ORIGINAL RESEARCH PAPER

Economics

A STUDY ON GLOBALIZATION AND CYBERCRIMES IN INDIA

KEY WORDS: Cyber Crime, globalization, crime rate, financial cyber crime, safeguards

Dr. Pramod Pandurangrao Lonarkar

Associate Professor, School of Social Sciences, S.R.T.M. University, Nanded.

ABSTRACT

In an era marked by globalization and technological advancements, cybercrimes have emerged as a pressing concern, particularly in India. This abstract encapsulates the multifaceted landscape of cyber threats and the challenges faced by the nation's cybersecurity infrastructure. It discusses the escalating trend of cybercrimes, especially financial frauds, across states and metropolitan cities, underscoring the urgent need for comprehensive measures to combat these threats. Drawing on data from the National Crime Records Bureau and scholarly research, the abstract highlights key objectives and methodologies of the study, shedding light on the trends, rates, and patterns of cybercrimes in India. Furthermore, it explores potential safeguarding measures, including legal reforms, capacity building, international cooperation, and public-private partnerships, aimed at bolstering India's cyber resilience. By implementing these strategies, India can effectively mitigate cyber risks and ensure a secure digital environment for its citizens, thereby safeguarding its digital assets and societal well-being in the face of evolving cyber threats.

INTRODUCTION:

Globalization, cybercrimes, and consumer security are interconnected phenomena that shape the modern landscape of commerce, communication, and societal interactions. As the world becomes more interconnected, the benefits of globalization come with new challenges, particularly in the realm of cybersecurity and the protection of consumer interests. In the contemporary era of globalization, the proliferation of digital technologies has brought about unprecedented connectivity and opportunities for economic growth in India, but it has also ushered in a simultaneous rise in cybercrimes, posing significant challenges to the country's cybersecurity infrastructure and law enforcement agencies (Gupta, 2019; Mishra & Rai, 2021). The exponential growth of internet penetration, coupled with the rapid adoption of smartphones and digital payment systems, has created a fertile ground for cybercriminal activities ranging from financial frauds, identity thefts, to cyberbullying and cyber warfare (Sinha & Jain, 2020; Singh & Garg, 2018). This surge in cyber threats can be attributed to various factors such as the lack of robust cybersecurity laws and regulations, inadequate awareness among the populace regarding cyber hygiene practices, and the evolving sophistication of cybercriminals exploiting vulnerabilities in the digital ecosystem (Verma, 2017; Kaur & Kaur, 2019; Pandey & Singh, 2020). Additionally, the borderless nature of cyberspace presents unique jurisdictional challenges, often complicating the process of apprehending and prosecuting cyber offenders (Sharma, 2021). Therefore, as India continues to integrate into the global digital economy, addressing the escalating menace of cybercrimes demands a multifaceted approach encompassing legal reforms, capacity building, international cooperation, and public-private partnerships to safeguard the nation's digital assets and ensure a secure cyber environment for its citizens (Patel & Mishra, 2022). This paper provides the exploration on the cyber crime situation in India. Following are the objectives of this study.

Objectives of the Study:

1) To explore the trend of cyber crime cases and the cyber crime rate in India.
2) To highlight the cybercrime cases across the state and metropolitan cities in India.
3) To discusses on the financial cyber crimes.
4) To suggest the measures for safeguarding the nation's digital assets and ensure a secure cyber environment.

METHODOLOGY OF RESEARCH:

To satisfy the above objectives, this study explores the cyber crime status in India by analysing the secondary data given in National Crime Records Bureau. The use of figures and simple statistics is made for the data analysis.

Globalization:

In economics globalization refers to the process of increasing interconnectedness and interdependence of economies across the world through the exchange of goods, services, capital, technology, and information. It is driven by advancements in transportation, communication, and technology, which have facilitated the integration of markets on a global scale. In a globalized economy, barriers to trade and investment are reduced or eliminated, allowing businesses to expand their operations internationally and access larger consumer markets. This phenomenon has led to the emergence of global supply chains, multinational corporations, and the free flow of capital across borders. Globalization has both benefits and challenges, including increased economic growth, efficiency, and innovation, as well as concerns about inequality, cultural homogenization, and vulnerability to economic shocks.

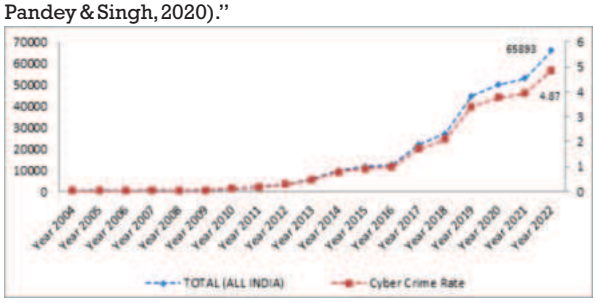
Globalization facilitates the free flow of goods, services, and capital across borders, promoting economic growth and market access for businesses. Globalization has driven the digital transformation of industries, enabling faster communication, innovation, and business processes. Globalization fosters cultural exchange, allowing consumers to access a diverse range of products, services, and ideas. The global digital economy facilitates seamless financial transactions, providing cybercriminals with opportunities for fraud. Globalization has undeniably transformed India's economic landscape, fostering increased interconnectedness and technological advancements. However, alongside these benefits, the country has encountered new challenges, notably in the realm of cybercrime. The following figures and descriptions portray India's situation on cybercrime in general and across states and union territories (UTs) in particular.

The Trend Of Cyber Crime Cases And The Rate In India:

In the following diagram the trajectory of cybercrime in India over a period spanning from 2004 to 2022, is presented in the form of total number of reported cybercrimes and the corresponding cybercrime rate per 100,000 population in the country.

A notable observation from the data is the consistent upward trend in both the total number of cybercrimes reported and the cybercrime rate over the years. For instance, in 2004, there

were 347 reported cybercrimes with a cybercrime rate of 0.03 per 100,000 population. However, by 2022, these figures had significantly escalated to 65,893 reported cybercrimes with a cybercrime rate of 4.87 per 1,00,000 population. "The data depicts a steady increase in cybercrimes in India over the past two decades, indicating a growing concern for cybersecurity in the country. This trend can be attributed to various factors such as the rapid expansion of digital infrastructure, increased internet penetration, proliferation of smartphones, and the growing reliance on digital platforms for everyday activities including banking, shopping, and social interaction (Singh & Garg, 2018; Mishra & Rai, 2021). Furthermore, advancements in cybercrime techniques and the emergence of sophisticated cybercriminal networks have also contributed to the surge in cybercrimes (Gupta, 2019; Pandey & Singh, 2020)."



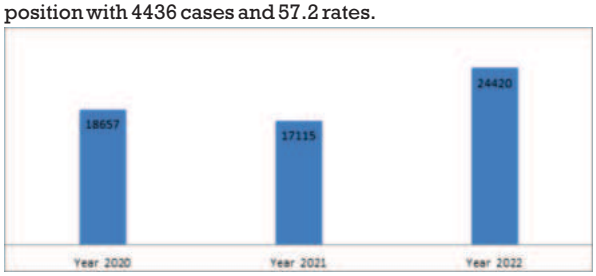
Source: Crime in India 2022, NCRB Ministry of Home Affairs.

Figure 1: Total Cyber Crime Cases and Crime Rate in India (2004-2022)

The Cyber Crime In Metropolitan Cities:

The metropolitan cities encompass the huge population and the financial resources, leading to the more use of computers, computer networks and networked devices and hence more exposed to the crimes. The total numbers of cyber crime cases registered in 19 metropolitan cities during are last three years (2020 to 2022) are 18.65 thousand, 17.11 thousand and 24.42 thousand. The rate of cyber crime in metropolitan cities is also very high i.e. 21.4 in comparisons with the rate at all India level i.e. 4.87 cases per lakh population.

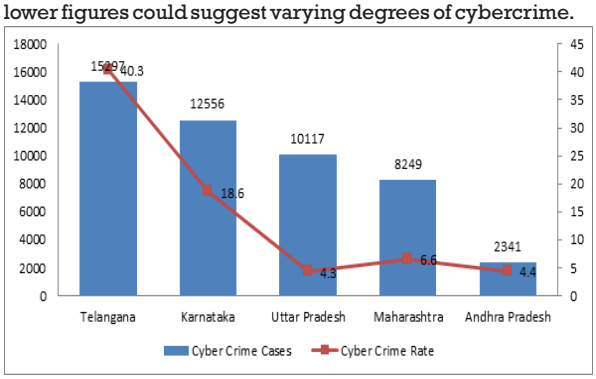
Among the 19 metropolitan cities Bengaluru, also known as "Silicon Valley of India" for its dominance in Information Technology reported highest cyber crime cases i.e. 9940 with 117 cyber crime rate in 2022. This is followed by Mumbai with 4727 cases and 25.7 rate. Hyderabad is also at the third position with 4436 cases and 57.2 rates.



Source: Crime in India 2022, NCRB Ministry of Home Affairs.
Figure 2: Cyber Crime cases in Metropolitan Cities (2020-2022)

Status Of Cyber Crime Across The States:

The cybercrime landscape in Indian states reflects a complex interplay of various factors such as technological advancement, internet penetration, regulatory frameworks, law enforcement capabilities, and socio-economic dynamics. Looking at the data provided for the top five states with registered cybercrime cases, it's evident that Telangana, Karnataka, Uttar Pradesh, Maharashtra, and Andhra Pradesh are among the states grappling with significant cybercrime challenges. Telangana emerges as the state with the highest number of reported cybercrime cases (refer the following diagram). The Karnataka follows closely, underscoring the prominence of cybercrime activities in major tech hubs like Bengaluru. Uttar Pradesh's high cybercrime figures may reflect the challenges faced in managing cyber threats in densely populated states with varying levels of digital literacy and infrastructure development. Maharashtra's relatively lower but still substantial cybercrime cases highlight the importance of addressing cybersecurity concerns in urban centers like Mumbai and Pune, which are crucial economic hubs. Andhra Pradesh's comparatively lower figures could suggest varying degrees of cybercrime.



Source: Crime in India 2022, NCRB Ministry of Home Affairs.
Figure 3: Top five States in Cyber Crime Cases (2022)

Deriving the mean cyber crime rate during 2004 to 2022 for Indian States it is found that the mean Crime rate in Telangana is at the top i.e. 13.77, followed by 4.60 in Karnataka, 2.64 in Assam, 1.74 in Maharashtra and 1.47 in Goa. The Standard deviation values indicate that except Goa all other states stand at the top in crime rate volatility. In place of Goa the state Uttar Pradesh stood at the fifth position (See table No. 1).

Table No. 1: The Crime Rate Across State (2004-2022).

States	Mean	Standard Deviation	Standard Error
Telangana	13.77	14.71	5.56
Karnataka	4.60	6.67	1.53
Assam	2.64	3.95	0.91
Maharashtra	1.74	1.98	0.45
Uttar Pradesh	1.40	1.84	0.42
Uttarakhand	0.99	1.73	0.40
Odisha	1.18	1.65	0.38
Andhra Pradesh	1.26	1.47	0.34
Goa	1.47	1.44	0.33
Meghalaya	1.22	1.36	0.31
Jharkhand	0.93	1.21	0.28
Manipur	0.54	0.90	0.21
Haryana	0.89	0.89	0.20
Sikkim	0.32	0.87	0.20
Rajasthan	0.85	0.86	0.20
Arunachal Pradesh	0.66	0.81	0.19
Mizoram	0.49	0.73	0.17
Gujarat	0.60	0.71	0.16
Tamil Nadu	0.40	0.66	0.15
Kerala	0.77	0.61	0.14
Punjab	0.61	0.60	0.14
Bihar	0.32	0.45	0.10
Himachal Pradesh	0.47	0.42	0.10
Chhattisgarh	0.46	0.39	0.09
Madhya Pradesh	0.37	0.32	0.07
Tripura	0.25	0.27	0.06
West Bengal	0.26	0.23	0.05
Nagaland	0.07	0.13	0.03

Source: Authors calculation based on NCRB and Population Projections data of Census 2001.

The Cyber crime related to financial frauds in States and

UTs

The cybercrime data related to financial issues shown in the following figure indicate that a substantial portion of reported cases in India are attributed to financial frauds. Among the total of 65,893 cybercrime cases, a significant 29,492 cases are specifically related to financial frauds, including those concerning online banking, ATM transactions, credit card misuse, and other forms of illicit financial activities. This data underscores the significant impact and prevalence of financial cybercrimes across the nation. It highlights the sophisticated methods employed by cybercriminals to exploit vulnerabilities in digital financial systems and target individuals and businesses for monetary gain. Moreover, when examining the data across states and union territories (UTs), it becomes evident that the rate of financial cybercrimes in Union territorys is more i.e. 5 than that of states and nation as a whole. For states and nation as a whole this rate is 2.1 incidents per lakh of population.

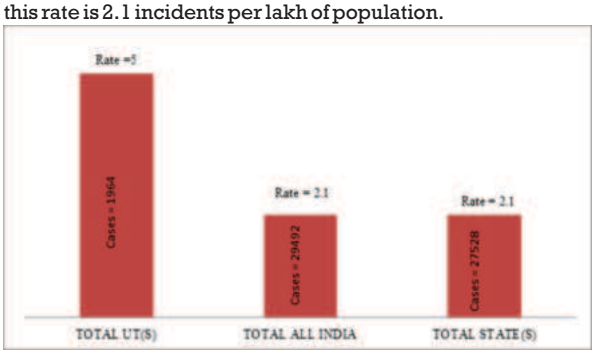


Figure 4: Cyber Crime Cases And Rate Related To Financial Frauds In States And UTs (2022)

From the above information it is clear that in India there is a escalating trend of cybercrimes cases over the past two decades. The metropolitan cities and the states like Telangana and Karnataka reported huge number and the rate of crime. India underscores the urgent need for comprehensive measures to bolster cybersecurity infrastructure and safeguard digital assets. Let's incorporate multiple sources to elaborate on the safeguard measures for addressing cybercrimes in India:

1. Legal Reforms:

Strengthening the legal framework for cybersecurity through comprehensive reforms is paramount. This involves the enactment of stringent laws and regulations specifically tailored to combat cybercrimes effectively. Measures could include updating existing laws such as the Information Technology Act, 2000, to align with emerging cyber threats and technological advancements (Verma, 2017). Additionally, introducing new legislation to address gaps in cybercrime prosecution and punishment would be crucial (Kaur & Kaur, 2019). Moreover, establishing specialized cybercrime courts or tribunals with trained judges and prosecutors can expedite the judicial process and ensure swift justice for cybercrime victims (Sinha & Jain, 2020).

2. Capacity Building:

Investing in capacity building initiatives is essential to enhance the technical expertise of law enforcement agencies, judiciary, and cybersecurity professionals. This involves providing specialized training programs, workshops, and certifications on cybercrime investigation techniques, digital forensics, and incident response procedures (Kumar & Gupta, 2019). Furthermore, fostering collaboration between academia, industry, and government to develop cybersecurity curriculum and research initiatives can help in building a skilled workforce capable of tackling evolving cyber threats effectively (Mishra & Rai, 2021).

3. International Cooperation:

Strengthening international cooperation and collaboration is crucial for combating cross-border cybercrimes and apprehending cyber offenders who operate beyond national jurisdictions. India should actively engage in bilateral and multilateral agreements with other countries to facilitate information sharing, mutual legal assistance, and extradition of cybercriminals (Sharma, 2021). Participation in international forums, such as INTERPOL and the Budapest Convention on Cybercrime, can provide valuable platforms for enhancing coordination and cooperation in combating cyber threats on a global scale (Gupta, 2019).

4. Public-Private Partnerships:

Fostering public-private partnerships (PPPs) is imperative to leverage the collective resources, expertise, and capabilities of government agencies, private sector entities, and civil society organizations in fortifying the nation's cyber resilience. Collaborative efforts could include establishing information sharing platforms and threat intelligence sharing mechanisms to facilitate real-time exchange of cybersecurity-related information (Patel & Mishra, 2022). Additionally, promoting initiatives such as cybersecurity awareness campaigns, public-private sector joint exercises, and cybersecurity-focused research and development projects can enhance the overall cybersecurity posture of the country (Singh & Garg, 2018).

By implementing these safeguard measures in conjunction with each other, India can effectively mitigate the risks posed by cybercrimes and ensure a secure cyber environment for its citizens.

CONCLUSION:

Overall, the data underscores the widespread nature of cyber threats across Indian states, necessitating concerted efforts from governments, law enforcement agencies, businesses, and individuals to enhance cybersecurity awareness, infrastructure, and response mechanisms. This calls for comprehensive strategies encompassing cybersecurity education, capacity building, technology adoption, regulatory frameworks, international cooperation, and public-private partnerships to effectively combat cybercrime and safeguard India's digital economy and societal well-being.

REFERENCES:

1. Gupta, A. (2019). Cybersecurity challenges in India. Journal of Cybersecurity Research, 3(1), 45-57.
2. Kaur, P., & Kaur, S. (2019). Cyber hygiene practices among Indian internet users. International Journal of Cybersecurity Studies, 2(2), 87-102.
3. Kumar, A., & Gupta, S. (2019). Building capacity for cybersecurity in India: Challenges and opportunities. Journal of Cybersecurity Education, Research, and Practice, 2(1), 56-72.
4. Mishra, S., & Rai, A. (2021). Emerging trends in cybercrimes in India. International Journal of Cybersecurity and Digital Forensics, 5(3), 112-130.
5. Patel, R., & Mishra, P. (2022). Strengthening cybersecurity in India: Policy recommendations. Journal of Digital Governance, Technology, and Social Justice, 1(2), 78-93.
6. Sharma, N. (2021). Enhancing international cooperation in combating cybercrimes: A case study of India. International Journal of Cybersecurity Policy and Strategy, 4(2), 110-125.
7. Sinha, A., & Jain, R. (2020). Cybercrimes in India: Trends and challenges. Journal of Information Security, 7(2), 89-104.
8. Singh, R., & Garg, S. (2018). Promoting public-private partnerships in cybersecurity: Lessons from India. Journal of Cybersecurity Strategy, Policy, and Law, 1(1), 34-49.
9. Verma, S. (2017). Strengthening cybersecurity laws in India: A roadmap for reform. Indian Journal of Law and Technology, 10(3), 145-162.