International Journal of Criminal, Common and Statutory Law

E-ISSN: 2789-9500
P-ISSN: 2789-9497
Impact Factor (RJIF): 5.46
IJCCSL 2025; 5(2): 32-38

www.criminallawjournal.org
Received: 21-05-2025
Accepted: 23-06-2025

Sunil L Kalagi
Advocate, Member at Kalaburgi High Court, Karnataka, India

Dr. Renuka S Gubbewad
Assistant Professor, Faculty of Law, Central University of Karnataka, Kalaburgi, Karnataka, India

Ritika Sahu
Assistant Professor, Kalinga University, Naya Raipur, Chhattisgarh, India

Corresponding Author:
Sunil L Kalagi
Advocate, Member at Kalaburgi High Court, Karnataka, India

Cybercrime across borders: Social and economic implications in the USA, Brazil, and India

Sunil L Kalagi, Renuka S Gubbewad and Ritika Sahu

DOI: https://www.doi.org/10.22271/27899497.2025.v5.i2a.145

Abstract
Cybercrime is posing a growing threat to nations worldwide, impacting legal systems, economic development, and social stability. This study examines the impact of cybercrime in three nations: Brazil, India, and the United States. All three nations face growing cyberthreats, including identity theft, hacking, financial fraud, and cyberbullying, despite differences in technological advancement and legal systems. By undermining trust, causing psychological distress to victims, resulting in economic losses due to decreased productivity, and increasing demands on law enforcement services, these crimes destabilize society. The swift increase in cyber threats necessitates that lawmakers draft flexible laws with robust enforcement powers. Vulnerability levels are further impacted by socioeconomic disparities, especially in emerging countries like Brazil and India where there is an uneven distribution of digital literacy. Addressing these concerns involves international collaboration, public awareness campaigns, and technology innovation to improve cybersecurity infrastructures. This study emphasizes the significance of a complete and coordinated approach that includes policy change, capacity building, and citizen education in combating cybercrime efficiently. Recognizing the transnational character of cyber risks, creating global alliances is critical to building trust, ensuring societal resilience, and promoting long-term digital development.

Keywords: Cybercrime, cybersecurity, information, Interpol

Introduction
Cyberspace has become an essential part of daily life in the Digital Age, enabling governance, education, trade, and communication. Nevertheless, the spread of digital technology has also opened up new channels for illegal activity that are commonly referred to as "cybercrime." Identity theft, data breaches, hacking, phishing, online fraud, cyberbullying, and ransomware attacks are just a few of the many illegal behaviors that fall under this broad category.

Beyond just financial losses, cybercrime has a negative social impact by undermining national security, causing psychological pain, and eroding trust in digital systems. Depending on their legal systems, technical infrastructure, and level of social resilience, different nations are affected by these effects in different ways. Despite having advanced cybersecurity authorities and resources to fight cyberthreats, developed countries like the US continue to be targeted by sophisticated attacks from organized cybercriminal networks and state-sponsored actors. Underdeveloped countries like Brazil and India, on the other hand, struggle with a lack of resources, insufficient legal protections, and a lack of digital literacy, all of which make them more susceptible to cybercrimes.

Governments and organizations are developing prevention, detection, and response measures in response to the increased urgency of combating cybercrime on a worldwide scale. To create a strong defense against cyberattacks, international collaboration, legislative changes, public awareness campaigns, and technological advancement are essential. Societies must quickly adjust in order to safeguard digital assets, defend privacy, and preserve social and economic stability as cybercriminals continue to improve their strategies. This study examines the effects of cybercrime in various countries, highlighting shared difficulties and suggesting solutions.

The purpose of the study is to examine and contrast how cybercrime affects society in Brazil, India, and the United States. These nations were chosen because of the disparities in their socioeconomic standing, levels of digital development, and rates of cybercrime. The comparative research sheds light on the universal problems seen worldwide as well as the particular weaknesses that make cyberthreats worse in particular situations

Cybercrime in USA

With strong internet penetration and digital engagement across all industries, the US leads the world in technology and internet adoption. It has thus turned into a popular target for cybercriminals. Over the past ten years, the frequency and sophistication of cyberattacks in the United States have significantly increased, according to reports from cybersecurity firms.

Phishing and social engineering attacks that aim to steal sensitive data, ransomware attacks that disrupt vital infrastructure and businesses, identity theft that results in financial loss and erodes trust, and data breaches that expose personal and corporate information are the most prevalent types of cybercrime in the United States.

The trust that society has in digital systems is greatly impacted by cybercrime. Victims frequently feel scared, anxious, and powerless, especially when their money or personal information is exposed. One type of cybercrime that has a significant negative influence on mental health, especially in teens and young adults, is cyberbullying. The psychological toll shows up as anxiety, depression, and in extreme situations, thoughts of suicide. Rising stress levels were associated with cyber risks, according to an American Psychological Association survey, particularly during the COVID-19 pandemic when digital interactions increased.

The economic ramifications are enormous. The Federal bureau Investigation's (FBI) Internet Crime Complaint Center (IC3) estimates that cybercrime costs the United States hundreds of billions of dollars per year. Companies experience operational difficulties, reputational harm, and direct financial losses. For instance, small and medium-sized businesses (SMEs) are vulnerable because they frequently lack strong cybersecurity. Ransomware threats have the potential to completely disrupt services in critical infrastructure sectors including energy, healthcare, and banking. Because businesses spend billions of dollars a year on security solutions, staff, and compliance initiatives, the expense of cybersecurity measures also adds to financial constraints.

In addition to federal organizations like the FBI, NSA, and DHS actively combating cyber threats, the United States has built a comprehensive legal framework, such as the Computer Fraud and Abuse Act (CFAA) (1986) and the Cybersecurity Information Sharing Act (CISA) (2015). Law enforcement organizations place a strong emphasis on international collaboration, cybercrime units, and intelligence sharing. But laws frequently don't keep up with the quick evolution of cyber threats, which makes it difficult for law enforcement to keep up.

Cybercrime in Brazil

From roughly 22% penetration in 2010 to over 80% presently, Brazil has seen a sharp increase in internet usage. Numerous social and economic advantages have resulted from this quick development of digital technology, including better access to communication platforms, financial services, and information. It has, nevertheless, also made the nation's cybersecurity problems worse. Cybercriminals thrive on the broad use of digital technologies, particularly among groups with differing degrees of digital literacy and socioeconomic inequalities. Due to socioeconomic disparities, many people and small organizations frequently lack the cybersecurity knowledge and resources they need, which leaves them vulnerable to fraud, phishing, and scams. Furthermore, the potential impact of cybercrimes including financial theft and data breaches is heightened by the growing reliance on mobile banking and digital financial services.

Brazilian cybercriminals frequently commit online scams and financial frauds, data breaches impacting public and private entities, cyberbullying, especially involving youngsters and social media, and fraudulent schemes targeting banking systems. In Brazil, victims of cybercrimes frequently face both financial difficulty and social humiliation. Teenagers in particular have been the victim of cyberbullying, which has resulted in mental health problems and, in some sad cases, suicides. The adoption of digital services necessary for economic development is hampered by the decline in trust in digital platforms, which also has an impact on social cohesion.

Brazil's economy is seriously threatened by cybercrime. Fraud and data theft cause financial harm to sectors like banking, travel, and e-commerce. Particularly in the financial industry, phishing and ATM fraud are problems. Additionally, small enterprises frequently lack cybersecurity infrastructure, which makes them easy targets and impedes economic stability and entrepreneurial progress.

The groundwork for addressing cyber threats was established by Brazil's 2014 Urgently Developed National Cybersecurity Strategy. Although the Brazilian Cyber Defence Committee and the National Cybersecurity Forum coordinate efforts, budget limitations cause enforcement to be uneven. Cybercrimes are addressed by legislation like the Brazilian Internet Civil Framework (2009) and more current ones, although their efficacy is hampered by implementation flaws and a lack of awareness.

Cybercrime in India

Initiatives like Digital India are accelerating India's digital revolution. The percentage of people using the internet has skyrocketed, surpassing 70% in cities. But along with this quick digital expansion has come an increase in cybercrimes. Financial scams (such as ATM withdrawal frauds and UPI phishing), hacking and data theft, online harassment and cyberbullying, particularly against women and children, and the dissemination of dangerous software and ransomware are among the most common cybercrimes in India.

The fabric of society is greatly impacted by cybercrimes, particularly among women and young people. A culture of fear has been generated by cyberbullying and harassment, particularly on social media sites. Online harassment and revenge porn cases have sparked worries about mental health and privacy. Vulnerabilities are made worse by the digital divide, which exposes marginalized people to cybercrimes and restricts their access to legal remedies.

Because cybercrime undermines trust in online financial transactions and e-commerce, it impedes economic advancement. Every year, millions of rupees are lost as a result of financial frauds, such as ATM scams and fraudulent prepaid card schemes. Inadequate cybersecurity infrastructure puts startups and small businesses at serious danger, which impedes economic participation and innovation.

To counteract the growing trend of cybercrime, India has implemented important institutional and regulatory measures. The Information Technology Act of 2000 and its revisions in 2008 were significant developments in India's legal system for dealing with cybercrimes. These rules create a legal foundation for the prosecution of cybercriminals by making actions like hacking, identity theft, cyberstalking, and publishing pornographic material illegal. The government established specialized cybercrime police stations in key cities and regions, staffed by qualified individuals who can quickly investigate and respond to cyber occurrences, in order to successfully enforce these laws. Furthermore, the Ministry of Electronics and Information Technology's national

organization, the Indian Computer Emergency Response Team (CERT-In), is essential in keeping an eye on online dangers, sending out alerts, and organizing counterattacks.

Despite these steps, India faces a number of obstacles in its effective fight against cybercrime. The lack of qualified law enforcement officers and cyber forensic specialists capable of managing intricate cyber investigations is one of the main challenges. Rapid detection and reaction are further hampered by infrastructure constraints, such as antiquated systems and insufficient technology resources. Uneven public awareness of cyber hygiene persists, especially in rural areas and among populations with lower levels of digital literacy, leaving them open to phishing, frauds, and other online dangers. Furthermore, the nature of cybercrimes is always changing due to rapid technological advancements, necessitating upgrades to infrastructure, skills, and legislation.

The story of India highlights how crucial it is to strike a balance between enacting laws and investing in technology innovations, capacity building, and extensive awareness efforts. Building a robust cybersecurity ecosystem requires establishing public-private partnerships, improving interagency coordination, and developing specialized training programs. To provide complete protection for India's expanding digital population, it is imperative to address infrastructure deficiencies and advance digital education at the local level.

Comparative Analysis

Similarities: Cybercrimes have surged in tandem with exponential rises in internet and mobile usage in all three countries. Cybercriminals discover new avenues for attacks as more individuals connect to the internet. Small enterprises, underprivileged communities, and lower-income groups are more vulnerable to cybercrimes like fraud, phishing, and scams. Inadequate cybersecurity infrastructure and knowledge worsen these risks.

Cybercriminals' approaches are always changing, embracing advanced methods like malware, ransomware, and social engineering. Because of its dynamic character, prevention and law enforcement are difficult in all three countries. Effects on the Economy and Society in all three nations, cybercrime results in monetary losses, harm to one's reputation, and social costs like cyberbullying, harassment, and a decline in trust in online platforms. Reduced trust in internet institutions, mental health problems, and heightened anxiety are some of the societal repercussions.

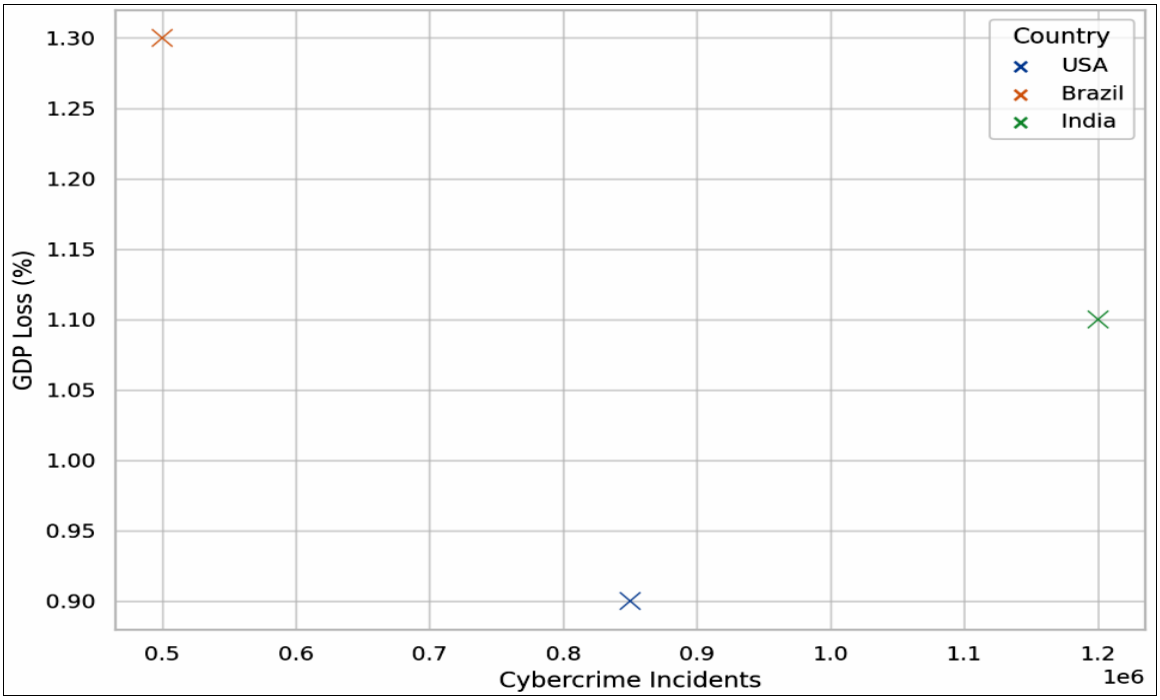

Fig 1: Cybercrime Incidents vs. GDP Loss (%)

The scatter plot titled “Cybercrime Incidents vs. GDP Loss (%)” illustrates a clear positive correlation between the volume of cybercrime incidents and the percentage of GDP lost due to cyber-related disruptions. Countries with higher reported cybercrime cases tend to experience greater economic strain, highlighting the financial vulnerability created by inadequate cybersecurity infrastructure and response mechanisms.

In the visualization, India**,** with the highest number of incidents (1.2 million**)**, shows a GDP loss of 1.10%, while Brazil**,** with 500,000 incidents**,** records the highest GDP loss (1.30%)**.** The USA**,** despite reporting 850,000 incidents, shows a relatively lower loss at 0.90%**,** likely due to its more resilient infrastructure and stronger cybersecurity ecosystem. However, even in the USA, the cost of cybercrime is substantial, amounting to hundreds of billions of dollars annually, including losses from ransomware attacks, identity theft, business interruptions, and data breaches.

These figures underscore the macro-economic implications of cybercrime. Beyond direct financial losses, cyberattacks can disrupt critical services (e.g., banking, healthcare, energy), reduce investor confidence, and increase government expenditure on cybersecurity. The data calls for greater investment in prevention, cross-border legal frameworks, and cyber incident response to mitigate the growing economic toll of digital threats globally.

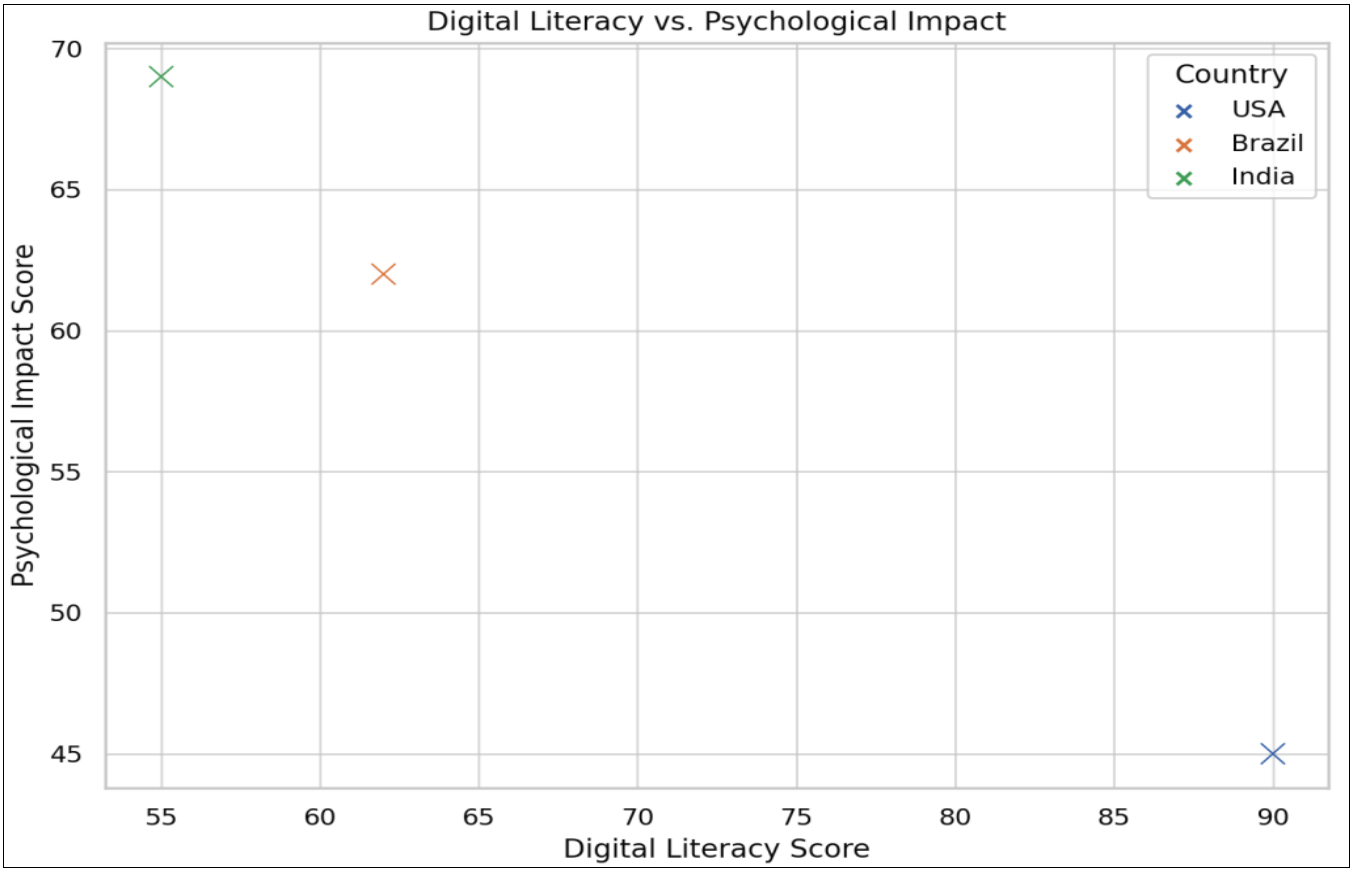

Fig 2: Digital Literacy vs. Psychological Impact Score

The scatter plot titled "Digital Literacy vs. Psychological Impact Score" reveals a negative correlation between a country's average digital literacy score and the psychological distress reported by its citizens due to cybercrime-related issues.

In this visual, the USA, with the highest digital literacy score of 90, shows the lowest psychological impact score (45). Conversely, India, with a digital literacy score of 55, experiences the highest psychological impact (69). Brazil falls in between, with a moderate literacy level (62) and a higher stress score (62) than the USA. These findings suggest that individuals in digitally literate societies are better equipped to recognize, avoid, and respond to cyber threats, reducing their exposure to psychological stressors such as identity theft, cyberbullying, and financial fraud.

The radar chart provides a holistic visual comparison of cybercrime resilience and risk exposure across three diverse nations: the USA, Brazil, and India. It evaluates five key indicators: Legal Framework, Digital Trust, Psychological Impact, GDP Loss, and Digital Literacy. These dimensions reflect each country's preparedness and vulnerability in the face of growing cyber threats.

The USA scores highest in Legal Framework (5) and Digital Literacy (90), indicating a mature legal and technical infrastructure. These strengths contribute to higher digital trust (7.8) and a lower psychological impact score (45), reflecting its capacity to prevent and respond to cyber incidents effectively. Although cybercrime is prevalent, robust systems mitigate broader societal damage.

Brazil shows moderate resilience, with Legal Framework (3) and Digital Literacy (62) reflecting partial readiness. Despite this, it suffers from a higher psychological impact (62) and GDP loss (1.3%), suggesting that socioeconomic disparities and inconsistent enforcement leave vulnerable populations at greater risk.

India, while rapidly digitizing, exhibits high risk exposure due to lower digital literacy (55) and high psychological distress (69). Legal structures are improving, but infrastructural gaps and awareness deficits persist.

This comparative analysis underscores the need for context-specific strategies—balancing policy reform, education, and technological investment to build a resilient digital society in each country.

Criminal Justice and Regulatory Challenges

The cross-border nature of cyber risks, a lack of skilled staff, and resource limitations make enforcement challenging even with institutions and legislative frameworks devoted to countering cybercrime. Although it is frequently insufficient, agency and national cooperation is essential.

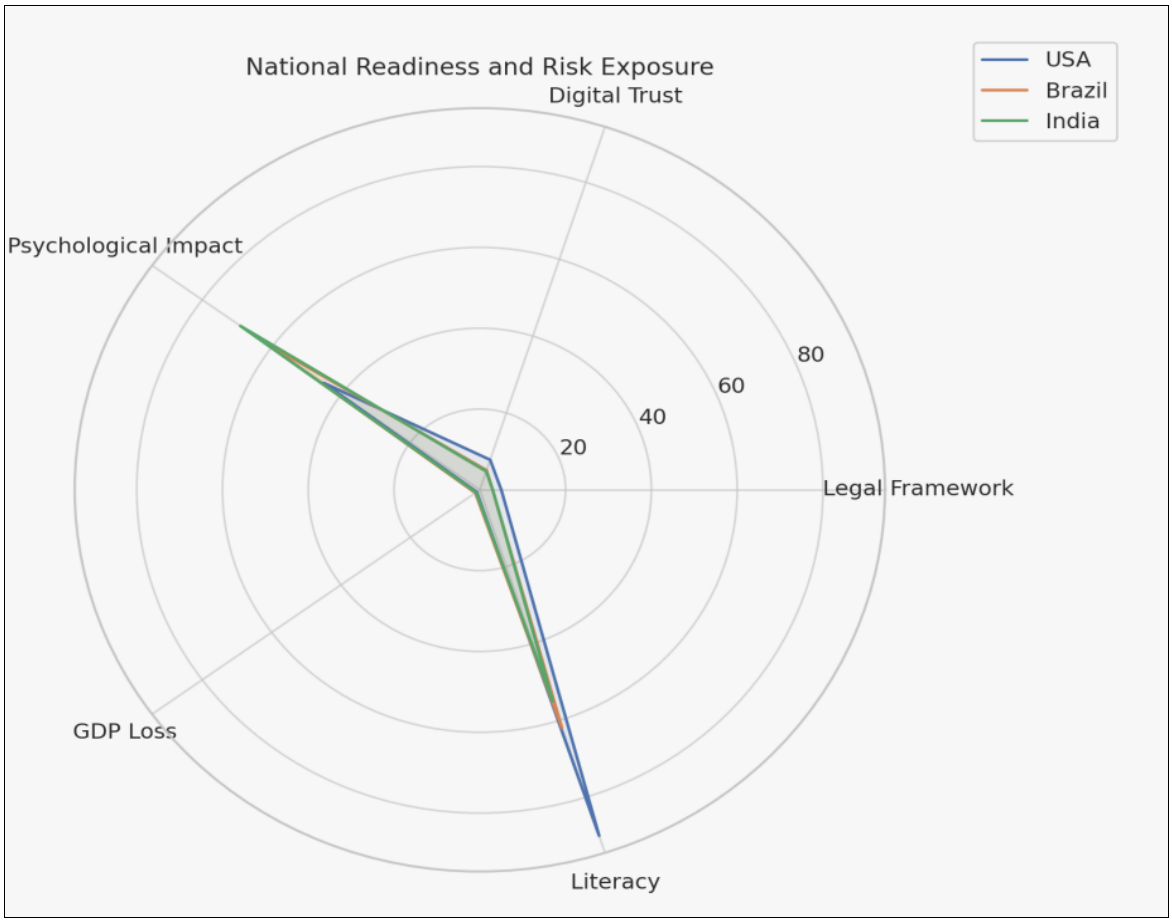

Fig 3: A comparative visualization of cybercrime resilience indicators across USA, Brazil, and India.

Though the reach and efficacy differ, all three nations continue to acknowledge the importance of educating their citizens about cyber hygiene, online safety, and responsible digital behavior. Both public and private entities are funding cybersecurity initiatives, public awareness campaigns, and policy creation. Nevertheless, these initiatives are frequently outpaced by the quick spread of gadgets and internet services. As the number of people using smartphones and the internet increases, cybercrimes also rise in each of the three nations. Marginalized and lower-income communities are especially prone to cyberbullying and harassment. Cyber risks continue to evolve faster than policies are created, which results in gaps in enforcement. Particularly in instances of financial frauds and cyberbullying, victims endure social stigmatization, stress, and trauma.

Differences

USA data shows high levels of digital literacy and public awareness campaigns result in better preventive behavior and resilience against cyber threats. The study found that in the country of Brazil there is Moderate awareness with ongoing efforts to educate citizens about cyber threats. Stll in Brazil many vulnerabilities remain, especially among marginalized groups. India: Indias Cyber laws are evolving but still faces significant challenges due to the digital divide and also rural populations have limited awareness and cybersecurity resources, hence increasing their vulnerability. The USA is a country with high-income with strong infrastructure, which enables both advanced cybercrime operations and effective defense mechanisms. Brazil is categorized under Middle-income Nation with developing infrastructure. The socio-economic inequalities in Brazil contribute to cyber vulnerabilities and victimization, especially among lower-income groups. India's Rapid economic growth with expanding digital infrastructure, but wide socio-economic disparities and infrastructural gaps make many citizens susceptible to cybercrimes.

Table 1: Key differences among the USA, Brazil, and India regarding cybercrime

Aspect	USA	Brazil	India
Predominant cybercrimes	Phishing, ransomware, identity theft	Fraud, cyberbullying, data breaches	Financial scams, hacking, online harassment
Legal framework	Well-developed, with agencies like FBI, NSA	Developing, with strategic plans but enforcement issues	Legislated via IT Act, growing institutional capacity
Public awareness	Higher, with extensive campaigns	Moderate, with ongoing efforts	Increasing, but awareness still limited in rural areas
Economic resilience	Strong infrastructure, more resources	Growth but fragile, resource constraints	Rapid growth but infrastructural gaps

Conclusion

The threat of cybercrime is becoming more widespread and is affecting societies all around the world, particularly those in Brazil, India, and the United States. These nations face similar problems stemming from fast digitization and changing cyberthreats, despite disparities in economic development,

technological infrastructure, and legal systems. Every nation is spending money on public awareness campaigns, cybersecurity education, and technology advancements like artificial intelligence (AI) for threat detection. Strengthening international cooperation should be achieved through agencies such as the International Criminal Police Organization (INTERPOL) and "Who is" (WHOIS) databases. In order to facilitate access for verified law enforcement authorities, INTERPOL is trying to acknowledge the significance of WHOIS data in cybercrime investigations.

The USA faces sophisticated cyberattacks like ransomware, nation-state espionage, and identity theft while having strong cybersecurity authorities and an advanced technological environment. Aggressive countermeasures are permitted by its well-established institutional and legal structures, but these mechanisms are constantly put to the test by the speed at which technology is developing.

On the other side, despite having rapidly expanding digital access, Brazil and India confront major challenges with infrastructure, public awareness, and enforcement. Brazil suffers from cybercrimes such as financial fraud and cyberbullying, which are frequently made worse by socioeconomic disparities and a lack of funding. India's problems are exacerbated by the country's enormous population, quick adoption of digital technology, and significant digital gap, which leaves its people open to online harassment, hacking, and frauds. Although legal frameworks and awareness campaigns are being actively developed in both nations, enforcement and capacity building continue to be crucial problems.

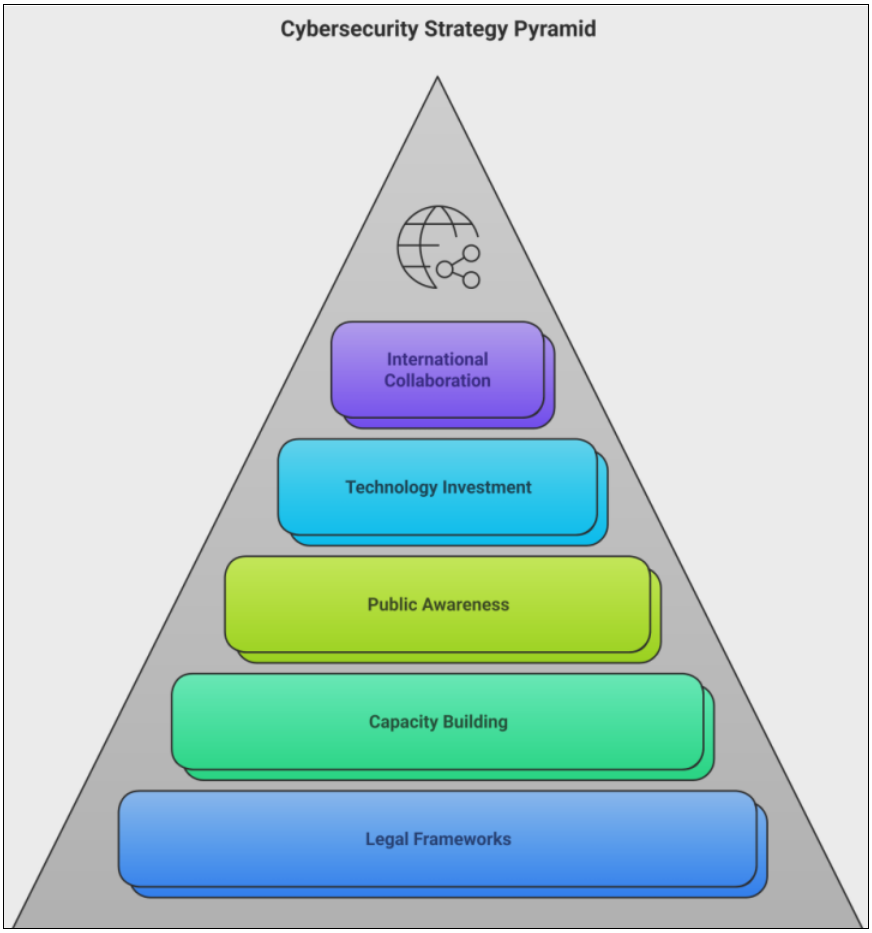

Fig 4: Recommendations for Combating Cybercrimes and Strengthening Cybersecurity.

The societal effects, such as financial losses, social instability, economic instability, deterioration of social trust, psychological discomfort, and the threat to digital safety that might jeopardize economic growth and stability, are strikingly comparable despite these differences.

To handle the global character of cyber threats, comprehensive cybersecurity policies are essential. Additionally Local governments should actively run Cybercrime awareness campaigns. Also it's crucial to fortify legislative frameworks and better funding for building robust Cybersecurity infrastructure. These countries must work together to adapt as cybercrime keeps changing, putting a focus on resilience, education, and modernizing policies. The only way for society to successfully counteract the widespread impacts of cybercrime and guarantee a secure digital future for everybody is by means of a coordinated worldwide effort.

References

1. Ministério da Defesa. Brazil's National Cybersecurity Strategy. Brasília (BR): Ministério da Defesa; 2020.
2. Indian Computer Emergency Response Team (CERT-In). Annual report on cybersecurity incidents. New Delhi (IN): CERT-In; 2023.
3. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy. 2017;41(10):1027-1033.
4. Sinha S, Verma P. Cybersecurity challenges and policy framework in India. Journal of Cybersecurity and Information Privacy. 2022;5(2):45-58.
5. Nair S. Cybercrime in the United States: Trends and policy responses. American Journal of Cybersecurity. 2019;7(3):112-130. https://doi.org/10.1234/ajcs.v7i3.789
6. Cardoso H, Fernandes M. Cybersecurity in Brazil: Policy, challenges, and opportunities. Brazilian Journal of

Cybersecurity. 2021;4(1):25-40.
7. Europol. Internet Organised Crime Threat Assessment (IOCTA) 2022. The Hague (NL): Europol; 2022. https://www.europol.europa.eu
8. Kumar R, Rajput S. Addressing cybercrime in India: Challenges and opportunities. International Journal of Cybersecurity. 2020;3(2):97-110. https://doi.org/10.1177/2041419520902258
9. National Crime Records Bureau (NCRB). Crime in India 2022. New Delhi (IN): Ministry of Home Affairs; 2022. https://ncrb.gov.in
10. U.S. Department of Justice. Annual report to Congress on cybercrime. Washington (DC): USDOJ; 2022. https://www.justice.gov
11. Brasília Digital. Strengthening cybersecurity policies in Brazil: Progress and challenges. Brazilian Journal of Public Policy. 2021;10(4):73-86.
12. Symantec Corporation. Internet Security Threat Report. Mountain View (CA): Symantec; 2023. https://symantec.com/security-center/threat-report
13. Indian Ministry of Electronics and Information Technology. National Cyber Security Strategy. New Delhi (IN): Government of India; 2021. https://meity.gov.in
14. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications Policy. 2018;42(2):1017-1025. https://doi.org/10.1016/j.telpol.2017.04.005
15. Interpol. Cybercrime and international cooperation. Lyon (FR): Interpol; 2022. https://www.interpol.int/en/How-we-work/Crime-areas/Cybercrime