CYBERCRIME AND SOCIAL CHANGE: EVALUATING TRADITIONAL CRIME THEORIES IN THE DIGITAL AGE

***DR. NABAMITA PAUL RAY**

Abstract

The inexorable growth of digital technology and the Internet has radically transformed the social environment and gave rise to new forms of criminal behavior which we collectively refer to as cybercrime. The paper challenges the interaction between social change and cybercrime and will focus on whether established criminological theories are relevant to explaining digital deviance. Although such schemas as the Classical Theory of Crime, the Positivist Theory, the Strain Theory, and the Differential Association Theory have traditionally provided some valuable information about the proximate causes of crime, the transposability of these theories to the cyber domain is still a topic of intense criticism. This research uses a doctrinal and analytical approach and relies extensively on the secondary sources, including the academic material, reports on empirical findings, and legal frameworks. It questions how technological advances, effects of globalization, and the anonymity provided by cyberspace have upset traditional crime dynamics and thus posed a daunting predicament to both criminological paradigm as well as control laws. The argument of the analysis is that though classical theories still equally have certain explanatory value, they lack the ability to capture the multifaceted complexities that characterize cybercrime and especially its transnational character, the virtual environment and constantly emerging strategies. In addition, the study highlights the growing prominence of modern criminological theories, especially Routine Activity Theory, and the dominant discourses in the field of cyber criminology, which in sum provide more refined tools to understand online crimes. These conclusions suggest the adaptive re-calibration of already existing theoretical constructs and the development of inter-disciplinary approaches that complement each other with the integration of legal, technological, and sociological perspectives. To conclude, cybercrime is not a technological dilemma that is to be left to technology but a manifestation of the general metamorphoses in society, which requires

*Associate Professor, South Calcutta Law College, University of Calcutta

a further development of criminological conceptualizations and legal responses to respond skillfully to the imperatives of the digital age.

Keywords: Cybercrime; Social Change; Criminological Theories; Digital Deviance; Routine Activity Theory; Strain Theory; Cyber Victimization; Digital Sociology.

1. Introduction

1.1 Background of Cybercrime as a Global Socio-Legal Issue

Cybercrime has become a multi-faceted international socio law dilemma, involving the people, businesses, and governments at cross-jurisdictions. The growing reliance on digital infrastructure has created more paths of crimes including identity theft, financial fraud and data breaches and drawn serious concerns of privacy, security and enforcement of regulations. Law in many countries across the world, such as regulations of the Information Technology Act in India and the International conventions such as the Budapest Convention[1] are trying to deal with these threats but due to the constraints set by jurisdictions and technology these have yet to be properly enforced.

1.2 Development of Digital Technology and Reshaping the Crime Patterns.

The rapid rise of digital finance, usage of internet, and artificial intelligence has completely changed the pattern of crime. Traditional crimes have transitioned to advanced cyber based crimes, which are and can be characterized by means of automation, scalability and a small physical presence. The widespread use of smartphones and social media platforms have also aggravated the exposure to cyber risks redefining the offender tactics and victim types as well.

The move towards virtual spaces at the expense of brick-and-mortar crime is gradually turning into a trend.|

1.3 Physical Crime to Virtual Environments.

1. Council of Europe, Convention on Cybercrime art. 1, Nov. 23, 2001, ETS No. 185.

Crime has gained popularity in the virtual realm with physical locations giving way to it as offenders with anonymity and encryption can commit crimes at a lesser risk of being noticed. Cyber offenses do not respect geographical boundaries as is the case with conventional crimes hence it makes it hard to investigate and prosecute the offender. This shift highlights the ineptitude of law doctrines that are limited by territories in combating digital deviance.

1.4 1. Need to Revise Old Criminological Concepts in Cyberspace.

The classical and strain theories emerge as traditional criminology theories that were formulated in physical environments and do not necessarily reflect the nature of cybercrime. It poses new variables of cyberspace which only become relevant through theory changes, which is digital identity and mediation through technology.

1.5 2. Research Gap and Study Objectives.

Although there has been an increasing scholarship, there is still a research gap on the application of classical criminological theories on cybercrime. This paper will attempt to critically assess these theories in the digital context and see if they have any limitations and can be adapted or not. These are studying the crime pattern transformation, evaluating the relevance of theories, and a framework of understanding cybercrime during the epoch of rapid social transformation.

2. Conceptual Framework

2.1 Cybercrime: Definition and Scope

Cybercrime[2] relates to any illegal actions performed by computers and networks, or digital devices and are directed to computers, in which computers themselves act as the instruments and the objects of the crime. It is very broad and covers a lot of activities such as hacking, phishing, identity theft, cyberstalking and ransomware attacks, all of which are manifestations of the growing sophistication of digital criminals. Anonymity, which means that the attackers remain unidentified; transnationality, meaning that a crime can happen in two or even more jurisdictions; and scalability, meaning that the consequences of a single attack can affect thousands of victims at a

2. United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2021).

time are the main distinguishing features of these offenses. Physical barriers are removed, forcing the use of technological infrastructure to enforce the law, which makes the current legal systems difficult to address, and further frustrates the current law enforcement system.

2.2 The Digital Age of Social Change.

The digital age has come with tremendous social changes that have altered the way people relate, communicate and engage in economic and government structures. The high rate of penetration of the internet as well as the hacking of social media sites has transformed the traditional meaning of social relations and the creation of virtual communities that are no longer bound by geographical constraints. Communication has been brought close to the moment and global, and economic activities progressively depend on digital spaces, such as e-commerce and digital banking. There is also a shift in governance where governance models are now e-governance which makes them more accessible though prone to cyber threat. These shifts have led to the creation of new digitalized forms of identity and social activities, which have determined the character of criminal conduct and victimization tendencies in cyberspace[3].

3. Overview of Traditional Crime Theories

3.1 Classical Theory

Classical According to the birth places of Cesare Beccaria and Jeremy Bentham, the criminological theory puts much emphasis on the rational choice and the free will, and states that people find themselves committing crimes after they have contemplated on the costs and benefits, which will possibly accrue. The framework can be used to the present-day challenge of cybercrime since criminals are likely to play the game of risk to rewards (need money or access to data) and risk to detection (could be detected). Rationality of decision making is also improved by the cheapness of entry and alleged anonymity that is a part of cyberspace[4].

3.2 Strain Theory (Merton)

3. INTERPOL, *Global Cybercrime Report* (2023).
4. Neal Kumar Katyal, Criminal Law in Cyberspace, 149 U. Pa. L. Rev. 1003 (2001).

As far as the Strain Theory is concerned, it is based on the premise that a disintegration between the objectives that are accepted within the society and the ways of achieving them through the law produces crime. One of the cyber-enabled crimes that individuals who may be under financial or social pressure can resort to in the digital economy so as to seek alternative measures that can make them succeed is online fraud or identity theft. These opportunities are augmented by the presence of digital means and cybercrime is a desirable method of venting strain-inducing deviance.

3.3 Social Learning Theory (Bandura/Akers).

Social Learning Theory stresses that, criminal conduct is learned in an interaction, imitation and reinforcement. The experience and information on cyber crimes are disseminated via the cyberspace[5], online forums and communities, and through dark web networks. Some of the propagation of cyber deviance includes the exposure of the individuals to norms and behavior which is deviant and is reinforced by peer validation and anonymity.

3.4 Routine Activity Theory (Cohen and Felson)

Routine Activity Theory of crime is a description of the contributions made by motivated offender, the presence of appropriate target and absence of capable guardian. This model can be applied particularly in the online platform where people are likely to release personal data but cybersecurity is lax. Note of bad digital parenting exposes an individual further to victimization of the internet.

3.5 Control Theory (Hirschi)[6]

The Control Theory is based on the belief that weak social bonds (attachment, commitment, involvement and belief) are the reasons that lead to deviant behavior. Online relationships lose strength to anonymity, reduced social responsibility, and a sense of immunity to the perpetration of crime, which is what cybercrime is all about. It is against this that the virtual setting interferes with traditional channels of social control that allow deviant behavior.

5. Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (2010).
6. Travis Hirschi, *Causes of Delinquency* (1969).

4. Cybercrime in the Digital Age: Nature and Trends

Cybercrime in the digital age has been transformed into an omnipresent and ever growing worldwide phenomenon, which is becoming more sophisticated and large-scaled. According to recent world surveys, it has been estimated that yearly cybercrime losses amount to trillions of dollars, an indication that it has a great economic and social effects among countries. The trends in cybercrime indicate a new focus on the financially motivated crimes like ransomwares, phishing, and business email compromise, as well as the enduring popularity of data breaches and identity theft. The COVID-19 also contributed to a higher pace of digital dependency, which led to the exposure to more cyber risks and the emergence of new opportunities of cyber offenders.[7]

One such trend is that there is an increased prevalence of organized networks of cybercrime that is highly coordinated and specialized. These communities operate like conventional criminal structures with hierarchies in place and provide crime-as-a-service, for example, such products as malware or phishing kits are marketed on the black market. Such activities are now found at the center of the dark web, which enables illicit dealings and buying and selling of illegal goods and services anonymously. Cryptocurrencies are an important component in this ecosystem, since they make financial transactions safe, pseudonymous, and difficult to track and prosecute criminals.

The victimization of cybercrime has also increased across a broad demographic, and it has happened among both individuals, businesses as well as governments. Social groups that are susceptible to online fraud and scams are especially the old and digitally inexperienced users. Meanwhile, in the modern society, cybercrime is highly widespread and not targeted at anyone, as data breaches and intellectual property theft become challenges that corporations have to contend with, on the one hand.

5. Evaluation of Traditional Crime Theories in Cyber Context

5.1 Applicability of Classical Theory

Classical theory can still be applied partially in explaining cybercrime because it focuses on making rational decisions. Cyber criminals tend to take calculated risks taking into consideration

7. Cybersecurity Ventures, *2023 Official Cybercrime Report* (2023).

the small likelihood of being discovered in opposition to a potential high monetary or reputation. Cyber offences are appealing to the rational actors because the low risk-high reward dynamic is only amplified by the anonymity of the digital setting as well as little physical risk.

5.2 Strain Theory of Digital Crimes.

The Strain Theory[8] gains an even greater importance in the online environment, so the economic strains and the social demands push people to committing crimes becoming cyber-enabled like the phishing and online fraud. The ubiquitous presence of social media only contributes to the social comparison process and makes a person experience a higher degree of relative deprivation and desire to deviate to experience the supposed success.

5.3.1 Social Learning Under the Internet.

Social Learning Theory[9] is an effective concept that would explain how internet based cybercrimes are extended. The acquisition of technical skills and deviant norms is achieved through digital platforms, such as forums, hacking communities, informational content in the format of a tutorial. Peer validation, anonymity and a lack of the immediate social sanctions reinforce the normalization of cyber deviance.

5.4.1 Routine Activities Theory as applied to Cybercrime.

The applicability of Routine Activity Theory is very high to cyberspace wherein the occurrence of crimes is because of predisposed offenders, the presence of an appropriate target, and the lack of an effective guardian. These inefficient cybersecurity systems and more frequent exposure also open up opportunities of victimization especially in places where there are no well established digital protection systems.

5.5. Limitations of the Traditional Theories.

Even though they are relevant, the classical criminological theories have flaws in explaining cybercrime in a comprehensive way. They in most cases do not consider major aspects of cyberspace that include anonymity, virtual identity and the involvement of technological

8. Robert Agnew, Foundation for a General Strain Theory of Crime and Delinquency, 30 Criminology 47 (1992).
9. Albert Bandura, *Social Learning Theory* (1977)

infrastructure. Additionally, the theories are mostly based on geographically contained settings and hence incapable of describing the transnational and borderless aspect of cybercrime.

6. Emerging Perspectives and Theoretical Adaptations

6.1 Cyber Criminology

Cyber criminology is an interdisciplinary discipline that is still evolving to incorporate the old tenets of criminology into the technological aspects of criminal activities that are happening online. It is about how the information and communication technologies transform the crime behavior, the victimization trends, and the responding of the law enforcement. Cyber criminology offers a more extensive theoretical scope in the analysis of cyber offences by drawing on information discovered in computer science and the digital sociology field, as opposed to the traditional theoretical frameworks.

6.2 Space Transition Theory (Jaishankar)

The theory of Space transition suggested by K. Jaishankar[10] is used to describe the change in behavior of people during the transition between physical and cyberspace. It further implies that the people who might abide by the norms of the given society in real life might act defiantly in the virtual world as a result of anonymity, the absence of consequences, and the freedom of shape of identity. This theory is especially applicable in the context of the interpretation of fact that cyberspace allows the release of hidden criminal orientations.

6.3 In addition, the digital routine activity theory is presented

In cyberspace, the concept of the Guardianship is altered with the hint of the digital versions of the Routine Activity Theory[11]. Unlike physical environments, cybersecurity systems, encryption protocols, and user awareness are competent guardians in the cyberspace. The lack or inadequacy

10. K. Jaishankar, Space Transition Theory of Cyber Crimes, in *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* 283 (2008).
11. Marcus Felson & Lawrence E. Cohen, Human Ecology and Crime: A Routine Activity Approach, 8 Hum. Ecol. 389 (1980).

of such digital guardians makes one more susceptible to cybercrime and it is necessary to redefine traditional aspects of the crime opportunity in the online space[12].

6.4 Network Theory and Cybercrime.

Network theory offers great explanations as to the role of connection and web interactions in easing cybercrime. Cyber offenders are normally working in decentralized networks, which allow collaboration, sharing of information and sharing of resources.

7. Impact of Social Change on Crime Patterns

The accelerated social change powered by a digital transformation[13] has not only transformed the nature of crime but also brought about new types of deviance in addition to changing the usual moves of criminology. Among the major reasons that contributed to this change, it is possible to note the digital divide which indicates the uneven distribution of access to technology and digital literacy. Although it has provided more chances to be economically and socially involved, it has also caused inequalities, which can result in victimization and criminality. Less digitally aware people are susceptible to online fraud and abuse whereas more technical-savvy individuals might use any vulnerabilities against others to achieve criminal ends.

The use of digital spaces by youths has also led to development of cyber deviance. Digital natives as younger populations are highly dependent on the online platform and their exposure to cyber risks grows as well as they can be engaged in deviant behaviors. Peer interaction in online gaming communities, hacking forums, social media sites may serve as an environment where deviant behaviors are learned, normalized, and reinforced in the social environment.

Also, social media culture has altered the nature of crime by maximizing visibility, comparison, and immediate gratification. The platforms that focus on interaction and share content materials may, unintentionally, promote risky or unethical actions, such as cyberbullying, falsified identities,

12. Thomas J. Holt & Adam M. Bossler, Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization, 33 Deviant Behav. 308 (2012).
13. Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (2012).

14. · Jan van Dijk, *The Deepening Divide: Inequality in the Information Society* (2005).

and internet frauds. Also, the relationships between victims and offenders have been changed and roles are more revived, on the cyber space. People might be victim and offender at the same time and this is a complex and interactive nature of the digital environment.

8. Legal and Policy Implications

The vigorous growth of cybercrime poses a lot of challenges to legal systems and policy constructs around the globe. Technical complexity of digital crimes, necessitating special skills, high levels of forensic competence, and constant adjustment to changing technology is just one of the main problems of cyber law enforcement. The law enforcers are commonly challenged with problems in collecting, attributing criminals and ensure the integrity of the electronic evidence, thus restricting successful prosecution.

Enforcement of cyber laws is also complicated by the jurisdictional issues since cybercrime often spreads across the borders. Criminals might be based in a given country, but caused harm to another thereby creating conflict of jurisdiction and legal inconsistencies. The lack of standardized laws in international boundaries will not permit the speed in which an investigation and prosecution should take place and more frequently offenders will be able to use an available loophole in the law.

The legal systems[14] require a revision and the new systems should be more consistent with the dynamism of cyberspace. Current legislation, which is usually created to combat historical crimes, is not adequate to respond to the challenges of data breaches, computer spy, and even cryptocurrency-related crimes. Reform of the legislation should integrate technological advances and offer sophisticated definitions, penalty, and enforcement strategies specific to cybercrime.

Transnational collaboration is important to overcome such challenges. Just like in combatting transnational cybercrime, collaborative approaches in the form of treaties, information sharing approaches, and joint operations in cyberspace are paramount. Organizations like INTERPOL[15]

15.INTERPOL, *Global Cybercrime Report* (2023).

and committees like the Budapest Convention enable the integration of cross-border efforts to counter cyber threats in an increasingly globalized world.

9. Critical Analysis

Traditional criminological theories give a background on how criminals will act in the manner they do due to the main motivational processes including rational choice, social pressure, and learned deviance. Classical, Strain, and Social Learning theories are also useful in establishing the reasons behind the involvement of people in cybercrime especially in the context of finances, peer pressure and perceived to have opportunity. They assist in making the case that cyber criminals, like traditional criminals, fall victim to cost benefit analysis, social conditions and structural imbalances.

Nevertheless, the theories have considerable weaknesses when directed in the technologically advanced sphere of cybercrime. They usually do not take into consideration such vital factors as digital anonymity, encryption, automation and the influence of highly-developed technological frameworks. The dynamism and fast changing characteristic of cyberspace provides variables beyond the general limits of the classical theoretical frameworks and it becomes challenging to argue and explain completely the behavior of cybercriminals through the use of conventional models.

This disparity brings the issue of interdisciplinary methods combining knowledge of sociology and criminology with information technology. Cybercrime[16] cannot only be understood through a human behavior analysis but also through the study of the technological systems through which human behavior is facilitated and formed. Digital forensics, cybersecurity principles, and data analytics are added to criminological research in order to better explain the existing theories in around.

A synthesized system that incorporates conventional criminological views together with technological and sociological understanding is needed to deal with the intricacies of cybercrime.

[16] Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (2010).

This will allow a deeper probing into the behavior of offenders and systemic weaknesses to facilitate the formation of effective prevention and policy strategies.

10. Future Research Directions

Future Research need should be done to establish hybrid criminological models that intersect traditional criminological theories with technology dimensions that can help substantiate cybercrime[17]. Artificial intelligence and machine learning in predicting crimes are becoming particularly important, which suggests a chance of identifying patterns, anomalies, and preventing cyberspace crimes[18]. Also, cyber offenders should be studied during the behavioral analysis, as it is necessary to comprehend their motivations, decision-making and the impact of digital context. Empirical studies are also urgently needed in developing nations, where fast digitalization is not accompanied by appropriate cybersecurity awareness and infrastructure, which results in an increased exposure to cyber threats.

11. Conclusion

This analysis sheds light on the fact that conventional criminological approaches are still useful in explaining basic motifs to commit cybercrimes[19], but they should be heavily changed to accommodate the dynamic of the digital era. The dynamic character of cybercrime demands versatile and inter-disciplinary approaches that embrace the technological, social, and legal outlooks. Policy measures should be reinforced and continuous research must be encouraged to efficiently overcome cybercrime and handle the challenges of the constant social and technological change[20].

REFERENCES:

17.David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007).
18.Thomas J. Holt, *Cybercrime Through an Interdisciplinary Lens* (2020).
[19] Majid Yar & Kevin F. Steinmetz, *Cybercrime and Society* (3d ed. 2019).
20.Ronald L. Akers & Christine S. Sellers, *Criminological Theories: Introduction, Evaluation, and Application* (6th ed. 2013).

1. Council of Europe, Convention on Cybercrime art. 1, Nov. 23, 2001, ETS No. 185.
2. United Nations Office on Drugs and Crime (UNODC), *Comprehensive Study on Cybercrime* (2021).
3. INTERPOL, *Global Cybercrime Report* (2023).
4. Neal Kumar Katyal, Criminal Law in Cyberspace, 149 U. Pa. L. Rev. 1003 (2001).
5. Susan W. Brenner, *Cybercrime: Criminal Threats from Cyberspace* (2010).
6. Thomas J. Holt, Adam M. Bossler & Kathryn C. Seigfried-Spellar, *Cybercrime and Digital Forensics: An Introduction* (2d ed. 2018).
7. Manuel Castells, *The Rise of the Network Society* (2d ed. 2010).
8. Cesare Beccaria, *On Crimes and Punishments* (1764).
9. Jeremy Bentham, *An Introduction to the Principles of Morals and Legislation* (1789).
10. Robert K. Merton, Social Structure and Anomie, 3 Am. Soc. Rev. 672 (1938).
11. Ronald L. Akers, *Social Learning and Social Structure: A General Theory of Crime and Deviance* (1998).
12. Albert Bandura, *Social Learning Theory* (1977).
13. Lawrence E. Cohen & Marcus Felson, Social Change and Crime Rate Trends: A Routine Activity Approach, 44 Am. Soc. Rev. 588 (1979).
14. Travis Hirschi, *Causes of Delinquency* (1969).
15. Cybersecurity Ventures, *2023 Official Cybercrime Report* (2023).
16. Europol, *Internet Organised Crime Threat Assessment (IOCTA)* (2022).
17. Federal Bureau of Investigation, *Internet Crime Report* (2023).
18. Derek B. Cornish & Ronald V. Clarke, *The Reasoning Criminal: Rational Choice Perspectives on Offending* (1986).
19. Robert Agnew, Foundation for a General Strain Theory of Crime and Delinquency, 30 Criminology 47 (1992).
20. Ronald L. Akers, *Social Learning and Social Structure: A General Theory of Crime and Deviance* (1998).
21. Marcus Felson & Lawrence E. Cohen, Human Ecology and Crime: A Routine Activity Approach, 8 Hum. Ecol. 389 (1980).
22. David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007).
23. Yvonne Jewkes & Majid Yar, *Handbook of Internet Crime* (2d ed. 2010).

24. K. Jaishankar, Space Transition Theory of Cyber Crimes, in *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* 283 (2008).
25. Thomas J. Holt & Adam M. Bossler, Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization, 33 Deviant Behav. 308 (2012).
26. Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (2012).
27. Jan van Dijk, *The Deepening Divide: Inequality in the Information Society* (2005).
28. Sonia Livingstone & Leslie Haddon, *EU Kids Online: Final Report* (2009).
29. Danah Boyd, *It's Complicated: The Social Lives of Networked Teens* (2014).
30. Susan W. Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (2012).
31. Council of Europe, Convention on Cybercrime art. 22, Nov. 23, 2001, ETS No. 185.
32. Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596 (2003).
33. INTERPOL, *Global Cybercrime Strategy* (2022).
34. Ronald L. Akers & Christine S. Sellers, *Criminological Theories: Introduction, Evaluation, and Application* (6th ed. 2013).
35. David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (2007).
36. Thomas J. Holt, *Cybercrime Through an Interdisciplinary Lens* (2020).
37. Majid Yar & Kevin F. Steinmetz, *Cybercrime and Society* (3d ed. 2019).