



THE EVOLVING CRIMINAL LANDSCAPE OF NORTHWESTERN INDIA: FROM TRADITIONAL BANDITS TO DIGITAL THREATS

*Mehak Marodia**

Abstract

In an age where technology is the backbone of ultramodern civilization, a silent yet redoubtable trouble is growing at an intimidating rate — cybercrime particularly in northwestern states. As the expression "new wine in an old bottle", representing an apt description of cybercrime. This exploration examines how states like Punjab, Haryana, and Rajasthan, formerly agonized by traditional crimes, bandits, now face cybercriminal orchestrating large- scale fiscal frauds, phishing swindles, and identity theft. The study delves into case studies such as phishing scams, bank Heists, Punjab's ₹150 crore darknet drug trade operations, Rajasthan's Alwar sextortion racket illustrate India's western borders to punctuate the socio-economic and security counteraccusations representing cybercrime from transition of cultural by digital age leading to internet crime. The study hypothesizes on India's legal frame, the IT Act, 2000, BNS 2023, Digital Personal Data Protection Act, with international scenario, further marking significant challenges.

Keywords: Cybercrime, Traditional Crimes, Digital Transformation of Crime, Legal Framework (IT ACT,2000), Challenges, Visionary Strategy

*

Student, BA. LL.B. 2nd Semester, University Institute of Legal Studies, Panjab University, Chandigarh. Email: maroriasunita@gmail.com, Contact No.-8168374201

I Introduction

"The Internet is becoming the town square for the global village of tomorrow." – Bill Gates.

YET, AT the very heart of this digital village, a new breed of bandits has become apparent—not with swords and firearms, but with malware, phishing scams, and data theft, hacking– Cybercrime. Peace is one of the paramount requisites of human in any society. The economic development and hence overall development of the economy to a large extent depends on the peaceful environment i.e. absence of violence. Freedom from violence, as an aspect of the quality of life, is a neglected issue in development studies.¹ But what if this violence becomes non visible, what if it doesn't remain what is traditionally, we believe? How does the alarming rise of cybercrime in India, evidenced by the emergence of digital equivalents to traditional offenses (e.g., online heists replacing dacoity, digital arrests mimicking kidnapping and so forth), necessitate a shift in law enforcement focus and resource allocation, without undermining the ongoing need to address persistent traditional criminal activities?

Traditionally, violence was defined by physical aggression—wars, dacoity, and personal assaults. However, with the advent of the digital era, violence has transcended physical boundaries, emerging as cybercrime.² Freedom from violence is an essential capability that contributes to the quality of life.³ India has recorded the second-highest

¹ Neha Gupta & Lalit, "Crime in India: An Inter-State Analysis" 18(1) *Maharshi Dayanand University Research Journal ARTS* 82 (2019).

² *Id.*

³ Amartya Sen, *Commodities and Capabilities* 70 (Oxford University Press, England, 1985).

number of encrypted cyber-attacks globally, with 5.2 billion attacks between October 2023 and September 2024, according to the Zscaler ThreatLabz 2024 Encrypted Attacks Report⁴.

II Digital Boom: Explosion of Cyber Crime

The label "Cybercrime" is a misnomer. This term is comprehensible but has nowhere been specified in any Act passed or enacted by the Indian Parliament. Cybercrime is not utterly dissimilar from the concept of conventional or traditional crime. Both include conduct whether act or omission, which cause breach of rules of law and counter balanced by the sanction of the state⁵. Cybercrime is a complicated problem in the cyber world.

What is Cyber crime?

According to Van der Merwe the American author Donn B Parker defined computer crime as: - *"any intentional, malicious act associated with computers as objects, subjects, instruments or symbols in which a victim suffered a loss and a perpetrator made, or may have made, a gain"*.

*"The computer didn't make it easier to steal, but it sure did make it, faster."*⁶

Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as:

⁴ KV Kurmanath, "At 5.2 billion attacks, India ranks second globally in encrypted cyberattacks: Zscaler", *The Hindu*, December 13, 2024.

⁵ Parthasarathi Pati, Cyber Crime available at <https://www.naavi.org/pati/pati_cybercrimes_dec03.htm> (last visited on 27 February 2025).

⁶ Donn B. Parker, *Crime by Computer* 194 (Charles Scribner's Sons, New York, 1976).

*"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice b.oards and groups) and mobile phones (SMS/MMS)."*⁷

Ritu Kohli Case: Recognized as India's first cyber stalking incident, a woman named Ritu Kohli reported receiving obscene calls due to a perpetrator impersonating her in online chat and sharing her personal contact information.⁸

Factors contributing to cyber crimes

Lack of Security Awareness: Many individuals or organizations unknowingly click on suspicious links without understanding the security risks.⁹ Only amateurs attack machines; professionals target people.¹⁰ Example: - The Bangladesh Bank Heist (2016), Even a central bank failed to follow basic cyber security protocols, proving that lack of awareness can lead to massive financial losses.

Financial motivation (Monetary gains): Cyber criminals go to the range of carrying out personal data theft, phishing, hacking bank accounts, or deploying ransom ware. Sociologist Robert K. Merton, in his

⁷ Debarati Halder and K. Jaishankar, *Cyber Crime and the Victimization of Women: Laws, Rights and Regulations* 15 (Information Science Reference, United States of America, 2012).

⁸ Priya Gupta and Dr. Abhay Chand Mall Visen, "Cyberstalking Against Women in the Indian Perspective: An Overview" 29 *IOSR Journal of Humanities and Social Science* 58 (2024).

⁹ Factors Causing Cyber Crimes to Easily Occur - INDONET, available at: <https://indonet.co.id/factors-causing-cyber-crimes-to-easily-occur/> (last visited on 2 March 2025).

¹⁰ Bruce Schneier, *Schneier on Security* 50 (Wiley Publishing, Inc., Indianapolis, 2008).

Strain Theory, argues that when legitimate means to success are blocked, individuals turn to illegal methods. This applies to financially motivated cybercriminals seeking wealth through hacking, fraud, and ransom ware attacks.¹¹

Political and Geopolitical motives: Cyber warfare is the new battlefield where nations fight without traditional weapons, using code and intelligence as their primary arsenal.¹² Example: - Chinese Espionage Campaign Infiltrating U.S. Government Emails (May 2023):¹³ leading to criticism of Microsoft's security measures and highlighting the evolving tactics of state-sponsored cyber threats.

III Unfolding Face of Traditional Crimes: in North West India

There is various traditional crime prevalent in India mainly in North western states, like terrorism, Honor killings, kidnapping, and so forth:

Terrorism

Terrorism was the sole weapon of Pakistan in Punjab, a Northwestern State. Khalistan is of strategic importance to Pakistan. It firmly believes that non-existence of a barrier at the Indo-Pakistan border is a dangerous situation for security of and Khalistan as a buffer state would provide barrier that would ensure territorial integrity of Pakistan, simultaneously, carving out Khalistan would cut the Jammu & Kashmir

¹¹ Robert K. Merton, *Social Theory and Social Structure* 131 (The Free Press, New York, 1968).

¹² *Supra* note 10 at 216.

¹³ Department of Justice, U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure, *available at*: <https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical> (last visited on 2 March 2025).

from Indian roadways and railways that is crucial for India.¹⁴ Pakistan's Inter-Services Intelligence (ISI) is employing new strategies to revive militancy in Punjab and putting pressure on the remaining militants to undertake some sensational terrorist actions, according to official sources here.¹⁵ Pakistan-based Punjab militant groups, particularly Khalistan Commando Force (Panjwar) (KCF-P). Babbar Khalsa International (BKI) and International Sikh Youth Federation (ISYF), are under pressure from ISI to undertake some sensational terrorist actions in India.¹⁶

The Nexus of Cattle Smuggling and Lynching in Haryana

The illegal cattle trade, oftentimes chained to beef transportation and slaughterhouses, has inflamed mob violence, yielding in brutal lynchings. India cannot and should not be allowed to descend into chaos and civil unrest as happening in Syria, Iraq, Lebanon etc., under the machination of Centre Intelligence Agency and US Imperialism. The danger of both majority and minority communalism needs to be resisted and reduced to create and maintain a modern civil society which is possible only by strengthening the class unity of the peasantry as well as the working class.¹⁷ 97% of all cow-vigilante attacks reported since 2010.¹⁸ About 25 of 29 persons who were lynched were Muslims. Of all victims, killed or injured, whose identities were reported in the media, 53% were Muslim,

¹⁴ Jimmy Singh Kushwaha and Rupali Rathore, *Cross Border Terrorism in India* 164 (SSDN publishers & distributors, New Delhi, 2017).

¹⁵ Editorial, "ISI putting pressure on Punjab Militants" *The Tribune*, July 28, 1999.

¹⁶ *Supra* note 15 at 165.

¹⁷ Bhumi Adhikar Andolan, "Divide and Rule in the Name of Cow: Report of Fact-Finding Team on Lynchings in Haryana and Rajasthan" 3 (2018).

¹⁸ Indiaspend, 25 Cases Of Cow-Related Violence In 7 Months Of 2017, Surpassing 2016 As Worst Year *available at*: <http://www.indiaspend.com/26-cases-of-cow-related-violence-in-7-months-of-2017-equalling-2016-as-worst-year-21119> (last visited on 3 March 2025).

12% were Dalit, and 10% were Hindu. Among the 78 incidents reported, the number of total victims was 293, 29 of those persons were lynched. 50 out of 78 incidents occurred in Northern India.

According to the National Crime Records Bureau (NCRB) 2023 report, Haryana recorded, 23 incidents of mob lynching linked to cow protection vigilantes between 2015 and 2023. 47% increase in violence related to cow protection from 2018 to 2023. The 2023 Haryana riots commonly referred to as the Nuh violence were a series of clashes in northern India, Clashes broke out between two groups in Haryana's Muslim-dominated Nuh district on July 31 during Vishwa Hindu Parishad's Brij Mandal Jalabhishek Yatra with the armed mob pelting stones and setting the vehicles on fire.¹⁹ *The Pehlu Khan Lynching Case (2017)*²⁰ On April 1, 2017, Pehlu Khan, a dairy farmer from Rajasthan, was lynched by cow vigilantes near Behror in Alwar, on the Haryana-Rajasthan border. He was transporting cattle with a valid permit, but the mob accused him of smuggling cows for slaughter. The case drew national and international outrage, highlighting the rising mob justice trend under the guise of cow protection. The Haryana Gauvansh Sanrakshan and Gausamvardhan Act, 2015²¹, The Prevention of Cruelty to Animals Act, 1960²²: Prohibits illegal cattle transportation. It is an offense to cruelly transport, confine, chain or tether an animal, and Prevention of Mob Lynching Act, 2022.²³

¹⁹ The Hindu Bureau, "Clashes break out between two groups during VHP procession in Haryana's Nuh; prohibitory orders imposed" *The Hindu*, Aug. 1, 2023.

²⁰ Special Correspondent, "Pehlu Khan lynching case: HC issues warrant against accused" *The Hindu*, Sep. 7, 2021.

²¹ Haryana Gauvansh Sanrakshan and Gausamvardhan Act, 2015 (Haryana Act 20 of 2015), s. 13.

²² The Prevention of Cruelty to Animals Act, 1960 (Act 59 of 1960).

²³ The Prevention of Mob-Lynching Bill, 2022 (Bill no. 209 of 2022).

Honor Killings

Sharif Kanaana, professor of anthropology at Birzeit University, says that Honour killing is: *"A complicated issue that cuts deep into the history of Arab society. What the men of the family, clan, or tribe seek control of in a patrilineal society is reproductive power. Women for the tribe were considered a factory for making men. The honour killing is not a means to control sexual power or behavior. What's behind it is the issue of fertility, or reproductive power."*²⁴

An honour killing is the homicide of a member of a family or social group by other members, due to the belief of the perpetrators that the victim has brought dishonour upon the family or community.²⁵ In northern regions of India, mainly in the Indian states of Uttarakhand, Punjab, Rajasthan, Haryana, Uttar Pradesh also many instances of honour killings have been noted. Even as these incidents take place across the country, these two states (Punjab and Haryana), however, rank ahead. According to data compiled by the Punjab Police, 34 honour killings were reported in the state between 2008 and 2010: ten in 2008, twenty in 2009, and four in 2010. Haryana is also notorious for incidents of honour killing, mainly in the upper caste of society, among raj puts and jaats. Bhagalpur in the eastern Indian state of Bihar has also been notorious for honour killings. Recent cases include a 16-year-old girl, Imrana, from Bhojpur who was set on fire inside her house in a case of what the police called

²⁴ Arun Pal, *Honour killing Culture, Dilemma and Ritual 2* (Arise Publishers & distributors, New Delhi, 2012).

²⁵ Aishwarya Sandeep, Honour Killings in India available at: <https://aishwarya.sandeep.wordpress.com/2021/06/25/honour-killings-in-india/> (last visited on 5 March 2025).

'moral vigilantism'.²⁶ *Manoj-Babli Honor Killing Case (2007) – Haryana*²⁷, *Nitish Katara Murder Case (2002) – Uttar Pradesh*²⁸. Honor killings are not restricted to Northwestern India; they are prevalent globally. The number of women and girls in the UK suffering violence and intimidation at the hands of their families or communities is increasing rapidly reports went up by 47% in just a year.²⁹ The Prohibition of Unlawful Assembly (Interference with the Freedom of Matrimonial Alliances) Bill, 2011: Proposed a ban on Khap Panchayats' unlawful activities but remains pending. In 1990 the National Commission for Women set up a statutory body in order to address the issues of honor killings among some ethnic groups in North India³⁰.

Syrian law: July 1, 2009, President Bashar al-Assad abolished *Article 548* of the Penal Code, which had waived punishment for a man found to have killed a female family member in a case "*provoked*" by "*illegitimate sex acts*," as well as for a husband who killed his wife because of an extramarital affair.³¹ In Haiti, Article 269 of the Penal Code states that "in the case of adultery as provided for in Article 284, the murder by a husband of his wife and/or her partner, immediately upon discovering them in flagrante delicto in the conjugal abode, is to be pardoned." The

²⁶ Dr. P. Chand Basha, "Honour Killings – Causes" 4 *International Journal of Enhanced Research in Educational Development* 33-34 (2016).

²⁷ *Seema vs State Of Haryana & Ors.*, 2024:PHHC:024668.

²⁸ *State vs. Vikas Yadav & Vishal Yadav*, S.C. No. 78/2002.

²⁹ Rachel Williams, "Honour crimes against women in UK rising rapidly, figures show" *The Guardian*, Dec.3, 2011.

³⁰ Himani Grover, Essay on Honor killing in India, *available at*: <https://www.civilserviceindia.com/subject/Essay/honor-killing-in-india4.html> (last visited on 7 March 2025).

³¹ Syria: No Exceptions for 'Honor Killings, Human Rights Watch, *available at*: <https://www.hrw.org/news/2009/07/28/syria-no-exceptions-honor-killings> (last visited on 6 March 2025).

law is not applicable to murder by a wife of her husband.³² "Honor killings reflect deep-seated patriarchy and caste-based violence, where women are viewed as bearers of family honor.

Bandits

Banditry is a type of organized crime committed by outlaws typically involving the threat or use of violence. A person who engages in banditry is known as a bandit and primarily commits crimes such as extortion, robbery, kidnapping, and murder, either as an individual or in groups.³³

The Chambal Dacoits (1930s–1970s) – Rajasthan and Uttar Pradesh

The Chambal Valley, spanning parts of Rajasthan, Uttar Pradesh, and Madhya Pradesh, was a notorious hub for dacoit gangs. Phoolan Devi, the Bandit Queen, led a gang of dacoits and carried out revenge killings and looting in the 1980s. Man Singh, known as the "Robin Hood of Chambal," operated in the region during the 1930s–1950s. **The Bawaria Gang Heists:** The Bawaria gang, a notorious group of highway robbers, operated across Haryana, Rajasthan, and Punjab.

Murder

In Northwestern India, comprising Haryana, Punjab, Rajasthan, and parts of Uttar Pradesh, the incidence of murder has been steadily rising, fueled by caste violence, honor crimes, political rivalries, land disputes, and organized crime.

³² Stop Violence Against Women, Causes and Risk Factors for "Honor" Killings and Crimes *available at*: https://www.stopvaw.org/causes_and_risk_factors2 (last visited on 8 March 2025).

³³ Wikipedia, Banditry *available at*: <https://en.m.wikipedia.org/wiki/Banditry> (last visited on 8 March 2025).

Sl	State/ UT	2020	2021	2022	Mid-Year Projected Population in lakhs (2022)	Rate of Murder (2022)	Charge sheeting Rate (2022)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	Andhra Pradesh	853	956	925	530.3	1.7	93.1
2	Arunachal Pradesh	45	49	56	15.5	3.6	75.3
3	Assam	1131	1192	1072	354.9	3.0	37.1
4	Bihar	3150	2799	2930	1255.3	2.3	92.1
5	Chhattisgarh	972	1007	1013	299.5	3.4	93.0
6	Goa	34	26	44	15.7	2.8	88.6
7	Gujarat	982	1010	959	709.3	1.4	91.8
8	Haryana	1143	1112	1020	299.7	3.4	74.0
9	Himachal Pradesh	91	86	85	74.4	1.1	90.3
10	Jharkhand	1592	1573	1550	391.4	4.0	81.5
11	Karnataka	1331	1357	1404	674.1	2.1	90.2
12	Kerala	306	337	334	356.8	0.9	96.1
13	Madhya Pradesh	2101	2034	1978	858.9	2.3	94.7
14	Maharashtra	2163	2330	2295	1257.4	1.8	92.5
15	Manipur	46	46	47	32.0	1.5	37.5
16	Meghalaya	79	80	72	33.3	2.2	37.3
17	Mizoram	28	24	31	12.3	2.5	95.7
18	Nagaland	25	27	21	22.2	0.9	62.1
19	Odisha	1470	1394	1379	460.8	3.0	77.0
20	Punjab	757	723	670	306.0	2.2	83.7
21	Rajasthan	1719	1786	1834	804.4	2.3	57.5
22	Sikkim	11	14	9	6.8	1.3	100.0
23	Tamil Nadu	1661	1686	1690	767.1	2.2	96.9
24	Telangana	802	1026	937	379.5	2.5	92.2
25	Tripura	114	122	109	41.2	2.6	72.3
26	Uttar Pradesh	3779	3717	3491	2340.9	1.5	83.0
27	Uttarakhand	160	208	187	115.6	1.6	78.6
28	West Bengal	1948	1884	1696	987.6	1.7	82.9
	Total State(s)	28493	28605	27838	13403.0	2.1	81.2

The increasing rate of murder is centre of attention in several north-western states of India. Haryana, for example, recorded a murder rate of 3.4, succeeded by Rajasthan at 2.3 and Punjab at 2.2. Notably, even Uttar Pradesh, while having a lower rate compared to its neighbors at 1.5, still bestows to the altogether burden of violent crime. This data underscores that law enforcement agencies continue to grapple with deeply entrenched traditional criminal activities. With the help of this data, it can be comprehended that the rate of Murder is not at a decrease. Against this backdrop of persistent traditional crime, India is simultaneously witnessing an alarming surge in cybercrime.

Simultaneously, the exponential growth of cybercrime presents a parallel and increasingly complex challenge.

IV The Digital Transformation of Northwestern India's Criminal Landscape

The major distinguishing criteria between digital and traditional crime is not the crime itself, but the speed and scale at which it can now be committed. For decennium, traditional crimes such as banditry, dacoity, honor killings, and terrorism subjugated the crime landscape of Northwestern India. However, with the onset of the digital age, a new breed of crime has become apparent—cybercrime, which is gradually obscuring this conventional misdemeanor. The region, once plagued by dacoits, highway robbers, and land-related murders, is for the time being beholding a shocking surge in phishing, hacking, ransomware attacks, identity theft, scams and digital arrests and never-ending list.

From Dacoity to Digital Heists

Dacoity, defined under Section 310 of BNS³⁴, involves armed robbery by five or more persons. It has historically been rampant in rural Rajasthan, Haryana, and Punjab. Modern Cybercrime Parallel: - Bank hacking, online financial fraud, and phishing have displaced physical dacoities. Instead of storming into banks or homes, cybercriminals empty accounts digitally. Nainital bank's server hack case in which some unidentified accused allegedly siphoned off ₹16.71 crore in 84 transactions using the bank manager's credential.³⁵ Twitter Breach (2022): The Twitter APIs faced a classic case of excessive data exposure in 2022 when attackers sold 5.4

³⁴ Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023), s. 310.

³⁵ Arun Singh, "Nainital Bank's server hacking: Police freeze ₹1.90 crore across India" *Hindustan Times*, July 27, 2024.

million users' information on a hacking forum. In January 2023, attackers further scraped 400 million users' public and private data, selling it on the dark web.³⁶

From Kidnapping to Digital Arrests

Kidnapping under Section 140 in BNS involves forcibly abducting individuals for ransom or coercion. It was a common crime in Northwestern states, especially targeting businessmen and landowners. Modern Cybercrime Parallel: **Digital arrest and virtual kidnapping** have emerged, where victims are digitally abducted through fake police calls or ransomware attacks. A case in Faridabad where a man was duped into traveling to Bihar after receiving a video call from individuals posing as CBI and TRAI officials while his family was away. His bank account was subsequently emptied, highlighting "digital arrest" tactics through official impersonation. One identified himself as a CBI officer – a Deputy Commissioner of Police (DCP) and the other as an officer with Telecom Regulatory Authority of India (TRAI).³⁷ Digital arrest is prominently done by impersonating some official to gain confidentiality. Fake money laundering case: 77-year-old kept under 'digital arrest' for a month, loses Rs 3.8 crore, *this tactic is no longer limited to India—it has emerged as a global threat, with cases reported in the USA, China, Australia, and Europe, targeting individuals, corporations, and even government officials.* - In 2019, in Mexico City, several wealthy individuals were victims of a digital arrest scam. Scammers posed as federal police officers, claiming the victims were linked to drug cartels.

³⁶ Venkatesh Sundar, "39 Most Notorious Hacks in History that Fall Under OWASP Top 10" *Indusface*, Feb. 19, 2025.

³⁷ HT News Desk, "Digital arrest scam: Ex Air Force employee made to travel from Faridabad to Bihar, bank account wiped clean" *Hindustan Times*, Nov. 27, 2024.

Australian police warned of a massive wave of digital arrest scams. Victims received calls from individuals claiming to be from the Australian Federal Police.

Anti-Scam Caller Tunes: In response to the rise in "digital arrest" scams—where fraudsters impersonate officials to extort money—authorities have implemented caller tunes warning the public about such schemes. Cyber Crime Helpline is 1930. European union: General Data Protection Regulation (GDPR) (2018) Protects personal data from cyber threats by imposing strict security standards. European union is the 1st country to address it; The General Data Protection Regulation (GDPR) is the toughest privacy and security law in the world. The GDPR will levy harsh fines against those who violate its privacy and security standards, with penalties reaching into the tens of millions of euros.³⁸

Impact on Women: Digital Exploitation Replacing Physical Crimes

Women in Northwestern India, previously vulnerable to honor killings, dowry violence, and sexual assault, are now increasingly targeted through cybercrimes, including cyber stalking, harassment, and revenge pornography. Rajasthan: Nagaur records maximum number of pornography cases in last four years, according to the data provided by Rajasthan's Home Department in the state assembly.³⁹ Cyber stalking and harassment have replaced physical forms of intimidation. Women are now targeted through hacking social media accounts and morphing images. In 2022, a site was launched under the name 'Bulli Bai' that contained doctored pictures of few Muslim women. This was aired on

³⁸ General Data Production Regulation, European Union Security Laws, EU, *available at*: <https://gdpr.eu/what-is-gdpr> (last visited on April 2, 2025).

³⁹ PTI, "Rajasthan: Nagaur records maximum number of pornography cases in last four years" *Deccan Herald*, July 23, 2023.

twitter as “deal of the day.” Along derogatory content. These photos are contended to be taken from social media handle, edited and loaded to the website without women's consent. The content was allegedly uploaded to create tension and discord between religious groups in India. A man in California, USA was arrested and sentenced to 5 years in prison for cyber stalking multiple young women.⁴⁰

V Legal Provisions against Cyber Crime: The Demur of Defining and Punishing Evolving Digital Offenses

In India's northwestern states, the rise of cybercrime is posing a unique legal challenge. Unlike traditional crimes such as dacoity, murder, and kidnapping, which are clearly defined under the Bhartiya Nyaya Sanhita (BNS),²⁰²³ with codified punishments, cybercrimes mature swiftly—making it arduous for legal frameworks to keep pace.

Existing Legal Framework in India

The Information Technology (IT) Act, 2000, provides legal recognition to electronic transactions and addresses cyber offenses. IT Act 2008 added updated and redefined terms for current use, expanding the definition of cybercrime and the validation of electronic signatures. It also strongly encourages companies to implement better data security practices and makes them liable for data breaches⁴¹. Information Technology (Amendment) Act, 2021: Expanded the definition of cyber terrorism and enhanced the accountability of intermediaries, including social media

⁴⁰ Department of Justice, Former Marine Sentenced for Cyberstalking Young Women in Sextortion Campaign, *available at*: <https://www.justice.gov/archives/opa/p/former-marine-sentenced-cyberstalking-young-women-sex-tortion-campaign> (last visited on 9 March 2025).

⁴¹ UpGuard, Top Cybersecurity Regulations in India, *available at*: <https://www.upguard.com/blog/cybersecurity-regulations-india> (last visited on 9 March 2025).

platforms. *The Digital Personal Data Protection Act* was passed in early August of 2023. The law outlines the rights of data principals, obligations of data fiduciaries, penalties for data breaches, and introduces a special category called significant data fiduciaries. *Indian Computer Emergency Response Team (CERT-In)*⁴²: Functioning under the Ministry of Electronics and Information Technology, (CERT-In) is the national agency responsible for responding to cyber security incidents. CERT-In also operates the *Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre)*, launched in 2017 to detect compromised systems and provide tools for malware removal. *Shreya Singhal v Union of India*⁴³, The Supreme Court declared Section 66A of the Information Technology Act, 2000, unconstitutional and struck it down. This judgment affirmed the importance of protecting free speech and expression while also establishing that any restrictions imposed should be precise and not open to arbitrary interpretation.

Increase in Cyber Police Units, in 2023, Haryana established three new cyber police stations in Gurugram, Faridabad, and Karnal.⁴⁴ Punjab SIM Swap Fraud (2023): *A gang in Ludhiana conducted large-scale SIM swapping fraud, transferring funds from victims' accounts.* Arrested under Section 66C (identity theft) and Section 66D (impersonation) of the IT Act. Despite arrests, financial recovery was difficult due to the use of crypto currency wallets, which remain untraceable. In Jaipur, the police

⁴² Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, India, *available at*: <https://www.cert-in.org.in/> (last visited on March 9, 2025).

⁴³ AIR 2015 SC 1523.

⁴⁴ Debashish Karmakar, "Gurugram gets three new cyber police stations" *Hindustan Times*, June 25, 2022.

conducted awareness programs on digital arrests and phishing. Introduced cyber literacy programs in the schools and colleges.⁴⁵

However, to understand more effectively we can have a glimpse of Various countries and international bodies who have implemented measures to combat cyber threats effectively. *The Computer Fraud and Abuse Act (CFAA) of 1986* is United States legislation that imposes criminal penalties on individuals who intentionally access a protected computer without proper authorization or whose access exceeds their authorization.⁴⁶ France's new cybercrime law, effective January 2023, positions the country as a leader in combating online crime. *The LOPMI law* includes a €15 billion, five-year plan to address security threats and holds tech executives, like Telegram CEO Pavel Durov, criminally responsible for crimes on their platforms. Durov was formally charged and faces up to 10 years in prison and fines of €500,000 (\$556,300).⁴⁷ Even, UN Secretary-General António Guterres welcomed the adoption of the Convention – the first international criminal justice treaty to have been negotiated in over 20 years.⁴⁸

Challenges in Cybercrime Law Enforcement

Though we have strong provisions for handling cybercrime but the increasing rate of it reminds us that there still persist many challenges in Cybercrime law enforcement, some of which are as follows:

⁴⁵ TNN, "Need to increase cyber literacy among public" *The Times of India*, Apr. 17, 2021.

⁴⁶ Robert Sheldon, "Computer Fraud and Abuse Act (CFAA)" *TechTarget*, Aug. 1, 2023.

⁴⁷ Matthew Giannelis, "France's New Cybercrime Law Targets Tech Execs, Including Telegram CEO Pavel Durov" *Tech News*, Sept. 21, 2024.

⁴⁸ Vibhu Mishra, "UN General Assembly adopts milestone cybercrime treaty" *UN News*, 24 December 2024 available at: <https://news.un.org/en/story/2024/12/1158521> (last visited on 11 March 2025).

Lack of Clear Definitions: Cybercrimes such as digital arrest, virtual kidnapping, and crypto fraud are not explicitly defined in the IT Act. Law enforcement often relies on broad interpretations of existing laws, making prosecution inconsistent.

Cross-Border Crime: Cybercriminals often operate from abroad, making it difficult for Indian law enforcement agencies to track and extradite them. Example: Punjab digital fraud cases linked to Pakistan-based hackers face jurisdictional challenges. As traditional crimes are defined, we know them and they have codified punishments but cybercrime though it has cyber law, but the evolving nature it's becoming difficult to define each, and proper punishment specifying for them.

New-age cybercrimes: such as digital arrest, crypto fraud, ransomware attacks, and deepfake extortion are not explicitly defined in the Act. Law enforcement struggles to charge criminals due to the lack of specific legal provisions. The Rajasthan government released an advisory on 'Deepfakes' to spread awareness among individuals and organizations about the associated threats and possible ways of prevention. Many victims do not report cybercrimes due to stigma, embarrassment, or lack of trust in law enforcement. For instance, In Rajasthan (2023), only 30% of victims of online blackmail reported the crime due to fear of social shame.

Encryption and Anonymity Tools: Cybercriminals use VPNs, Tor networks, and encryption to hide their identities, making it difficult for law enforcement to trace them. Example: In Punjab's Dark Web Drug Trafficking Case (2024), dealers used encrypted messaging apps to evade tracking. The rise of deepfake technology makes impersonation and extortion cases harder to detect.

Police personnel lack expertise in dealing with complex cybercrimes involving cryptography, blockchain, and dark web activities, while northwestern states like Punjab and Haryana have cyber cells, they are understaffed and lack advanced forensic capabilities.

Importantly, the coexistence of old and new criminal practices reflects a dynamic strategy by criminal groups who fuses traditional tactics with digital platforms, creating a hybrid criminal ecosystem that confronts conventional policing methods in Northwestern India.

VI The Way Forward: Improving Cybercrime Law Enforcement

The rapid surge in cybercrimes across India and globally has exposed the gaps in legal frameworks, investigation capabilities, and enforcement mechanisms.

Use Strong Passwords: Use distinct user ID / password combinations for divergent accounts. Make them more complex by adding letters, numbers, special characters. After Twitter suffered major data breach in 2020: Twitter is reportedly in plans to introduce “two-factor authentication” to boost the security on its service, especially in light of the recent security breach, to prevent unauthorized access.⁴⁹

Awareness Campaigns & Digital Literacy: Public awareness can prevent individuals from falling prey to scams. The lack of digital literacy among rural communities is a critical factor contributing to their vulnerability. Over 75% of India’s internet users are new to digital platforms, and a report by the Digital Empowerment Foundation (DEF)

⁴⁹ Anuradha Shetty, “Twitter may introduce two-factor authentication” *Firstpost*, February 5, 2013.

states that more than 90% of Indians lack basic digital literacy.⁵⁰ So that they can be stay informed on the increasingly advanced tactics used in cyber-enabled financial crimes, making detection significantly more challenging. ⁵¹ Instead of abstract concepts, campaigns should use relatable and practical scenarios with examples of frequent scams to illustrate the risks.

Enhancing Digital Forensics: Establishing forensic labs in all the states with advanced capabilities for blockchain tracing, dark web analysis, and data recovery. Training the law enforcement in digital forensic skills. It enables the investigation of cybercrimes, such as hacking, online fraud, and identity theft, by uncovering critical evidence that might otherwise remain hidden. . These solutions offer significant benefits in the digital forensic investigation of various domains by leveraging the inherent strengths of blockchain technology, such as transparency, immutability, and decentralization.

Equip cyber police units with advanced tools: Such as AI-powered predictive analytics to detect potential cyber threats. Automated malware detection systems. Cyber patrolling bots to track suspicious online activities. AI-based threat detection is designed to prevent evolving threat tactics that are difficult to detect and mitigate, such as expanding attack vectors, including IoT devices, cloud deployments, and mobile devices. Its objective is to address the increasing volume and

⁵⁰ Ravi Mittal, "Building cyber resilience: Safeguarding rural communities and children in the digital age" *The Times of India*, Jan. 11, 2025.

⁵¹ Interpol, Be Cyber Aware, available at: <https://www.interpol.int/en/Crimes/Cybercrime/Be-Cyber-Aware> (last visited on March 13, 2025).

velocity of cyber-attacks, especially ransomware.⁵² For example, ML algorithms can detect and prevent fraud in financial transactions by identifying patterns that indicate fraudulent activity and flagging them for review.⁵³

VII Contribution to Existing Knowledge and Directions for Future Research

This research makes a significant contribution to criminological and legal scholarship by situating the upheaval of cybercrime within the historical context of traditional criminal practices in Northwestern India. While existing literature has often served conventional crime and cybercrime as isolated phenomena, this research signifies the interconnected evolution of these criminal forms, revealing how regional socio-economic vulnerabilities, technological innovations, and legal vacuums together shape hybrid criminal ecosystem. One of the essential impacts of this study is its focus on region-specific crime patterns, which have majorly been overlooked in national crime analyses. By documenting how former crime-prone areas — once dominated by dacoits, banditry, kidnapping and smuggling cartels — have now become locus for organized cybercrime, the research emphasizes the constancy and adaptability of criminal networks in return to dynamic occurrences.

Future research should aim for in-depth qualitative studies, incorporating fieldwork, community surveys, and interviews with local law enforcement officers and cybercrime victims, could offer vivid,

⁵² What Is the Role of AI in Threat Detection? Palo Alto Networks, *available at*: <https://www.paloaltonetworks.com/cyberpedia/ai-in-threat-detection> (last visited on March 13, 2025).

⁵³ What Is Cyber Crime? - Types, Impact & Preventions, Proof point, *available at*: <https://www.proofpoint.com/us/threat-reference/cyber-crime> (last visited on March 13, 2025).

grassroots outlooks on crime rates. A key area for future inquiry is the role of blockchain technology in this unfolding criminal landscape. While blockchain offers capability for encrypted transactions and transparent record-keeping, it is gradually being manipulated for unlawful activities such as cryptocurrency laundering, ransomware payments, and dark web transactions. Research into how law enforcement agencies can build technical competency to track and measure blockchain related crimes, will be vital in the coming years.

VIII Conclusion

This study underscores the dynamic evolution of criminality in Northwestern India, where the legacy of rural banditry and violent crime has moderately intersected with contemporary cyber-enabled offences. The research substantiates that while traditional crimes have not disappeared completely, there's an exponential growth of digital crimes, especially in states like Punjab, Rajasthan, and Haryana. One of the most concerning findings is the capacity of criminal groups to rapidly accustom to digital platforms, leveraging both local socio-economic vulnerabilities and the anonymity of cyberspace. The analysis also highlights several socio-economic factors endowing to this criminal shift, such as growing unemployment, insufficient digital literacy among vulnerable populations, and gaps in regional cyber law enforcement infrastructure. Once plagued by banditry, honor killings, dacoity, and land-related violence, the region now faces a far more complex and insidious threat—cybercrime. Unlike traditional crimes, which are physically evident, cybercrimes are borderless, anonymous, and swiftly sprouting, making them assiduous to define, investigate, and prosecute. The legal framework for conventional crimes in India is well-established,

