

**CYBERCRIME AND ITS IMPACT ON SOCIETY: A SOCIOLOGICAL PERSPECTIVE****Syed Riyaz Pasha**

Assistant Professor , HOD Department of Sociology,
Sri D. Devaraj Urs Government First Grade College, Hunsur, Mysore ,
Karnataka, India.

1. ABSTRACT

The rapid expansion of digital communication, online banking, social media, e-commerce, cloud services and mobile technologies has transformed the organization of contemporary social life. At the same time, these technologies have created new opportunities for cybercrime and have altered the relationship between offenders, victims, institutions and the state. This paper examines cybercrime and its impact on society from a sociological perspective. It treats cybercrime not merely as a technical or legal problem but as a social phenomenon shaped by unequal access to technology, patterns of digital behaviour, social networks, institutional trust, economic incentives, gender relations and changing forms of social interaction. The study uses a descriptive and analytical research design based primarily on secondary sources, including government publications, international reports, academic books and peer-reviewed studies. The analysis considers major forms of cybercrime such as online financial fraud, identity theft, hacking, cyberbullying, cyberstalking, ransomware, misinformation-related harms and technology-facilitated exploitation. The study finds that cybercrime can produce economic loss, psychological distress, reputational damage, social isolation and reduced trust in digital institutions. It also shows that vulnerability is socially differentiated: children, older persons, digitally inexperienced users, women facing online harassment, small organizations and economically vulnerable groups may encounter distinctive risks. Effective prevention therefore requires a combination of digital literacy, institutional capacity, victim support, responsible platform governance, cyber hygiene and cooperation among families, educational institutions, law-enforcement agencies and technology providers.

KEYWORDS: Cybercrime; Digital Society; Social Impact; Cybersecurity; Cyber Victimization; Digital Inequality.

2. INTRODUCTION

Digital technologies have become deeply embedded in everyday social life. Individuals increasingly communicate through social networking platforms, conduct financial transactions through digital payment systems, obtain public and private services online, study through digital platforms and maintain professional relationships through networked communication. The growth of cyberspace has therefore produced a significant transformation in the organization of social interaction. David Wall argues that information technologies have transformed the opportunity structures through which conventional offences can be reproduced and through which new forms of offending can emerge .



Cybercrime may broadly be understood as unlawful conduct in which computers, communication devices or networks are used to commit or facilitate an offence. The Indian National Cyber Crime Reporting Portal recognizes a wide range of cyber offences, including online financial fraud, hacking, ransomware, cryptocurrency-related crime, social-media crime and crimes involving mobile devices . This broad character demonstrates why cybercrime should not be reduced to hacking alone. It includes offences against individuals, property, organizations and public institutions, as well as harmful conduct mediated through digital communication.

From a sociological viewpoint, the significance of cybercrime lies in its relationship with social structure and everyday behaviour. Routine Activity Theory proposes that crime becomes more likely when a motivated offender encounters a suitable target in the absence of effective guardianship. Majid Yar's analysis shows that elements of this framework can be applied to cybercrime, although the virtual environment introduces important differences from physical settings [3]. In digital environments, people may repeatedly expose personal information, reuse passwords, interact with unknown persons, or conduct transactions without recognizing the risks. At the same time, offenders can operate across jurisdictions and can automate attacks, creating a scale and speed that challenge conventional forms of guardianship .

Cybercrime also reflects the changing character of social relationships. Social networking platforms can strengthen social connection, but they can also facilitate harassment, impersonation, cyberstalking and the circulation of harmful material. The National Cyber Crime Reporting Portal specifically identifies cyberstalking and cyberbullying among online harms and provides safety guidance for young people and families . Such harms are sociologically important because they affect identity, dignity, social participation and perceptions of safety. A person who is repeatedly harassed online may withdraw from digital spaces even when those spaces are necessary for education, employment and social interaction.

Economic globalization and digitalization have further expanded the potential reach of cybercrime. Online fraud can target victims without the offender being physically present. Europol's Internet Organised Crime Threat Assessment identifies cyber-attacks, online fraud and child sexual exploitation as major areas of concern and notes the role of enabling technologies such as cryptocurrencies and the dark web . The United Nations Office on Drugs and Crime has likewise emphasized the transnational character of cybercrime and the need for international cooperation . Thus, cybercrime is simultaneously local in its effects and global in its organization.

The Indian context is particularly significant because digital public infrastructure, mobile connectivity and online payments have expanded rapidly. The Government of India has established the Indian Cyber Crime Coordination Centre (I4C), including the National Cyber Crime Reporting Portal, cyber-forensic and training components, to strengthen coordinated responses . The reporting system also provides the cybercrime helpline 1930 for immediate reporting of cyber financial fraud . These institutional developments demonstrate that cybercrime has become a recognized public policy and social governance issue.

The present study therefore examines cybercrime through a sociological lens. It focuses on the social causes and consequences of cyber victimization, the unequal distribution of vulnerability, changes in social trust and the institutional responses required to create a safer digital society. Rather than treating technology as an independent cause, the study understands cybercrime as an interaction between technological opportunities and social conditions.

3. OBJECTIVES

1. To examine the concept and major forms of cybercrime from a sociological perspective.
2. To analyse the social, economic, psychological and institutional impacts of cybercrime.
3. To identify social groups and situations associated with greater vulnerability to cyber victimization.
4. To examine how digital inequality, social behaviour and institutional trust influence cybercrime risks.
5. To suggest sociologically informed measures for prevention, awareness, victim support and institutional response.

4. RESEARCH METHODOLOGY

The present study adopts a descriptive, exploratory and analytical research design. It is a secondary-data-based sociological study and does not claim to present an original population survey. The research draws on published academic literature, government and law-enforcement materials, international reports, books and peer-reviewed studies concerning cybercrime, digital inequality, online victimization and cyber governance. The National Cyber Crime Reporting Portal, CERT-In, the Ministry of Home Affairs, the International Telecommunication Union, Europol and UNODC were treated as important institutional sources because they provide official or internationally recognized information on cybercrime and cybersecurity.

The literature was examined thematically. Five analytical themes were used: (a) forms and patterns of cybercrime; (b) social causes and opportunity structures; (c) consequences for individuals and communities; (d) institutional and legal responses; and (e) prevention through education and collective responsibility. Sociological concepts such as socialization, digital inequality, routine activities, social control, trust, stigma and social vulnerability were used to interpret the literature. The study also draws on the broader criminological work of Wall, Yar and other scholars who have examined cybercrime as a transformation of crime in the information age.

A limitation of the methodology is that cybercrime statistics are affected by under-reporting, differences in legal definitions, variations in reporting practices and the rapid emergence of new forms of online offending. Victims may avoid reporting because of embarrassment, fear of blame, uncertainty about where to complain or lack of confidence in institutional processes. Consequently, recorded cases should not automatically be interpreted as the complete incidence of cybercrime. The findings in this paper are therefore presented as a synthesis of documented evidence and sociological interpretation rather than as a statistical estimate of prevalence.

5. FEATURES OF THE STUDY

The first feature of the study is its sociological orientation. Cybercrime is examined as a social relationship involving offenders, victims, institutions, families, peer groups, markets and technology platforms. This approach avoids an exclusively technical understanding of cybersecurity and asks why particular social conditions make certain individuals or organizations vulnerable.

The second feature is its interdisciplinary character. Cybercrime intersects sociology, criminology, law, computer science, psychology, economics and public administration. Technical security measures such as authentication, encryption and malware detection are necessary, but they cannot by themselves explain why people respond to fraudulent messages, disclose personal information, reuse passwords or fail to report victimization. Social norms, trust and digital literacy influence these behaviours.

The third feature is attention to digital inequality. Access to technology is not equivalent to the ability to use technology safely. Differences in age, education, income, language, disability, digital experience and access to support can influence people's capacity to identify and respond to online threats. The sociological concept of the digital divide is therefore useful for understanding unequal exposure to cyber risks.

The fourth feature is the study of victimization and social consequences. Cybercrime can cause direct financial losses but may also affect mental well-being, family relationships, professional reputation and participation in digital society. Online harassment may create a continuing sense of surveillance or insecurity because the offending material can be copied, redistributed or encountered repeatedly.

The fifth feature is the focus on institutional response. Cybercrime crosses administrative and national boundaries, requiring cooperation between police, financial institutions, telecommunications providers, technology companies, educational institutions and international organizations. India's I4C framework and CERT-In's incident-response functions illustrate the increasing institutionalization of cybercrime governance.

6. FINDINGS AND SUGGESTIONS

6.1 Major Findings

The study finds that cybercrime is closely connected with the ordinary routines of digital society. As online banking, shopping, communication and public services become routine, the number of potential targets and points of interaction also increases. Wall describes this transformation as a change in the opportunity structure of crime, while Yar shows that established criminological concepts can be adapted to cyberspace but must account for its distinctive characteristics .

A second finding is that cybercrime has diversified beyond unauthorized access to computers. Online financial fraud, identity theft, phishing, impersonation, cyberbullying, cyberstalking, ransomware, cryptocurrency-related offences and technology-facilitated exploitation demonstrate the range of harms that can occur in networked environments. India's National Cyber Crime Reporting Portal explicitly provides reporting categories for several of these forms . The diversity of offences means that prevention cannot depend on a single technical solution.

A third finding concerns the economic and social impact of cybercrime. Financial fraud can produce immediate monetary loss, while ransomware and data breaches can interrupt organizational activities. For households, loss of savings can generate debt, family conflict and reduced trust in digital payments. For organizations, a cyber incident may affect productivity, reputation and customer confidence. The social cost can therefore extend beyond the original monetary value of the incident .

A fourth finding is that psychological and relational consequences are significant. Victims of cyberstalking, bullying, impersonation or sexualized online abuse may experience fear, humiliation, social withdrawal and reputational anxiety. These effects can be intensified when harmful content is persistent and easily redistributed. The Indian cybercrime portal specifically highlights cyberstalking, bullying and online exploitation as areas requiring awareness and preventive behaviour .

A fifth finding is that cyber vulnerability is socially differentiated. Children and adolescents may face grooming, bullying and peer-related risks; older adults may encounter difficulties recognizing sophisticated digital fraud; inexperienced users may be more vulnerable to phishing; and women may face gendered forms of harassment and stalking. These patterns should not be interpreted as inherent weaknesses of particular groups. Rather, they reflect differences in digital exposure, social power, access to information, confidence and support systems.

A sixth finding is that cybercrime challenges traditional boundaries of social control. A local victim may interact with an offender located in another city or country, while the relevant platform, payment intermediary and data server may be distributed across several jurisdictions. UNODC has emphasized the importance of international cooperation in addressing cybercrime, while Europol highlights the transnational and adaptive character of contemporary online offending .

A seventh finding is the problem of under-reporting. Victims may fear stigma, blame or financial consequences, or may not know which authority to approach. The availability of the National Cyber Crime Reporting Portal and the 1930 helpline is therefore socially important because accessible reporting mechanisms can reduce barriers between victims and institutions . However, awareness of these mechanisms must reach diverse linguistic, educational and socioeconomic groups.

Finally, the study finds that cybersecurity is partly a question of social trust. Repeated incidents can make citizens distrust online banking, e-commerce, social media or digital government services. Conversely, transparent institutional communication, timely assistance and visible enforcement can strengthen confidence in digital systems. Cybersecurity should therefore be understood as part of the broader social infrastructure of a digital society.

6.2 SUGGESTIONS

1. Strengthen digital literacy: Schools, colleges and community organizations should provide practical education on phishing, impersonation, privacy settings, password security, two-factor authentication and safe digital payments. Awareness should use local languages and examples relevant to different age groups.

2. Promote family and community awareness: Cyber safety should not be treated only as an individual responsibility. Families, peer groups, teachers and community organizations can create supportive environments in which victims can report incidents without fear of blame or embarrassment.
3. Improve victim-centred reporting: Reporting mechanisms should be simple, accessible and responsive. Public awareness of the National Cyber Crime Reporting Portal and the 1930 helpline should be expanded, especially among first-time digital users .
4. Strengthen institutional coordination: Police, cyber-forensic units, banks, payment providers, telecommunications companies and online platforms should develop clear mechanisms for rapid information sharing and victim assistance while respecting legal safeguards and privacy.
5. Build capacity in educational institutions: Colleges and universities should integrate cyber safety, responsible digital citizenship and basic cybercrime awareness into student orientation and extension programmes. Faculty and administrative staff should also receive periodic training.
6. Address gendered and youth-related harms: Prevention programmes should recognize cyberbullying, stalking, impersonation, online sexual exploitation and non-consensual sharing of intimate material as social harms requiring sensitive institutional responses. Children and adolescents need age-appropriate digital safety education .
7. Reduce digital inequality: Cybersecurity initiatives should account for differences in language, literacy, disability, age, income and access to support. A secure digital society requires not only connectivity but also the social capacity to use digital services safely.
8. Encourage responsible platform governance: Technology platforms should strengthen mechanisms for reporting abuse, detecting fraudulent activity, protecting user accounts and providing clear information about privacy and security.
9. Improve cybercrime research: Universities and research institutions should conduct localized sociological studies on victimization, reporting behaviour, digital trust, cyberbullying, financial fraud and the experiences of marginalized groups. Such research can support evidence-based policy.
10. Strengthen international cooperation: Because cybercrime frequently crosses national boundaries, law-enforcement and judicial cooperation, compatible legal procedures and responsible information sharing remain important .

7. CONCLUSION

Cybercrime is not simply a problem of computers or networks; it is a problem of social organization in the digital age. The expansion of cyberspace has changed opportunities for offending, patterns of victimization and the mechanisms through which individuals and institutions attempt to maintain social order. A sociological perspective demonstrates that cybercrime is shaped by routine digital practices, social inequality, trust, power relations, institutional capacity and the availability of guardianship. The consequences may include financial loss, psychological distress, reputational damage, social withdrawal and reduced confidence in digital institutions.

The appropriate response therefore requires more than technical security. Cyber safety must be supported by digital literacy, accessible reporting systems, victim-centred institutions, responsible technology governance, effective cyber-forensic capacity and international cooperation. In India, initiatives such as I4C, the National Cyber Crime Reporting Portal, CERT-In and the 1930 helpline provide important institutional mechanisms, but their effectiveness also depends on public awareness and accessibility [6-8]. Ultimately, building a safer digital society is a shared social responsibility involving citizens, families, educational institutions, civil society, governments and technology providers.

8. REFERENCES

1. Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press, Cambridge.
2. Indian Cyber Crime Coordination Centre (I4C), Ministry of Home Affairs, Government of India. National Cyber Crime Reporting Portal: Cyber Safety and Cybercrime Information.
3. Yar, M. (2005). The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology*, 2(4), 407–427. <https://doi.org/10.1177/147737080556056>
4. Europol. (2023). Internet Organised Crime Threat Assessment (IOCTA) 2023. European Cybercrime Centre, The Hague.
5. United Nations Office on Drugs and Crime (UNODC). (2013). *Comprehensive Study on Cybercrime*. United Nations, Vienna.
6. Ministry of Home Affairs, Government of India. Indian Cybercrime Coordination Centre (I4C): Overview and institutional framework.
7. Government of India. National Cyber Crime Reporting Portal: Reporting mechanisms and Cyber Crime Helpline 1930.
8. Indian Computer Emergency Response Team (CERT-In). (2024). *Annual Report 2024*. Ministry of Electronics and Information Technology, Government of India.
9. Wall, D. S. (2001). Cybercrimes and the Internet. In D. S. Wall (Ed.), *Crime and the Internet*. Routledge, London.
10. Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2018). *Cybercrime and Digital Forensics: An Introduction*. Routledge, New York.
11. Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). A typology of cybercriminal networks: From low-tech locals to high-tech specialists. *Crime, Law and Social Change*, 67, 39–57.
12. Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? *Social & Legal Studies*, 10(2), 243–249.
13. DiMaggio, P., Hargittai, E., Celeste, C., & Shafer, S. (2004). Digital inequality: From unequal access to differentiated use. In K. Neckerman (Ed.), *Social Inequality*. Russell Sage Foundation.
14. van Dijk, J. (2020). *The Digital Divide*. Polity Press, Cambridge.
15. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin*, 140(4), 1073–1137.
16. Hinduja, S., & Patchin, J. W. (2015). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (2nd ed.). Corwin, Thousand Oaks.
17. United Nations Office on Drugs and Crime (UNODC). (2024). *FAQ: Future international convention on countering the use of information and communications technologies for criminal purposes*.
18. International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index 2024*. ITU Development Sector, Geneva.
19. Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*, ETS No. 185. Council of Europe, Strasbourg.
20. Brenner, S. W. (2007). *Law in an Era of Smart Technology*. Oxford University Press, New York.
21. Clough, J. (2015). *Principles of Cybercrime* (2nd ed.). Cambridge University Press, Cambridge.
22. Jewkes, Y., & Yar, M. (Eds.). (2010). *Handbook of Internet Crime*. Willan Publishing, Cullompton.
23. Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: A comparative study of the nature and impacts of fraud victimisation and its victims. *Security Journal*, 27, 1–19.