CYBER CRIMES AND INDIA'S NATIONAL SECURITY: A RISING THREAT IN THE CYBER DOMAIN

ABHISHEK SHARMA

INTRODUCTION

Cyber space is considered to be the fifth domain of warfare. Even though it is placed last in the order, it still plays a critical role. However, if analysed, its direct impact would likely be the greatest on a state's and its citizens' security. India currently stands among the community of nations that aims to achieve increased digital penetration and access to internet networks and mobile devices to its citizens. This expansion has brought with it economic benefits and ease of living, but it has also brought with it the threat of cyber crimes, which are now increasingly becoming a threat to the citizens and the state's national security. Particularly after the COVID-19 pandemic, the number of cyber crimes has increased substantially; the victim count has increased by 69 per cent, the largest increase ever since 2001.[1] In India, cyber

Mr **Abhishek Sharma** is a Research Associate at the Centre for Air Power Studies, New Delhi.

1. "Cybercrime Statistics," *Surfshark*, https://surfshark.com/research/data-breach-impact/statistics. Accessed on February 1, 2024.

crime has increased by 300 per cent.[2] In the last decade, India has focussed on countering cyber crimes and their national security implications.[3] However, India still lags in having a comprehensive institutional mechanism that works at the central and state levels to deal with cyber crimes.

CYBER CRIMES AND NATIONAL SECURITY IN INDIA

India is the fifth-largest economy in the world and aims to become the third-largest by the end of this decade.[4] As the future economic growth will be driven by the 4th Industrial Revolution based on digitally driven technologies, it becomes critical to bring in systems that address their safety. Therefore, safeguarding these technologies would be an integral part of the economic security of India, which is part of India's national security. India's efforts on tackling cyber crimes are targeted at two different types of audience. The first are the big businesses and corporations, and, the second, the common citizens. The Indian approach to cyber safety is still work in progress as opposed to the developed countries like the US which have established mechanisms to deal with this issue.[5] However, the recent data protection Bill attempts to address the long-term gap, particularly concerning privacy and personal data. The Bill becomes more important in today's digital age, when citizens are more than ever connected to the internet, with increased chances of being targeted by cyber crimes. Today, 800 million Indians have a digital presence, and this is expected to increase by 400 million by 2025, an increase of 231

2. Sumit Bhattacharjee, "Visakhapatnam: Cybercrime Has Become a National Security Issue, Says Commissioner of Police," *The Hindu*, June 16, 2022, https://www.thehindu.com/news/cities/Visakhapatnam/cybercrime-has-become-a-national-security-issue-says-commissioner-of-police/article65533020.ece. Accessed on February 1, 2024.
3. Lior Tabansky, "Cybercrime: A National Security Issue?," *Military and Strategic Affairs* 4, no. 3, December 2012, pp.117–136, https://www.inss.org.il/he/wp-content/uploads/sites/2/systemfiles/SystemFiles/MASA4-3Engd_Tabansky.pdf. Accessed on February 1, 2024.
4. "India Will Become 3rd Largest Economy in My 3rd Term: PM Modi," *The Economic Times*, July 26, 2023, https://economictimes.indiatimes.com/news/india/india-will-become-third-largest-economy-in-my-third-term-pm-modi/articleshow/102145334.cms?from=mdr. Accessed on February 1, 2024.
5. The White House, "National Cybersecurity Strategy," March 2023, https://www.whitehouse.gov/wpcontent/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf. Accessed on February 1, 2024.

per cent internet connections in just eight years.[6] Access to cheaper data has only accelerated the adoption of the internet and associated technologies in India. This means more people with an online presence and, hence, more threats from cyber crimes. In September 2023, India registered 10.58 billion transactions amounting to Rs 15.76 lakh crore.[7] These data show how fast India is adopting these technologies, with the risks from cyber crimes increasing. Among all the stakeholders, be it citizens, businesses, corporations, states, and centre, the central government is the biggest stakeholder in ensuring the safety of digital technologies for its purpose, that is, e-governance. The use of the Digital Public Infrastructure (DPI) architecture, which consists of the aadhar (identity), payment mechanism (UPI), and data (government-issued documents) established by the central government, is now an essential instrument of governance in India, and it is critical to safeguard it.[8] The data proves that it is vital for this: in seven years, the government transferred Rs 23 lakh crore directly to beneficiaries from 52 ministries covering 300 schemes, which saved the government Rs 2 lakh crore.[9] Until now, the citizens have wholeheartedly accepted the digital transition, trusting the DPI. However, the trust will eventually erode if the infrastructure comes under attack and is used for furthering cyber crimes. Hence, for both political and security interests, it becomes vital for the state to enhance security and safety mechanisms.

India defines cyber crimes as "a broad term that is used to define criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything

6. Ministry of Home Affairs, "Union Home and Cooperation Minister Shri Amit Shah Addressed the National Conference on Cyber Safety and National Security in New Delhi Today," Press Information Bureau, June 20, 2022, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1835559. Accessed on February 1, 2024.
7. "UPI Transactions In India Cross 10 Billion Mark For First Time In August," *NDTV*, September 1, 2023, https://www.ndtv.com/india-news/upi-transactions-cross-10-billion-mark-in-august-here-s-how-it-plans-to-go-global-4347391. Accessed on February 1, 2024.
8 "India Stack," indiastack.org, https://indiastack.org/. Accessed on February 1, 2024.
9. Ministry of Home Affairs, "Union Home and Cooperation Minister Shri Amit Shah Addressed the National Conference on Cyber Safety and National Security in New Delhi Today," Press Information Bureau, June 20, 2022, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1835559. Accessed on February 1, 2024.

from electronic wracking to denial of service attacks."[10] Cyber crimes have become a severe national security threat for countries across regions, covering the number of victims targeted and the amount of funds lost. From 2001 till 2022, the number of victims increased 16 times (6 to 9 every hour), and the amount of financial losses almost 570 times (from $2,000 to $1.2 million per hour).[11] In 22 years, the number of victim accounts touched 7,303,267, and losses amounted to $36.4 billion.[12] Microsoft India Group Head and Director Ashutosh Chadha has said that the losses from cyber crimes cost $6 trillion annually and are expected to reach $10 trillion by 2025. The economic costs of cyber crimes are enormous for a state, and they impact the country's growth, and the profits and revenues of companies and corporations. While targeting individuals, the age group most vulnerable to cyber crimes comprises people over 60, and the least vulnerable are people below 20 years of age.[13] According to the 2022 Internet Crime Report released by the Federal Bureau of Investigation (FBI) in the US, citizens below 20 years of age registered 15,782 complaints compared to 88,262 from people above the age of 60; the former suffered a loss of $210.5 million as opposed to $3.1 billion by the latter.[14] In India, digital literacy being comparatively less, the risk is quite serious. These cyber crimes erode the trust of institutions and companies in the cyber domain. They impact the "strategic issue that shapes product capability, organisational effectiveness, and customer relationships."[15] All this

10. Government of India, "UN Ad Hoc Committee (AHC) to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes: Indian Contribution for 2nd Session of AHC Criminalization, General Provisions and Procedural Measures and Law Enforcement," *UNODC*, August 2022, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_intersessional_consultations/Revised_Indian_Text_for_UN_AHC_published_on_12.5.2022_-Revised_.pdf. Accessed on February 1, 2024.
11. "Cybercrime Statistics," *Surfshark*, https://surfshark.com/research/data-breach-impact/statistics. Accessed on February 1, 2024.
12. Ibid.
13. Ibid.
14. "FBI Internet Crime Report 2022," Internet Crime Complaint Centre, 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. Accessed October 17, 2023.
15. "Cyber Security Threats Are Biggest Risk to National Security: NCSC," *The Hindu*, June 24, 2022, https://www.thehindu.com/news/national/cyber-security-threats-

impacts national security. While addressing the convocation at the Gujarat Forensic Science University, the Indian prime minister said, "These cyber crimes are not just a risk to the privacy of citizens. But they also affect our important infrastructure such as financial institutions, power stations, and hospitals. Not only for the national security of India but for every country in the world, this is a challenge."[16] Indian Home Minister Amit Shah made the same assertion.[17] This sentiment is also echoed at the state level. Chief Minister of Karnataka, Mr. Siddaramaiah, expressed his concern regarding the rise of cyber crimes as a national security threat; he said, "It not only harms an individual but also poses a threat to national security. Cyber attacks and crimes have led to financial losses, damaged reputations, leading to endangering lives in some of the cases."[18] Similarly, National Cyber Security Coordinator (NCSC) Rajesh Pant has called "cyber security as one of the biggest risks to national security."[19]

INDIA'S NATIONAL SECURITY AND CYBER CRIMES

The cases of cyber crimes have drastically increased in India as illustrated in Table 1, particularly as the digitisation process has increased with the proliferation of services like banking, e-marketing, teaching, social networking, and official and personal communication. In 2018, Union Home Minister Amit Shah, informed the Rajya Sabha that cyber crime cases have increased in India—9,622 in 2014, 11,592 in 2015, and 12,317 in 2016.[20] The increase in cyber crimes from 2014 to 2015 was 24 per

are-biggest-risk-to-national-security-ncsc/article65558692.ece. Accessed on February 1, 2024.

16. Ibid.
17. n.6.
18. "Cybercrimes Are Threat to National Security: Karnataka CM Siddaramaiah at DGPs' Conference," *The Indian Express*, September 14, 2023, https://indianexpress.com/article/cities/bangalore/cybercrimes-threat-national-security-karnataka-cm-siddaramaiah-dgp-conference-8938874/. Accessed on February 1, 2024.
19. n.15.
20 Utpal Bhaskar, "Cyber-Crime Cases in India Almost Doubled in 2017: Mint," *Livemint*, October 22, 2019, https://www.livemint.com/companies/news/cyber-crime-cases-in-india-almost-doubled-in-2017-11571735243602.html. Accessed on February 1, 2024.

cent. To make sense, the number of cases in 2006 was a mere 453.[21] The number has only risen, almost doubling in 2017, numbering 21,796, constituting 56 per cent (12,213) fraud cases and 6.7 per cent (1,460) sexual exploitation cases.[22] All these reported cases are based on conservative figures as many remain unreported. Even the number of people arrested for cyber crimes has increased by 40 per cent—5,752 in 2014 to 8,121 in 2015.[23] In 2016, Uttar Pradesh, Rajasthan, Maharashtra, Telangana, and Karnataka reported the highest number of cases, and most arrests were made from Bihar, Andhra Pradesh and Assam.[24] As mentioned earlier, the largest number of cyber crimes comprise fraud cases.[25] In 2021, 14,007 cases of fraud were registered through online apps, particularly digital lending cases. In a reply in the Lok Sabha. Mr Bhagwat Karad, minister of state for finance, said that the Reserve Bank of India (RBI) has taken steps "to firm up the regulatory framework for digital lending and enhancing customer protection and making the digital lending ecosystem safe and sound."[26] Some sections of Indian society are particularly vulnerable to cyber crimes, such as women who have seen increasing cases of cyber abuse through digital bullying and stalking.[27]

21 Vishwa Mohan, "Cyber Crimes in India Grew 20% in 2015 over Preceding Year," *The Times of India*, August 31, 2016, https://timesofindia.indiatimes.com/india/cyber-crimes-in-india-grew-20-in-2015-over-preceding-year/articleshow/53951437.cms. Accessed on February 1, 2024.

22 Bhaskar, n. 20.

23 Mohan, n. 21.

24 Ibid.

25 Ministry of Home Affairs, "Increase in Cyber Fraud Cases," Press Information Bureau, July 26, 2022, https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1845004. Accessed on February 1, 2024.

26. "14,007 Cyber Fraud Cases Were Registered in India in 2021," *The Times of India*, July 24, 2023, https://timesofindia.indiatimes.com/india/14007-cyber-fraud-cases-were-registered-in-india-in-2021/articleshow/102085429.cms?from=mdr. Accessed on February 1, 2024.

27 Geeta Pandey, "Rising Crimes against Indian Women in Five Charts," BBC News, September 13, 2022, https://www.bbc.com/news/world-asia-india-62830634. Accessed on February 1, 2024.

Table 1: Number of Cyber Crimes in India

Year	Number of Cyber crime
2005	481
2006	453
2012	3,477
2013	5,693
2014	9,622
2015	11,592
2016	12,317
2017	21,796
2018	2,08,456
2019	3,94,499
2020	11,58,208
2021	14,02,809
2022	13,91,457

Source: Table created by the author based on different sources.[28]

Traditionally, India has not focussed much on the cyber security domain to protect itself from both state and non-state actors, be it the targeting of critical infrastructure like water pipelines, dams, electricity grids, hospitals, or individual attacks like phishing, sextortion, romance scams, etc. Even in the media, the subject doesn't get much attention. In 2022, however, the threat became more public with the All India Institute of Medical Science (AIIMS) ransomware attack. This also forced the government to come up with guidelines and Standard Operating Procedures (SOPs) to deal with these threats. Following the incident, the central government established the "*modus operandi* of 50 cyber attacks".[29] In an effort to work on every segment of total policing— "maintaining law and order, investigating the crime and ensuring that the guilty are punished through judicial

28. Bhaskar, n.20; Daniel Imber, "The Latest Cyber Crime Statistics (Updated October 2023)," AAG IT Services, October 2, 2023, https://aag-it.com/the-latest-cyber-crime-statistics/#:~:text=In%20Q3%20of%202022%2C%2022.3,and%20Spain%20(3.9%20million). Accessed on February 1, 2024.; Lok Sabha Secretariat, "Cyber Security Attacks," February 2023, https://pqars.nic.in/annex/259/AU1043.pdf. Accessed on February 1, 2024.
29. "Cyber Threat Now a Matter of National Security, Says Amit Shah," *The Economic Times*, March 29, 2023, https://economictimes.indiatimes.com/news/india/cyber-threat-now-a-matter-of-national-security-says-amit-shah/articleshow/99070814.cms?from=mdr. Accessed on February 1, 2024.

investigation"—India has opened universities for every segment and the National Forensic Science University is a part of it.[30]

INDIA AND CYBER CRIME GOVERNANCE

In India, 'police' and 'public order' fall under the state governments' jurisdiction and so does the responsibility for "prevention, detection, investigation and prosecution of crimes, including cyber crime".[31] The central government has limited power to intrude in this territory. It only "supplements the initiatives of the state governments through advisories and financial assistance under various schemes for their capacity building."[32] The ministry that holds the authority to legislate and assist at the central level is the Ministry of Home Affairs (MHA) which has a dedicated division to handle issues related to cyber security known as the Cyber and Information Security (C&IS) division.[33] The ministry's C&IS divison's C&IS-II desk focusses on cyber crimes, and its objective is "to strengthen the mechanism to deal with cyber crimes in a comprehensive and coordinated manner" and support the states and Union Territories through financial assistance under the Cyber Crime Prevention against Women and Children (CCPWC) scheme for facilitating the state's "efforts for setting up of cyber forensic-cum-training laboratories, training, and hiring of junior cyber consultants."[34] The Centre has provided Rs 2,971.51 crore for modernising the state police and acquiring "training gadgets, cyber policing equipment, weapons and advanced communication and forensic equipment."[35] Currently, the cases of cyber crimes

30 Ministry of Home Affairs, "Union Home Minister and Minister of Cooperation, Shri Amit Shah Lays the Foundation Stone of Guwahati Campus of National Forensic Science University (NFSU) in Assam Today," Press Information Bureau, May 25, 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1927340. Accessed on February 1, 2024.

31. Ministry of Electronics & IT, "Prevention of Cyber Crimes," Press Information Bureau, July 22, 2022, https://pib.gov.in/PressReleasePage.aspx?PRID=1845321. Accessed on February 1, 2024.

32. Ibid.

33 Ministry of Home Affairs, "CYBER AND INFORMATION SECURITY (C&IS) DIVISION," https://www.mha.gov.in/en/divisionofmha/cyber-and-information-security-cis-division. Accessed on February 1, 2024.

34. n. 31, and Ibid.

35. Anish Yande, "Saved Rs 188 Crore in 1.1 Lakh Cyber Crime Cases: Govt Tells Lok Sabha," *Hindustan Times*, December 21, 2022, https://www.hindustantimes.

are dealt with under the existing Information and Technology Act, 2002, along with the Indian Penal Code, with punishment ranging from two years, life imprisonment to the death penalty.[36] The home minister has expressed his belief that cyber awareness is an important pillar to address safety issues and has further stated the government initiatives in this direction, such as to "create awareness amongst the people through various steps like cyber cleanliness, measures for prevention of cyber crimes, popularization of crime reporting portal, popularization of cyber financial crime reporting helpline number."[37] The process started in 2015 when the MHA accepted the recommendation of an expert group to set up a National Cyber Crime Coordination Centre (IC4).[38] Now, India has an IC4 whose objective is "to overcome obstacles by assisting state Law Enforcement Agencies (LEAs) in all aspects regarding cyber crime intelligence development and sharing, training, forensics, research, and also by facilitating exchange of information and cooperation amongst them".[39] The aim is to make cyber space more safe with a mission to "create an effective framework and ecosystem for the prevention, detection, investigation, and prosecution of cyber crimes in the country".[40] The cyber security division in the MHA takes care of cyber crimes through the existing institutions. The MHA works on the prevention of cyber crimes under its seven pillars.[41] These are as following:

1. National Cyber Crime Threat Analytics Unit (NCTAU).
2. National Cyber Crime Reporting Portal (NCRP).
3. National Cyber Crime Training Centre (NCTC).
4. National Cyber Crime Research and Innovation Centre (NCR&IC).

com/india-news/saved-rs-188-crore-in-1-1-lakh-cyber-crime-cases-govt-tells-lok-sabha-101671598414429.html. Accessed on February 1, 2024.

36. Ministry of Women and Child Development, "Many Measures in to Check Cyber Crimes against Women: Dr. Virendra Kumar," Press Information Bureau, July 26, 2018, https://pib.gov.in/PressReleasePage.aspx?PRID=1540340. Accessed on February 1, 2024.
37. n.6.
38. Ministry of Home Affairs, "National Cyber Crime Coordination Centre," Press Information Bureau, December 23, 2015, https://pib.gov.in/newsite/PrintRelease.aspx?relid=133895. Accessed on February 1, 2024.
39. "CyTrain," National Cybercrime Research Bureau, https://cytrain.ncrb.gov.in/local/staticpage/view.php?page=CyTrain. Accessed on February 1, 2024.
40. Ibid.
41. n.17.

5. Joint Cyber Crime Coordination (JCCC).
6. National Cyber Crime Ecosystem Management Unit (NCEMU).
7. National Cyber Crime Forensic Laboratory (NCFL).

The Government of India (GoI) has also worked on spreading awareness and knowledge about cyber crimes, particularly through social media platforms via X (earlier Twitter) '@ Cyberdost', Facebook(CyberDostI4C), Instagram (cyberdosti4c), Telegram(cyberdosti4c).[42] The MHA also operates the number 1930 cyber crime helpline and regularly runs targeted campaigns about safety and hacking issues.[43] In addition, "capacity building/training of law enforcement personnel/prosecutors/judicial officers", "issuance of alert/advisories", and "improving of cyber forensic facilities" are routinely undertaken.[44] Under the IC4, the National Cyber Crime Training Centre emphasises "capacity building focussed on combatting cyber crimes, impact containment and investigations".[45] The NCRB also regularly hosts cyber hackathons, cyber *Jagrookta Diwas*, and cyber challenges in association with organisations and the participation of law enforcement agencies, tech companies, students, and cyber experts with "an aim to enhance, deepen the skills of police personnel."[46] Along with this, the MHA releases a newsletter and provides a manual on cyber crimes on NCRP.[47] The MHA has focussed on the safety and security of women and children by establishing a new scheme, the CCPWC, for handling cyber crimes against women

42. Ministry of Home Affairs, "Cyber Crime Awareness," Cytrain.ncrb.gov.in, https://cytrain.ncrb.gov.in/staticpage/r0.php.; PIB Delhi, "SCAM BY FRAUDSTERS," Press Information Bureau, March 21, 2023, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1909195. Accessed on February 1, 2024.
43. Ministry of Home Affairs, "Cyber Frauds Helpline," Press Information Bureau, April 6, 2022, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1814120. Accessed on February 1, 2024.
44. n. 31.
45. n. 39.
46. "CCTNS Hackathon & Cyber Challenge 2023," *NCRB*, https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/custom/1691130450Hackathon-Result-2023.pdf. Accessed on February 1, 2024.; Ministry of Home Affairs, "SCAM BY FRAUDSTERS," Press Information Bureau, March 21, 2023, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1909195. Accessed on February 1, 2024.
47. Ministry of Home Affairs, Ibid; "Cyber Awareness," National Cyber Crime Reporting Portal, https://cybercrime.gov.in/Webform/CyberAware.aspx. Accessed on February 1, 2024.

and children focussing on "online cyber crime reporting platform, one national level cyber forensic laboratory, training of police officers, judges and prosecutors, cyber crime awareness activities, and research and development."[48] A separate website has also been set up by the MHA to report cyber crimes (www.cybercrime.gov.in), with special focus on children and women.[49] In 2021, for reporting cases of financial fraud, a Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS) was launched with a helpline number 155260, later changed to 1930.[50] The CFCFRMS was set up to develop "quick reporting of financial cyber frauds and monetary losses suffered due to use of digital banking/credit/debit cards, payment intermediaries, UPI, etc" and a platform where all relevant stakeholders like LEAs, banks, NPCI, RBI, and payment wallets can work together.[51] In December 2022, Minister of State Ajay Mishra Teni, in a reply in the Lok Sabha, said that a total of 6 lakh complaints, were registered on the CFCFRMS portal and in 1.1 lakh complaints, an amount of Rs. 188 crore was recovered.[52] As per the National Cyber Crime Helpline 1930 and the NCCRP, an estimated Rs 735 crore had been saved from fraudsters' hands until September 30 2023.[53] With the proliferation of mobile applications, the risk of cyber crimes like fraud, extortion, and theft has recently increased. To counter this, the government routinely restricts access to applications to Indian

48. Ministry of Home Affairs, "Cyber Crime Prevention against Women and Children," Press Information Bureau, January 8, 2019, https://pib.gov.in/Pressreleaseshare.aspx?PRID=1559115. Accessed on February 1, 2024.
49. n. 36; n. 44.
50. "Govt Launches National Helpline No. to Report Cyber Crime; All You Need to Know: Mint," *Livemint*, June 21, 2021, https://www.livemint.com/news/india/govt-launches-national-helpline-no-to-report-cyber-crime-all-you-need-to-know-11623950388095.html. Accessed on February 1, 2024.
51. "NATIONAL CYBERCRIME REPORTING PORTAL [NCRP]," Indian Cybercrime Coordination Centre (I4C), https://i4c.mha.gov.in/ncrp.aspx. Accessed on February 1, 2024.
52. Yande, n. 35.
53. @Cyberdost, "#AskCyberDost | As per the Records, National Cybercrime Helpline 1930 & National Cybercrime Reporting Portal Has Saved over Rs 765 Crores of Defrauded Money from Reaching the Hands of Fraudsters till 30.09.2023.," *X/Twitter*, October 7, 2023, https://twitter.com/Cyberdost/status/1710650782520164652. Accessed on February 1, 2024.

citizens. On the advice of IC4, the Home Ministry blocked access to 500 internet based applications.[54]

INDIA, CYBER CRIMES AND THE WAY FORWARD

The 2013 National Cyber Security Strategy document currently dictates the cyber security approach.[55] However, with the new Cyber Security Strategy to be released soon, it seems that cyber crimes will be given the required attention, with IC4 continuing to be the nodal agency for cyber crimes.[56] The National Cyber Security Coordinator, Lieutenant General (Dr) Rajesh Pant, has said that the "new strategy would cover the entire ecosystem of cyber security, and proposes a national approach."[57] He further stated that the strategy would be based on Common But Differentiated Responsibilities (CBDR) between individuals, businesses, academia, and the government, where individuals have "good cyber hygiene," and enterprises have "zero-trust architecture."[58] Going forward, the central government can support the states by providing greater financial assistance, policy guidelines, and bringing laws through amendments, enacting new legislation, and introducing notifications to counter cyber crimes.[59] In addition, bringing guidelines and SOPs routinely for central agencies and public institutions is important to keep up

54. Vijaita Singh, "More than 500 Apps Blocked on the Advice of Cyber-Crime Centre, Says Home Minister," *The Hindu*, March 29, 2023, https://www.thehindu.com/news/national/more-than-500-apps-blocked-on-the-recommendation-of-cyber-crime-centre-amit-shah/article66672482.ece. Accessed on February 1, 2024.
55. "National Cyber Security Policy -2013," https://www.meity.gov.in/writereaddata/files/downloads/National_cyber_security_policy-2013%281%29.pdf. Accessed on February 1, 2024.
56. "CYBER SECURITY ATTACKS," February 2023, https://pqars.nic.in/annex/259/AU1043.pdf. Accessed on February 1, 2024; ET Telecom, "National Cybersecurity Strategy 2023 May Come out Soon: Pant," *ETTelecom.Com*, February 20, 2023, https://telecom.economictimes.indiatimes.com/news/national-cybersecurity-strategy-2023-may-come-out-soon-pant/98093316#:~:text=The%20existing%202013%20policy%20is,Pant%2C%20national%20cybersecurity%20coordinator%20said. Accessed on February 1, 2024.
57. ET Telecom, Ibid.
58. Ibid.
59. Ministry of Women and Child Development, "Measures to Prevent Cyber Crimes against Children," Press Information Bureau, July 20, 2022, https://www.pib.gov.in/PressReleseDetail.aspx?PRID=1843008. Accessed on February 1, 2024.

with the new Tactics Technologies Products (TTPs).[60] The number of cyber crime police stations has increased from 202 in 2021 to 262 in 2022 in India, which is a positive development, but more needs to be done.[61] Here, the responsibility of the state governments becomes greater in policy, practice, technology adaptation, infrastructure, and implementation, like many states have undertaken such as UP, Karnataka, Maharashtra, and Telangana.[62] Cyber training needs to be imparted to police officers, making them cyber warriors as the Telangana police has done.[63] Many cities are now following the Telangana model, which has a recovery state of 20 per cent as opposed to 7 per cent nationally.[64] A holistic approach and closer engagement between the central and state governments is the need of the hour.

60. "Safe & Trusted Internet: Guidelines on Information Security Practices for Government Entities," *Www.Cert-in.Org.In*(Indian Computer Emergency Response Team, MEITY, Government of India, June 30, 2023). Accessed on October 18, 2023, https://www.cert-in.org.in/PDF/guidelinesgovtentities.pdf. Accessed on February 1, 2024.
61. Ministry of Home Affairs, "Cyber Crimes and Frauds," Press Information Bureau, December 13, 2022, https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=1883066. Accessed on February 1, 2024; Ministry of Home Affairs, "Central Government Has Taken Various Measures to Supplement the Efforts of States/UTs Including Capacity Building of Law Enforcement Agencies (LEAs) to Deal with Cybercrimes," Press Information Bureau, February 8, 2023, https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1897437. Accessed on February 1, 2024.
62. "Karnataka Govt Approves Cyber Security Policy," *Hindustan Times*, August 10, 2023, https://www.hindustantimes.com/cities/bengaluru-news/karnataka-govt-approves-cyber-security-policy-101691678894791.html. Accessed on February 1, 2024; "Hyderabad Police to Go Hitech, Use AI, Have Support Centre Unit for Cybercrimes Https://Www.Newstap.in/Metro-City/Hyderabad-Police-to-Go-Hitech-Use-Ai-Have-Support-Centre-Unit-for-Cybercrimes-1456868?Infinitescroll=1," *NewsTap*, January 11, 2023, https://www.newstap.in/metro-city/hyderabad-police-to-go-hitech-use-ai-have-support-centre-unit-for-cybercrimes-1456868?infinitescroll=1. Accessed on February 1, 2024; Chaitanya Marpakwar, "Cabinet OKs Rs 837 Crore Plan, Call Centre to Fight Cyber Crime," *The Times of India*, September 7, 2023, https://timesofindia.indiatimes.com/city/mumbai/cabinet-oks-rs-837-crore-plan-call-centre-to-fight-cyber-crime/articleshow/103448281.cms?from=mdr. Accessed on February 1, 2024; "57 New Cyber Police Stations to Be Set up in UP in Two Months," *Deccan Herald*, August 26, 2023, https://www.deccanherald.com/india/uttar-pradesh/57-new-cyber-police-stations-to-be-set-up-in-up-in-two-months-2662083#. Accessed on February 1, 2024.
63. "800 Police Stations to Have Cyberwariors, Says Anjani," *Deccan Chronicle*, April 27, 2023, https://www.deccanchronicle.com/nation/current-affairs/260423/800-police-stations-to-have-cyberwariors-says-anjani.html. Accessed on February 1, 2024.
64. Ishita Singh, "Gurgaon Set to Go the Telangana Way in Tackling Cybercrime," *The Times of India*, September 22, 2023, https://timesofindia.indiatimes.com/city/gurgaon/city-set-to-go-the-telangana-way-in-tackling-cybercrime/articleshow/103850828.cms?from=mdr. Accessed on February 1, 2024.