International Journal of Information Science and Computing
Citation: *IJISC*: **11**(01): 43-52, June 2024
DOI: 10.30954/2348-7437.1.2024.5

INFORMATION SCIENCE AND TECHNOLOGY FOUNDATION

REVIEW PAPER

Cyber *Swachhata Abhiyaan* in India: A Comprehensive Review of Cybersecurity Initiatives and Emerging Threats

Deep Debnath

Department of CIS, Raiganj University, West Bengal, India

Corresponding author: d.debnath.infotech@gmail.com

Received: 22 Mar., 2024 **Revised:** 30 May, 2024 **Accepted:** 07 June., 2024

ABSTRACT

Cybersecurity has turned out to be a highly important issue in digital technologies across India, cybersecurity has become a critical issue. The Cyber *Swachhata Abhiyaan* (CSA) is an initiative launched by the Government of India towards creating a safer cyberspace through citizen education, free provision of tools, and addressing issues related to cybersecurity threats. This paper analyzes the CSA, in addition to other government initiatives that are there to combat cybercrime. It also talks about the emerging cyber threats like cyber slavery, digital arrest, doxxing, phishing, ransomware, identity theft, cyber-bullying, online scams, credential stuffing, and ad fraud. It further discusses how CSA and related policies help mitigate these cyber threats and enhance the security posture of India in terms of cybersecurity.

Keywords: Cyber *Swachhata Abhiyaan*, Cyber Security, Cybersecurity Initiatives, Cybersecurity Emerging Threats, CSA, Cyber Threats

1. Digital Transformation in India and the Rise of Cybercrime

This digital revolution is penetrating only transformatively in India as a result of the *Digital India*, increasing penetration of Internet. However, the rapid of increase in cybercrime is that there is an increase in the rate of digitizing services. One national response is adopting several initiatives that are meant to guard individuals and organizations against growing cyber threats. One of the major national initiatives is the *Cyber Swachhata Abhiyaan*, which is an effort at furthering cybersecurity awareness, tools to address cyber threats, and a more secure digital ecosystem[2].

How to cite this article: Debnath, D. (2024). Cyber *Swachhata Abhiyaan* in India: A Comprehensive Review of Cybersecurity Initiatives and Emerging Threats. *IJISC.,* **11**(01): 43-52.

Source of Support: None; **Conflict of Interest:** None

2. Need for Cybersecurity Initiatives in India

This increasing dependency on the digital world in terms of banking, healthcare, education, and governance has made India a juicy target for cybercriminals. More necessitous need for effective cybersecurity to counter cybercriminal activities and forthcoming interventions by government to secure cyberspaces against malicious actions against users has been promoted by this culture[2],[5].

OBJECTIVE OF WORK

This paper's main goal is to present a thorough analysis of the *Cyber Swachhata Abhiyaan* (CSA) and associated government programs aimed at thwarting new cybersecurity threats in India[6],[7]. Among the particular objectives are:

- **Examining the CSA Initiative:** To determine how well CSA is doing in raising awareness of cybersecurity, offering free tools, and creating a safer digital environment in India[7],[8].
- **Finding Emerging Cyberthreats:** To investigate the changing environment of cyberthreats, such as ransomware, phishing, identity theft, cyberbullying, cyberslavery, and doxxing, and to evaluate the effects they have on people and businesses[7].
- **Assessing Government Efforts:** To evaluate how well India's cybersecurity posture is being improved and cybercrimesare being addressed by a number of government frameworks and policies, including the Indian Cyber Crime Coordination Centre (I4C), CERT-In, and the National Cyber Security Policy[7].
- **Highlighting Difficulties:** To determine the difficulties in putting cybersecurity initiatives into practice, especially in rural areas and among groups that lack digital literacy.
- **Examining Future Directions:** To make practical suggestions for bolstering India's cybersecurity framework, encouraging public-private collaborations, and raising public awareness in order to successfully reduce cyberthreats[6].

METHODS

The chapter "*Cyber Swachhata Abhiyaan*: Mitigating Emerging Cyber Threats in India" is a conceptual work that was theoretically prepared using existing literature on cybersecurity, cyber threats, and related initiatives, including books, chapters, journals, and government reports. The official websites of organizations such as the Ministry of Electronics and Information Technology (MeitY), CERT-In, and the Indian Cyber Crime Coordination Centre (I4C), along with associated bodies and boards, have been examined in order to examine current and ongoing activities, policies, and services addressing cybersecurity challenges.

REVIEW OF EXISTING WORKS

It is suggested that this specific work be created with an analysis of existing related works; to do this, a number of important works should be studied and referred to in the chapter's Existing Review works section. According to the scientific/applied style guide, all generally refereed works are included in the chapter's Reference section.

Anderson, *et al.* (2019) examination of the costs of cybercrime, demonstrating notable changes in the market, including the replacement of PCs by mobile phones and the growth of cloud services. In addition to new crimes including business email breach and cryptocurrency-related charges, payment fraud has risen. The paper highlights the low to mid-range costs of cybercrime to citizens and calls for a change in defense tactics that prioritize response over prevention and better collaboration between law enforcement.

Behera, S. and Balaji, P. (2019) examine the goal of the Digital India initiative is to establish a society that is enabled by technology, with a focus on the shift to a "Faceless, Paperless, Cashless" economy. Demonetization stimulated digital transactions by increasing the usage of plastic cards, e-wallets, and e-banking. However, obstacles including human error, system breakdowns, and a lack of digital literacy in semi-urban areas impede advancement. The government is trying to encourage a cashless future and lessen reliance on currency.

Bossler, A.M. *et al.* (2019) introduced the quick rise in cybercrime, which is made possible by new technology. Cybertrespassing, cybertheft, cyberporn, and cyberviolence are some of the categories that fall under the umbrella of cybercrime. Because there are no defined legal definitions or trustworthy statistics, it is difficult to estimate the prevalence of cybercrime, despite its rise. Due to the lack of official data, researchers find it challenging to examine cybercrime and frequently turn to creative techniques like surveying people and examining internet conversations.

Kshetri, N. *et al.* (2016) explore to draws attention to India's difficulties in tackling cybersecurity (CS) issues, pointing to a lack of both domestic and international solutions in comparison to other big nations. Critics point to the National Cyber Security Policy (2013)'s unclear implementation, resource distribution, and practical initiatives. Progress is impeded by weak CS frameworks and institutional inadequacies. Although public-private partnerships are suggested as a crucial tool for bolstering cybersecurity infrastructure and filling in knowledge and resource gaps, more work is needed to achieve significant results.

Kshetri, N. (2016) conducted a report on India's growing cybercrime that focuses on the particular dangers that poorer nations confront. It integrates viewpoints from international relations, criminology, economics, and institutional studies. India's cybercrime situation is examined using a paradigm that examines the interactions between formal and informal institutions, developmental factors, and international relations. The results show that issues with foreign relations, development, and institutions have a big impact on cybersecurity and cybercrime in emerging nations like India.

Kumar, V. *et al.* (2024) explores the development of technology and the internet in India, emphasizing the surge in cybercrimes that has coincided with its gradual but steady growth. Numerous studies highlight how common and sophisticated cybercrime is becoming, with a 24% increase in incidents reported in 2022 (NCRB). In order to control and lessen cyber dangers in India, the literature emphasizes the urgent need for strong cybersecurity measures, efficient government policies, and a more solid legal framework.

Naha, A. (2022) introduced the development of security studies in international relations, which went beyond definitions that were centered on states to include personal security concerns including environmental difficulties, poverty, and education. It draws attention to the emergence of "cyber-politik," in which conventional state and military power is challenged by non-state entities including NGOs, multinational corporations, and cybercriminals. National security currently faces new, non-lethal threats that threaten stability and infrastructure due to the rise in cyberwarfare, espionage, and sabotage.

Parikh, V. *et al.* (2023) focuses on applying the Theory of Planned Behavior (TPB) paradigm to evaluate cybersecurity awareness among university students in Vadodara, India. Research shows that students between the ages of 18 and 23 have poor cybersecurity awareness, engage in risky behavior, and have unfavorable attitudes. Research emphasizes the correlation between TPB constructs, showing limited digital competency despite moderate internet usage. In order to enhance students' cybersecurity behavior and practices, the literature emphasizes the necessity of focused awareness campaigns and educational interventions.

Paul, P.K. *et al.* (2018) discussed beginnings in cryptography to more general areas like computer security, network security, online security, and data security, the literature demonstrates the development of cyber security. The development of these fields cleared the path for ideas like assurance, information security, and IT security. Important subjects like information and data protection are also becoming more popular. The purpose of this review is to increase knowledge of computing and information security issues among the IT and non-IT groups.

Paul, P.K. *et al.* (2018) emphasis on their importance in the digital age, the literature examines a variety of cyber-related topics, such as cybercrime, cybernetics, cyberspace, cyberwarfare, cyberculture, and cyber legislation. It presents cybernetics as a paradigm for system control and emphasizes how cybercrime is constantly changing, focusing on computers, networks, and databases. It also discusses the social effects of cyberwarfare and the place of cyberculture in the digital world, highlighting the increasing demand for educational initiatives in these new areas.

Paul, P.K. *et al.* (2018) examineat the expanding importance of information technology and the problems that come with it, including the increase in cybercrime. It draws attention to cybercrime as a serious criminal activity that compromises the security of computers, information, and mobile devices. Originally restricted to abuse of the internet and email, cybercrime has expanded to include a wider range of instruments and techniques. The nature, traits, and urgent problems of cybercrime are the main topics of this review, which also highlights the influence of cybercrime on the quickly changing IT landscape.

Shah, P. *et al.* (2020) analysis highlights how little is known about the cybersecurity practices of Indian smartphone users, underscoring their susceptibility as a result of their lack of digital device experience. It lists 28 suggested behaviors for smartphone security and cites research on international cybersecurity standards, including those from China and the USA. Demographics like gender and age are important determinants of cybersecurity practices. The results highlight the necessity of focused awareness campaigns to improve cybersecurity among Indian smartphone users.

Wall, D.S. (2024) this researched, "Transformation of Crime in the Information Age," focuses on how technical developments like social media, cloud computing, and cryptocurrencies have increased the chances for cybercrime since 2007. New threats that have grown to be serious issues, such as ransomware and data leaks, are covered in the book. Even if cybersecurity and policing have advanced, they are still reactive, and cybercrimes are still not adequately reported. Regulation and enforcement have difficulties due to the dynamic nature of cybercrime.

CYBER *SWACHHATA ABHIYAAN* – FEW ASPECTS

Objectives of Cyber *Swachhata Abhiyaan*

Cyber *Swachhata Abhiyaan* was launched by the Ministry of Electronics and Information Technology (MeitY) in 2017 to promote[6]:

- Awareness and importance of applying cybersecurity hygiene in the conduct of life.
- Provision of tools to help citizens detect and remove malware and other cyber threats without charge.
- Promotion of safe digital practices to protect individuals and organizations against cybercrime.
- Raising awareness among multi-nations towards the development of the nation to combat emerging cyber threats.

Key Features of CSA

The program introduces a variety of free tools available for malware removal and protection from cyber threats and also awareness campaigns to teach citizens how they should secure their devices, identify phishing attempts, and use safe online practices. Additionally, CSA fosters partnerships with private companies in the field of cybersecurity to provide better aggregate protection for users.

Government Initiatives to Combat Cybercrime

In India, many important government initiatives have been launched in order to deal effectively with the problems created by cybercrime:

- **National Cyber Security Policy:** The NCSP, which came into existence in 2013, provides the strategic framework for securing cyberspace in India by focusing on prevention of cybercrime, improving the parameters of cybersecurity infrastructure, and legal measures[9].
- **Indian Cyber Crime Coordination Centre (I4C):** This initiative, announced in 2020, has been established to provide a coordinated response to cybercrime across states and agencies. Prevention, detection, and prosecution of cybercrimes focus[9].
- **Cyber Crime Reporting Portal:** Now, with the help of this portal, citizens are able to report cybercrimes like online fraud, identity theft, and harassment directly to the authorities via a straightforward process[9].
- **CERT-In:** The Indian Computer Emergency Response Team (CERT-In) has an important role as far as responding to cyber threats is concerned, giving alerts and guidance information to government bodies, private companies and citizens in mitigating cyber risks.

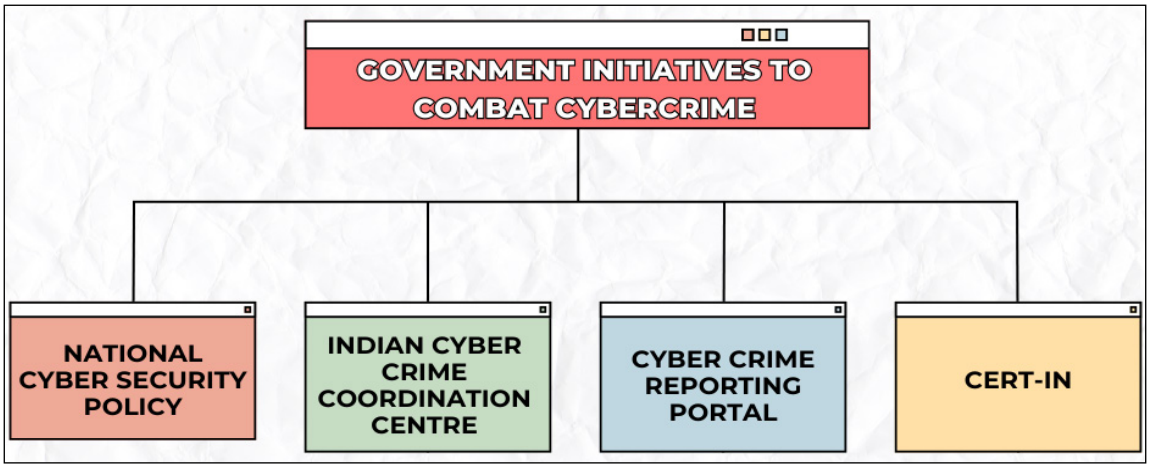

Fig. 1: Government Initiatives to Combat Cybercrime

KEY CYBER THREATS IN INDIA

Cyber slavery

Cyber slavery is when a person is forced for working or sexual acts through digital means like a fake job offer, online exploitative content, and through common digital methods of enslavement with malicious software. This prevalence in India is increasing with the digitization of processes; thus, very strict surveillance and prevention would have to be imposed by government bodies for the detection of such activities[9],[11].

Digital Arrest

Digital arrest is the illegal tracking and surveillance of people using digital technologies, such as unauthorized access to their personal devices and tracking their activities online. Such techniques can be resorted to by cyber criminals or even state actors to infringe upon the privacy rights of individuals. While such acts are being addressed in changing Indian laws like the Information Technology Act, challenges still remain in making such laws actually effective.

Doxxing

Doxxing refers to the insane online unveiling of private or identifying material about individuals without their consent, usually resulting in harassment, threats, and then actual harm. Doxxing is a dangerous threat to personal safety and individual's privacy due to the thousands of social networking and forum sites mushrooming. Cyber *Swachhata Abhiyaan* is working as an awareness campaign on the need to secure their personal information and to protect against doxxing.

Phishing

Phishing is one of the most common types of cybercrimes in India where criminal impersonates a legitimate organization or individual to steal sensitive information such as passwords and bank details. Attacks of phishing constitute almost all crimes committed over the cyberspace in India. The awareness campaigns of the government through CSA are meant to teach people how to identify phishing attempts so that they can save themselves from becoming victims of such scams[10].

Ransomware

Ransomware attacks, where cybercriminals encrypt the files of the victims and demand payment to restore access, have mushroomed in India. These attacks have hit businesses, government departments, and individual users. Such initiatives as CERT-In that have been established by the government stand a critical chance of helping in identifying the ransomware threats and acting on them.

Identity Theft

Identity theft is an unauthorized use of the person's personal data for committing fraud or theft with respect to that person. In India, identity theft has certainly emerged as a serious menace following the rapid adoption of digital banking as well as e-commerce. To tackle this menace in India, the government has enacted several laws such as Information Technology Act and undertaken such initiatives aimed to propagate the public on awareness of protecting their own personal information[10].

Cyber bullying

Cyber bullying is the latest and growing form of harassment today, particularly among children and teenagers in the country. It harasses, threatens, or embarrasses one online. The government has recognized this fact by putting a few hotlines and other online reports in conditions of cyberbullying, which will help in preventing antisocial dangers[1].

Scams on the Internet

Internet scams are schemes that sell fraudulently as buy-schemes through -the-fake sites, dubious advertisements, and false offers of rewards or benefits. Most of these schemes are financial or identity-related. The Cyber *Swachhata Abhiyaan* tells users about spotting and avoiding scams and encourages the use of secured platforms for accessing the internet[7].

Stuffing credentials

Credential stuffing is the use of stolen usernames and passwords to gain access to online accounts without authorization. This is becoming progressively successful, especially since most people use the same passwords in different sites. Cyber crime awareness programs in India are designed for propagating strong and unique passwords as well as using two-level verification, thus protecting against credential stuffing attacks[13].

Ad Fraud

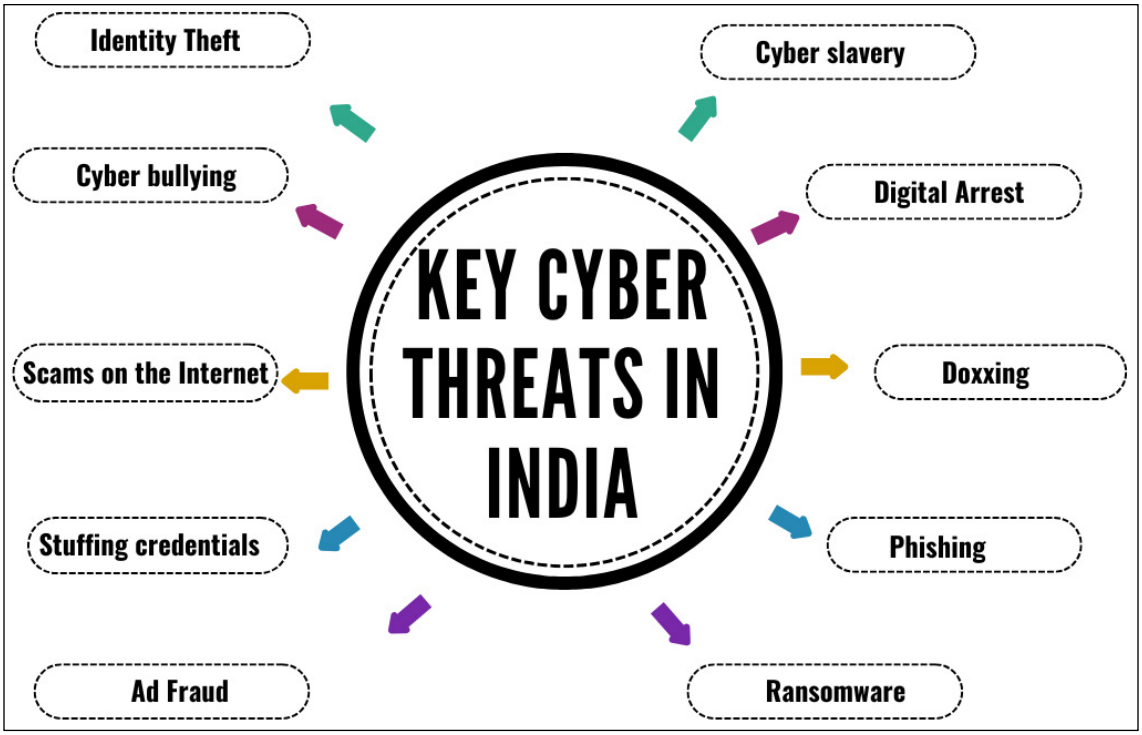

Fig. 2: Key Cyber Threats in India

Ad fraud is the act of manipulating online advertising infrastructures in pursuit of illegitimate financial returns, often by means of click fraud, false ad impressions, and misrepresentation of advertising performance. It may not be intentionally directed at the consumer but leads businesses and advertisers to lose revenues. The government is, however, working with the industry partners in ensuring that such regulations become tighter and that awareness programs are launched to mitigate advertisement fraud.

GOVERNMENT'S ROLE IN COMBATING EMERGING CYBER THREATS

Strengthening the Legal Framework

India has updated its legal framework to answer the emergent cyber threats. The core law in regulating cyber crimes, such as data protection, identity theft, and cyber bullying, is the Information Technology Act of 2000 with amendments in the year 2008. Further amendments and new enactments will be expected for cyber slavery, doxxing, and ransomware[1],[3].

Promoting Cybersecurity Awareness

Improving cybersecurity literacy is an outcome of government initiatives, such as the *Cyber Swachhata*

Abhiyaan. It aims at the sensitization of the citizenry about how to ensure safety in their personal data, recognize malicious activity, and safely use digital platforms. Different strata of citizens-children at school and seniors, are targeted in public campaigns, ensuring maximum security[9].

Public-Private Partnerships

That's been a great success point for CSA – the interplay between government and the private cybersecurity firms, because CSA has managed to offer very free cybersecurity tools, the malware removal tool, that has helped offer the opportunity to protect many citizens; hence, preparedness that will keep these citizens alert and on high alert should such threats crop up.

CHALLENGES AND FUTURE DIRECTIONS

Challenges in Implementation

Despite these efforts, challenges remain in reaching remote areas, dealing with the vast scale of emerging cyber threats, and addressing the lack of cybersecurity awareness in the general population. Digital illiteracy, particularly in rural India, poses a significant hurdle to the success of initiatives like CSA [13].

Future Directions

To mostly address the evolving cyber threat landscape, the Indian government needs to:

- ❒ Enhance public-private partnerships for better cybersecurity infrastructure.
- ❒ Increase investment in cybersecurity education and workforce development.
- ❒ Expand outreach to rural and underserved communities to bridge the digital divide.
- ❒ Strengthen international collaborations to combat transnational cybercrimes.

CONCLUSION

The Cyber *Swachhata Abhiyaan* has been one of the most important contributions that India has made in fighting cybercrime and building a safer digital environment. From public awareness campaigns, to legal reforms, to private sector partnerships, the government has made great strides in combating cyber threats, including phishing, ransomware, identity theft, and cyberbullying. However, with sophistication in cybercrimes, efforts must be sustained so that India remains a safe digital space for its citizens.

REFERENCES

1. Anderson, R., Barton, C., Böhme, R., Clayton, R., Ganán, C., Grasso, T. ... and Vasek, M. 2019. Measuring the changing cost of cybercrime.In The 18th Annual Workshop on the Economics of Information Security (WEIS 2019).

2. Behera, S. and Balaji, P. 2019. Cashless Economy: The Dream of Digital India. *International Journal of Management, Technology and Engineering,* **9**(4): 5629-5636.

3. Bossler, A.M. and Berenblum, T. 2019. Introduction: new directions in cybercrime research. *Journal of Crime and Justice,* **42**(5): 495-499.

4. Kshetri, N. 2016. Cybercrime and cybersecurity in India: causes, consequences and implications for the future. *Crime, Law and Social Change,* **66**: 313-338.

5. Kshetri, N. and Kshetri, N. 2016. *Cybersecurity in India. The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies*, pp. 145-157.

6. Kumar, V., Vati, K. and Chaudhary, A. 2024.Cyberspace vis-a-vis Cybersecurity in India through the Lens of Law and Policy. *Productivity,* **65**(1).

7. Naha, A. 2022. Emerging cyber security threats: India's concerns and options. *International Journal of Politics and Security,* **4**(1): 170-200.

8. Parikh, V. and Nimbekar, M. 2023. Socializing the Impact: An Analysis of the Theory of Planned Behavior's Influence on Increasing University Students' Cybersecurity Awareness. *Journal of Community Development,* **4**(2): 139-156.

9. Paul, P.K. and Aithal, P.S. 2018. Cyber Security to Information Assurance: The Changing World of Cyber Sciences.

10. Paul, P.K. and Aithal, P.S. 2018. Cyber crime: challenges, issues, recommendation and suggestion in Indian context. *International Journal of Advanced Trends in Engineering and Technology (IJATET),* **3**(1): 59-62.

11. Paul, P.K , Bhuimali, A., Aithal, P.S. and Rajesh, R. 2018. Cyber security to information assurance: an overview. *International Journal on Recent Researches in Science, Engineering & Technology* (IJRRSET), **6**(4): 8-14.

12. Shah, P. and Agarwal, A. 2020. Cybersecurity behaviour of smartphone users in India: an empirical analysis. *Information & Computer Security,* **28**(2): 293-318.

13. Wall, D.S. 2024. Cybercrime: The transformation of crime in the information age. John Wiley & Sons.