Academe *Journal of Education & Psychology* *ISSN: 2249-040X*
Volume-16, (Special Issue: March 2026) *Peer Reviewed & Refereed Journal (IF: 6.25)*
PP: 458-465 *Journal Website:* www.academejournal.in

A STUDY ON CYBERCRIME AND DIGITAL DEVIANCE: A SOCIOLOGICAL PERSPECTIVE

Swaran.B

Associate Professor
Dept of SociologyGovt College Mandya

ABSTRACT

In day-to-day language, deviance means moving from an accepted direction to a different direction, that is, not following the accepted norms and expectations of a specific social group is called deviation and crime is an important form of deviance. That is, crime is behaviour expressing violation of the law of the concerned state which brings into existence the prescribed punishment. The rapid expansion of the information revolution and the process of globalization made the concept of cyber-crime possible. Cyber-crime means a crime which is committed through computers and networks. Crimes used to happen earlier too but modern technology has not only created new forms of crime but has also increased the rate of crime.

Keywords: Virtual society, cyber-crime, online and offline relationships, cyber bullying, risk society, network society.

1. INTRODUCTION

Globalization has converted the whole world into a village (Global Village). It is true that due to the process of globalization, the society formed by the network of social relations has transformed into a virtual society formed by networks. Where there are no face-to-face relationships i.e., offline relations between individuals but there are online relations. It does not require repetition of contact, communication and interactions which are considered to be the constitutive elements of social relations. Now aspects like, share, comment, status updates are considered essential for online relationships. A virtual community consists of a group of people united by a common interest or motivation. They meet in a dedicated digital space where they can connect with each other, use each other's stories and experiences to drive progress and build meaningful relationships. Therefore, now it cannot be denied that no place or geographical space is required to formed a society, but through computers and internet, a virtual society of relationships can be established even without geographical space.

The evolution of internet technology has given us so many advantages to deal with future problems and grow with rapid rate but also it has provided the scope for criminals to commit their crime with least chance of detection. The cyberspace has proved a boon to the deviant behaviour in the society. The concept of Cyber Crime has gained speed and we are facing great threat of its impact on world society. The human society is become vulnerable to Cyber Crime due to more and more dependence on technology. Cyber Crime becomes a global phenomenon and hence the nationwide generalization of crime cannot workable in present scenario. Our understanding and regulation of Cyber Crime cannot be national but has to be international. Technology is always a double-edged sword and can be used for both the purposes – good or bad. Steganography, Trojan Horse, Scavenging (and even DOS or DDOS) are all technologies and per se not crimes, but falling into the wrong hands with a criminal intent who are out to capitalize them or misuse them, they come into the gamut of Cyber Crime and become punishable offences.

2. IMPORTANCE OF CYBER LAW

Cyber law plays a very important role in this new epoch of technology. It is important as it is concerned to almost all aspects of activities and transactions that take place either on the internet or other communication devices. Whether we are aware of it or not, but each action and each reaction in Cyberspace has some legal and Cyber legal views.

3. NEED FOR CYBER LAW

There are various reasons why it is extremely difficult for conventional law to cope with cyberspace. Some of these are as below.

a. Cyberspace is an intangible dimension that is impossible to govern and regulate using conventional law.

b. Cyberspace has complete disrespect for jurisdictional boundaries. A person in India could break into a banks electronic vault hosted on a computer in USA and transfer millions of Rupees to another bank in Switzerland, all within minutes. All he would need is a laptop computer and a cell phone.

c. Cyberspace handles gigantic traffic volumes every second. Billions of emails are crisscrossing the globe even as we read this, millions of websites are being accessed every minute and billions of dollars are electronically transferred around the world by banks every day.

d. Cyberspace offers enormous potential for anonymity to its members. Readily available encryption software and steganography tools that seamlessly hide information within image and sound files ensure the confidentiality of information exchanged between cyber-citizens.

4. DIFFERENT TYPES OF CYBER CRIME AGAINST INDIVIDUAL

4.1. E-Mail Spoofing

This means a spoofed email is one that appears to originate from one source but actually has been sent from another source. This can also be termed as E-Mail forging. The main goal of the attacker in this case is to interrupt the victim's email service by sending him a large number of emails.

4.2. Phishing

Phishing means trying to fool people into parting with their money. Phishing refers to the receipt of unsolicited emails by customers of financial institutions, requesting them to enter their username, password or other personal information to access their account. The criminal then has access to the customer's online bank account and to the funds contained in that account. The customers click on the links on the email to enter their information, and so they remain unaware that the fraud has occurred.

4.3. Spamming

Spam is the abuse of electronic messaging system to send unsolicited bulk messages indiscriminately.

4. 4. Cyber defamation

It involves any person with intent to lower down the dignity/image of the person by hacking his mail account and sending some mails with using vulgar language to unknown persons mail account.

4.5. Cyber stalking and harassment

The use of Internet to repeatedly harass another person group, or organization. This harassment could be sexual in nature, or it could have other motivations including anger.

4.6. Computer sabotage

The use of the internet to halt the normal functioning of a computer system through the introduction of worms, viruses, or logic bomb is referred to as computer sabotage.

4.7. Malware

Malware is any software that infects and damages a computer system without the owner's knowledge or permission and takes control of any individual‘s computer to spread a bug to other people‘s devices or social networking profiles. Such software can also be used to create a _botnet‘— a network of computers controlled remotely by hacker to spread spam or viruses.

5. SOCIOLOGICAL PERSPECTIVE

From a sociological perspective, **cybercrime** and **digital deviance** are viewed not just as technical failures, but as socially constructed behaviors occurring within a distinct digital environment. This field explores how the shift from physical to virtual spaces reshapes human interaction, social control, and the "hows and whys" of rule-breaking.

5.1. Conceptual Framework: The Digital Environment

Sociologists Roderick Graham and Shawn Smith conceptualize the online space as a distinct environment for social interaction, similar to how urban sociology views cities.

- **Social Construction**: Crime is a socially constructed category shaped by political authority and moral consensus; the digital age compels a shift from territorially grounded definitions to network-based conceptions of harm.
- **The Digital Divide**: Digital inequality (differences in access and skills) remains a predictor of who becomes a victim or a perpetrator.

5.2. Typology of Digital Deviance

Scholars often apply David Wall’s typology to categorize digital transgressions based on traditional legal and moral categories:

- **Cybertrespass**: Crossing digital boundaries, such as unauthorized access or hacking.
- **Cyberdeception/Fraud**: Using digital tools for theft or scams, including identity theft, phishing, and romance scams.
- **Cyberviolence**: Acts intended to harm others, such as cyberbullying, trolling, flaming, and hate speech.
- **Cyberpornography**: Moral transgressions related to the distribution or consumption of prohibited sexual content.

5.3. Sociological Theories Applied to Cyberspace

Traditional theories are reinterpreted to explain digital deviance:

- **Routine Activity Theory**: Explains cyber-victimization by looking for the convergence of a motivated offender, a suitable target (e.g., weak passwords), and the absence of a capable guardian (e.g., poor cybersecurity).

- **Social Control Theory**: Focuses on how the erosion of traditional community bonds (family, neighborhood) in the anonymous online world leads to increased deviance.
- **Labeling Theory**: Examines how being labeled a "hacker" or "deviant" by society can influence an individual's future behavior and identity.
- **Strain Theory**: Suggests digital crime arises when individuals face blocked opportunities in the physical world and turn to online deviance to achieve social or economic goals.

5.4. Mechanisms of Social Control

As deviance moves online, so do the methods of policing and surveillance:

- **Algorithmic Governance**: Control increasingly operates through automated systems that detect "suspicious" behavior or moderate content, shifting from punitive justice to risk management.
- **Digital Panoptic on**: Drawing on Michel Foucault's theories, sociologists examine how continuous observation via metadata and surveillance technologies creates a self-disciplining environment.
- **Online Disinhibition Effect**: The anonymity of the internet reduces fear of immediate social sanction, leading to more aggressive or morally transgressive behavior.

5.5. Cyber victimization

Sociology highlights that cyberspace often reproduces existing power asymmetries. Groups already vulnerable—such as women, minorities, and activists—are frequently targets of cyber violence, including doxxing and online harassment.

6. SOCIOLOGY THEORIES EXPLAINING CYBERCRIME-PDF

Sociological theories offer diverse frameworks to understand the rise and mechanisms of cybercrime by examining the interplay between technology, social structures, and individual behavior.

6.1 Primary Sociological Theories of Cybercrime

Routine Activity Theory (RAT): This is one of the most widely applied theories in cyber criminology. It posits that for a crime to occur, three elements must converge in time and space:

- **A Motivated Offender:** Someone with the intent and ability to commit the crime.
- **A Suitable Target:** Vulnerable digital assets, unprotected devices, or users with low technical literacy.
- **Absence of a Capable Guardian:** Lack of effective antivirus software, weak passwords, or insufficient law enforcement oversight in digital spaces.

6.2 Social Learning Theory: Theorizes that cybercriminal behavior is learned through social interactions with peers and family. Key components include:

- **Differential Association:** Individuals learn techniques and motives for hacking or digital piracy by associating with others who engage in such behaviors.

- **Reinforcement:** Positive outcomes, such as financial gain or social status within hacker communities, reinforce the criminal behavior.

6.3 General Strain Theory (GST): Suggests that individuals commit cybercrimes as a way to cope with "strains" or negative emotions like anger and frustration.

- Strains can arise from the **failure to achieve valued goals** (e.g., financial success) or the **presentation of negative stimuli** (e.g., unemployment or bullying).
- Research indicates that GST may manifest differently by gender; for example, divorce or anonymity might drive offending in women, while falling victim to a crime might drive it in men.

6.4 Structural Functionalism (Anomie Theory): Views crime as a response to the gap between societal goals (like wealth) and the legitimate means to achieve them.

6.5 **Institutional Anomie Theory (IAT):** Specifically examines how an overemphasis on economic achievement can lead to higher rates of cybercrime.

6.6 Space Transition Theory: A newer framework developed specifically for cybercrime, suggesting that people behave differently in "cyber-space" than they do in physical "land-space" due to anonymity and the lack of physical boundaries.

Summary of Theoretical Applications

Theory	Focus of Explanation	Common Cybercrime Examples
Routine Activity	Opportunity and lack of protection	Phishing, malware distribution
Social Learning	Peer influence and skill acquisition	Hacking, digital piracy
Strain Theory	Emotional coping with societal pressure	Online scams, cyber-harassment
Social Control	Failure of social bonds to prevent deviance	Youth-led cybercrime, data theft

7. SOCIAL FACTORS BEHIND CYBERCRIME

Social factors behind cybercrime are rooted in the **modern obsession with material success** combined with a significant **decline in traditional social control** within digital spaces. Institutional Anomie Theory suggests that when society prioritizes wealth above all else, individuals may bypass legal means to achieve it, fueling the rise of online scams and financial fraud. This behavior is often reinforced through **social learning**, where association with delinquent peer groups or specialized online forums provides the technical "know-how" and moral justification to engage in hacking or piracy.

Furthermore, the **anonymity and physical distance** inherent in the internet reduce the fear of social stigma, leading to a "deindividuation" effect where offenders feel less empathy for victims they cannot see. Finally, as digital dependency grows, a lack of **"capable**

guardianship"—exemplified by low technical literacy among vulnerable demographics like the elderly—creates a constant supply of easy targets, making cyber-offending a low-risk, high-reward social phenomenon.

8. SOCIAL CONTROL AND REGULATION

Social control and regulation in the digital age involve a combination of **formal legal frameworks** (direct regulation) and **sociological mechanisms** (indirect regulation) designed to manage online behavior and mitigate cybercrime.

8.1. Theoretical Perspectives on Social Control

Social control theory suggests that an individual's bond to society—through attachment, commitment, involvement, and belief—reduces the likelihood of deviant behavior.

- **Internal vs. External Constraints**: Regulation occurs through internal moral commitments (socialization) and external structural constraints like laws and surveillance.
- **Indirect Prevention**: Education and the promotion of "conscientious use of the internet" serve as indirect social control tools to prevent cybercrime by aligning user values with legal norms.
- **Space Transition Theory**: This theory explains that individuals may behave differently in cyberspace compared to "meat space" (physical world) due to perceived anonymity and lack of immediate social consequences.

8.2. Formal Regulatory Frameworks (India)

Modern regulation is built upon specific statutes that define offences and empower authorities:

- **Information Technology (IT) Act, 2000:** The primary legislation for cyber law, covering identity theft (Sec 66C), privacy violations (Sec 66E), and child pornography (Sec 67B).
- **IT Rules, 2021**: Imposes "due diligence" on social media intermediaries to remove unlawful content within 24–72 hours.
- **Digital Personal Data Protection (DPDP) Act, 2023**: Regulates how personal data is processed, focusing on user consent and protecting children from tracking or harmful advertising.
- **Bharatiya Nyaya Sanhita (BNS), 2023**: Replaces parts of the IPC to address modern harms like misinformation and electronic obscenity.

8.3. Institutional Mechanisms of Control

Beyond laws, specialized bodies enforce digital order:

- **Indian Cyber Crime Coordination Centre (I4C):** National hub for coordinating cybercrime response across various states.
- **CERT-In:** The national agency for incident response, issuing guidelines on security threats and mandatory reporting.
- **National Cyber Crime Reporting Portal:** A public-facing tool allowing citizens to report incidents directly to law enforcement.

9. INDIAN CONTEXT

Cyber Crimes are a new class of crimes which are increasing day by day due to extensive use of internet these days. To combat the crimes related to internet The Information Technology Act, 2000 was enacted with prime objective to create an enabling environment for commercial use of Information Technology. The Information Technology Act specifies the acts which have been made punishable. The Indian Penal Code, 1860 has also been amended to take into its purview Cyber Crimes. The various offenses related to internet which have been made punishable under the IT Act and the IPC are enumerated below:

9.1 Cyber Crimes under the IT Act

- Tampering with Computer source documents - Sec.65
- Hacking with Computer systems, Data alteration - Sec.66
- Publishing obscene information - Sec.67
- Un-authorised access to protected system Sec.70
- Breach of Confidentiality and Privacy - Sec.72
- Publishing false digital signature certificates - Sec.73

9.2 Cyber Crimes under IPC and Special Laws

- Sending threatening messages by email - Sec 503 IPC
- Sending defamatory messages by email - Sec 499 IPC
- Forgery of electronic records - Sec 463 IPC
- Bogus websites, cyber frauds - Sec 420 IPC
- Email spoofing - Sec 463 IPC
- Web-Jacking - Sec. 383 IPC
- E-Mail Abuse - Sec.500 IPC

9.3 Cyber Crimes under the Special Acts

- Online sale of Drugs under Narcotic Drugs and Psychotropic Substances Act.
- Online sale of Arms Arms Act.

10. PREVENTIVE MEASURES TO AVOID CYBER CRIMES

♣ Cyber Forensics can be used to detect cyber Evidence

♣ To make necessary amendments not to suppress the criminal activity, this act has defined certain offences and penalties to smother such omissions, which is understood to come within the characterization of Cyber Crimes. From this it can be inferred that the law cannot afford to be static, it has to change with the changing times and viz. cyber space this is all the more required, as there many application of the technology that can be used for the betterment of the mankind, similarly it equally true that such application can also be used for the detriment of the mankind as has been demonstrated by the Spy–cam case. The bottom–line is that the law should be made flexible so that it can easily adjust to the needs of the society and the technological development. Cyber cell of the law enforcement agencies have started operating in metropolitan cities like Pune, Mumbai, Hyderabad, Chennai, Bangalore etc. in Indian laws to control on Cyber Crimes (Yougal Joshi, 2013)**.**

11. CONCLUSION

Cybercrime is best defined as any crime that is committed over the internet. Cybercrime has been an issue ever since the birth of the internet, dating back to as early as the 1980s. Technology currently plays a big part in people's lives, especially in this era of technology evolution, which has led to the ability of criminals to abuse technology for personal gain.

A Sociological perspective shows that cybercrime and digital deviance are not merely technical or legal problem, but social phenomena rooted in;

- ❖ Inequality
- ❖ Power relation
- ❖ Cultural norms
- ❖ Institutional weaknesses

Understanding cybercrime sociologically helps design ethical, inclusive and socially informed digital policies rather than purely punitive responses.

REFERENCE

1. Dr. Jyoti Sidana (2024): Sociology of Cyber Crime: A Discourse Analysis with Special Reference to India.
2. Rahaf Salem Darabseh and Ahed J Alkhatib: The Sociology of Cybercrime: Causes and Prevention .
3. Roderick S. Graham, 'Shawn K. Smith (2019): Cybercrime and Digital Deviance
4. Brennrer W Susan, (2010), “Cyber Crime Criminal Threats form Cyberspace” Praeger, New York.
5. Bhanot,Astha, (2013), Gender Violence, Pointer, Jaipur, India https://ncrb.gov.in/sites/default/files/CII%202020%20Volume%201.pdf http://debaraticyberspace.blogspot.com .
6. Farooq, Ahmad (2011), “ Cyber Law in India”, New Era law, New Delhi .
7. Halder Debarati and K. Jaishankar (2011), “Cyber Crime and Victimization of Women’s Law, Rights and Regulation”. IGI Global, New York.
8. Kumar, Sanjeev&Priyanka,. (2019). CYBER CRIME AGAINST WOMEN: RIGHT TO PRIVACY AND OTHER ISSUES,
9. Dr. Sumathi (2020): Cyber crime in India: A theoretical study