastructure from cyber-attacks. Additionally, the policy aims to protect various forms of information, including personal data of web users, financial and banking information, and crucial sovereign data of the country. The Ministry of Communications and Information Technology, Government of India, has outlined the objectives of this policy, which include establishing a secure cyber ecosystem within the nation, fostering trust and confidence in IT systems and online transactions, and promoting the widespread adoption of IT across all sectors of the economy**.**

Indian Computer Emerging Response Team (CERT-In)

The Indian Computer Emergency Response Team, also known as CERT-In or ICERT, operates under the Ministry of Electronics and Information Technology in the Indian government. Its main role is to tackle cyber security threats such as hacking and phishing. CERT-IN was established in

 E-ISBN: 978-93-6252-893-3

2004 as apart of the Ministry of Communications and Information Technology, in accordance with the Information Technology Act of 2000. In December 2013, CERT-In highlighted an increase in cyber-attacks on various government organizations, including banking, finance, oil and gas, and emergency services. To address this, it issued a set of security guidelines for all critical departments. In September 2022, CERT-In collaborated with the Cyber Security Agency of Singapore to host an exercise called 'Synergy'. This event, which was part of the International Counter Ransomware Initiative-Resilience Working Group, saw the participation of 13 countries.

National Critical Information Infrastructure Protection Centre (NCIIPC)

The NCIIPC is an organization that works within a country's framework to protect critical information infrastructure from cyber threats and attacks. They focus on identifying, responding to, and preventing cyber incidents that could disrupt essential services or sectors such as energy, transportation, finance, telecommunications, and government operations. NCIIPCs collaborate with government agencies, private sectors, and international partners to develop strategies, guidelines, and best practices to strengthen the resilience of critical information systems against cyber threats. They play a crucial role in assessing risks, providing cybersecurity advisories, and fostering a robust cybersecurity ecosystem to safeguard vital national assets from potential cyber threats and attacks.

National Cyber Policy, 2013

The 2013 National Cyber Policy Framework in India was a comprehensive document that aimed to tackle the challenges and opportunities presented by the digital world. It had a strong focus on creating a secure cyberspace, promoting affordable and secure access to the internet, and enablinga robust ecosystem for the growth of the information technology sector. The policy also aimed to enhance the security of critical information infrastructure, improve preparedness to prevent and respond to cyber threats, and strengthen legal and regulatory frameworks to combat cybercrime and enhance law enforcement capabilities in cyberspace. Ultimately, the policy aimed to establish a secure and resilient cyberspace that would support India's social and economic growth while safeguarding national security interests in the digital domain.

Online Cyber Crime Reporting Portal

An online platform for reporting cybercrimes is an essential tool in the fight against digital threats. It allows people to report cybercrimes or

 E-ISBN: 978-93-6252-893-3

suspicious activities, providing a safe and accessible space for victims and concerned citizens to seek help or share information. These platforms often work closely with law enforcement agencies to take swift action against cyber threats. They offer various features, including:

a. Reporting Incidents: Users can provide details about cybercrimes they have encountered, such as fraud, hacking, phishing, or identity theft.
b. Anonymous Reporting: Options for anonymous reporting encourage victims or witnesses to come forward without fearing any retaliation.
c. Secure Communication: Encrypted channels ensure that the communication between the reporting individual and law enforcement agencies is secure, protecting sensitive information.
d. Tracking and Updates: Systems are in place to track the progress of reported incidents and provide updates to the reporter about the status of their case.

National Cyber Security Coordination Centre (NCCC)

The NCCC, or National Cyber Security Coordination Centre, is a centralized entity that oversees cybersecurity efforts at a national level. Its main goal is to monitor, detect, respond to, and prevent cyber threats and attacks that could potentially harm critical infrastructure, government systems, businesses, and citizens. NCCCs work closely with government agencies, law enforcement, intelligence services, private sector organizations, and international entities to share information, develop cybersecurity strategies, and implement measures to enhance overall cyber resilience. Additionally, they may offer guidance, support, and resources to different stakeholders to improve their cybersecurity posture.

Cyber Swachhta Kendra

The Indian government is providing free tools to detect and remove botnets through its 'Cyber Swachhta Kendra', also known as the Botnet Cleaning and Malware Analysis Centre. This initiative, part of the Digital India campaign under the Ministry of Electronics and Information Technology (MeitY), aims to ensure a safe online environment by identifying botnet infections in India and assisting individuals in securing their affected systems. As stated on the Cyber Swachhta Kendra website, the centre operates in partnership with Internet Service Providers (ISPs) and antivirus companies, and is managed by the Indian Computer Emergency Response Team (CERT-In).

 E-ISBN: 978-93-6252-893-3

Conclusion

India has emerged as one of the fastest-growing markets for digital technologies, aligning with the government's Digital India mission. The government has been actively promoting digital adoption by creating broadband highways, introducing services like DigiLocker, and implementing e-governance schemes such as the Jan Dhan Yojana. As a result, India now boasts a staggering 1.15 billion phones and over 800 million internet users, making it a prime target for cyber threats (Mathur). But there is a growing rate of cybercrime in the country. Many times governmental agencies are unable to trace the source of the miscreants. Many people have been victimised due to fraudulent of money, stealing of data, threats through email or social media etc (Athavale). It has become more vulnerable to old age people because some time they are asked through fraud phone calls or emails to give OTPs (one Time Password) or Bank account numbers or Personal identities cards numbers (Singh). As soon as they provide these information they fall into a deep trap. Most of the times there is a possibility that their saving money is stolen digitally and other important personal identities get leaked. There have been many such incidents where the police or government agencies have failed to find culprits. But this era is considered as digital era where the importance of cyber benefits cannot be refuted. So it is a utmost responsibility of the government to strengthen the cyber policy and cyber network so that common people should not get harassed and tortured by cyber miscreants.

Bibliography

[1] 80% of cyber crimes from 10 districts; Rajasthan's Bharatpur new Jamtara: study. (2023, September 2023). *The Economic Times* .

[2] Alpna, & Malhotra, S. (2016). Cyber Crimes-Its types, analysis and prevention techniques. *International Journal of Advanced Reserach in Computer Science and Software Engineering , 6* (5).

[3] Athavale, D. (2014, March 10). Cyberattacks on the Rise in India. *The Times of India* .

[4] Buzan, B. (1991). *People, States, and Fear: An Agenda for International Security Studies in the Post Cold War Era.* London: Harvester Wheatsheaf.

[5] Davidpur, N. (2022, january 4). Which Countries are Most Dangerous? Cyber Attack Origin – by Country. *CyberProof* .

[6] Devi, S. (2019). Cyber Security In The National Security Discourse. *The Journal ofInternational Issues , 23* (2), 146-159.

[7] Gercke, M. (2009). *Understanding Cybercrime: A Guide for Developing Countries.* Geneva: ITU Publication.

[8] Kandpal, V. (2017). Latest face of cybercrime and its prevention in India. *International Journalof Science, Technollogy and Management , 6* (4).

[9] Kant, V. (2023, May 22). NCR belt emerges new cybercrime epicentre. *Hindustan Times* .

[10] Mathur, A. (2022, March 9). Cybersecurity: How is India faring? *The Economic Times* .

[11] Most Cyberattacks on India Show Chinese IP Address: NTRO. (2014, November 13). *The Economic Times* .

[12] Prasanthi, M. L., & Ishwarya, T. (2015). Cyber Crime- Prevention & Detention. *International journal of advanced research in computer and communication engineering , 4* (3).

 E-ISBN: 978-93-6252-893-3