INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 4 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 4 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-4-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 4 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

REASONS FOR CYBER CRIMES AND CYBER CRIMINALS

AUTHOR – MOHAMMAD FAISAL SHAIKH* & MS MANASVI AGARWAL**

* STUDENT AT AMITY UNIVERSITY LUCKNOW

** ASSISTANT PROFESSOR AT AMITY UNIVERSITY LUCKNOW

BEST CITATION - MOHAMMAD FAISAL SHAIKH & MS MANASVI AGARWAL, REASONS FOR CYBER CRIMES AND CYBER CRIMINALS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (4) OF 2025, PG. 568-575, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

In the digital age, cybercrime threatens people, businesses, and governments worldwide. This article examines cybercrime incentives, cybercriminal traits, and cybercrime prevention challenges. Cybercriminals are driven by intellectual challenge, personal vendettas, political or ideological ideas, or money. These ideals drive cyberstalking, cyberbullying, cyber espionage, identity theft, cyberattacks, and financial crime. Cybercriminals range from major criminal groups to lone hackers seeking fame or a challenge, according to the report. Nation-states and politically motivated actors use cybercrime for espionage, political disruption, or strategic advantage, but business insiders are a threat driven by grievances or financial motivations. Each profile shows the complexity and diversity of cybercrime, underlining the need for specialized tactics against distinct offenders. Internet anonymity, a lack of knowledge and preparation, and weak legislative frameworks make cybercrime harder to fight. Cybercriminals often cross borders due to a lack of international coordination and outdated laws that have not kept up with cyber threats. This article recommends improving international law enforcement collaboration, cybersecurity infrastructure, and public campaigns and education to reduce cybercrime. Finally, to fight cybercrime, public awareness, technology, and law enforcement are needed. Global collaboration, solid security, and proactive education are the only ways to reduce cybercrime and make the internet safer for everyone.

Keywords: Cybercrime, Hacking, Financial fraud, Ransomware, Cyber espionage, Cyberbullying, Insider threats, Organized crime syndicates, Nation-state actors, Cybersecurity, Law enforcement, Anonymity, Digital threats, Online harassment, Cybercriminal profiles.

Introduction

Cybercrime is any illegal use of computers, the internet, or digital devices. The exponential rise of the internet and the digitization of many aspects of life have altered cybercrimes during the past 20 years. Despite the obvious benefits of widespread usage of online platforms for communication, trade, and innovation, bad actors may now more easily exploit security weaknesses in these systems. Cybercriminals may attack individuals, corporations, and governments with a wide range of tools and tactics, causing great financial, psychological, and social damage. Many internet crimes fall under the category of "cybercrime." This includes hacking, phishing, financial fraud, cyberstalking, harassment, cyberterrorism, and ransomware attacks. Mobile devices, cloud computing, and social media have given cybercriminals new targets and attack channels. Cybercrime is growing as we utilize more technology, so understanding its sources and purposes is crucial (Al-Suwaidi et al., 2018). The widespread impact of cybercrime on

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

people, businesses, and governments makes it worth studying. Cybercrime is becoming a global problem, not just for tech-savvy criminals. Cybersecurity Ventures estimates that cybercrime would cost $10.5 trillion annually by 2025, surpassing the global trade of all major illegal drugs. This alarming number highlights the problem's scope and urgency. over small stores to Fortune 500 corporations, more sophisticated cyberattacks targeted businesses in 2023, up 38% over the year before. Too often, thieves' understanding of security flaws causes disaster. Concerning is the rise of ransomware, which encrypts user data and locks machines unless a ransom is paid. Cybercrime may have far-reaching effects on society, as seen with the US Colonial Pipeline assault that caused fuel shortages. Cybercrime is driven by profit. Cybercriminals typically steal identity, financial, and credit card information from individuals and businesses. Criminals sell stolen data on the dark web or exploit it for financial fraud or identity theft. Ransomware is when cybercriminals encrypt victims' files and demand payment. When governments or large corporations are targeted, cybercrime may be financially rewarding. Hackers sometimes get into systems to prove themselves; they like deceiving security mechanisms or breaking seemingly indestructible systems (Datta et al., 2020). Because these risk-takers see their actions as a game or challenge, they may not consider the consequences. Finally, cybercrime is motivated by psychological factors, ideological beliefs, financial gain, and anonymity. Cybercriminals are continually looking for new methods to breach the law and exploit vulnerabilities, so it's crucial to understand why. The root causes of cybercrime must be addressed to develop effective preventative and mitigation methods.

2. Types of Cyber Crimes

Cybercriminals attack individuals, corporations, and governments. Each cybercrime exploits a distinct digital system vulnerability with varying degrees of sophistication. Cybercrime's many manifestations must be understood to establish effective prevention and response strategies. Some of the most common and catastrophic cybercrimes are listed here.

Hacking and Unauthorized Access

Hacking, or unauthorized access to data, networks, or computers, is a prevalent criminal. Hackers exploit software, security, or user activities to obtain unauthorized access. Once entered, they may disrupt operations or steal vital data. The biggest issue with hacking is data breaches, when attackers steal login passwords, financial information, and more. These breaches can cause huge financial losses and permanent reputation damage to businesses and individuals. The frequency and breadth of data breaches have made SMEs vulnerable since they often lack the sophisticated security infrastructure of larger enterprises. Some hackers utilize SQL injection, cross-site scripting, and social engineering to bypass security (Deora& Chudasama, 2021).

Financial Frauds

Criminals are growing better at stealing from people and companies online. Phishing, in which fraudsters impersonate trustworthy organisations to steal passwords and credit card details, is a common financial cybercrime. Phishing schemes use fake emails, texts, or websites that steal information. The thief can open bank accounts, borrow money, and submit phony tax returns using the victim's details. Identity theft victims experience emotional and financial hardship while restoring their identity and fixing the damage. Credit card fraud occurs when cybercriminals steal credit card information and make illegal purchases. This data is often accessible via hacking, phishing, or e-commerce security flaws. Since fraudsters may now operate from wherever, credit card theft has surged with internet buying. Due to its global nature, financial fraud is hard to prosecute.

Cyber Terrorism and Espionage

Cyber espionage and terrorism attack nations, infrastructure, and large companies. These

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

crimes often aim to overthrow governments, foment conflict, or steal secret data for personal or financial gain. Instead of profiting from cybercrime, cyberterrorism tries to inspire fear, disrupt essential networks, or undermine a nation's economy and military. Cyber spies break into commercial or government networks to steal data, trade secrets, or designs. Disclosure of sensitive material to hostile foreign parties for political sabotage, extortion, or leverage can devastate national security plans and initiatives (Okutan, 2019). Some states allegedly encouraged cyber espionage to gain economic and geopolitical advantages. Known as one of the most prominent cyber espionage cases, the Stuxnet virus attacked Iran's nuclear facilities to stop its nuclear development.

Online Harassment and Cyberbullying

Online harassment and cyberbullying rise with internet use, especially on social media. Online harassment includes threatening communications, misinformation, and public humiliation. Cyberbullying—harassment, threats, or degrading conduct on digital media—disproportionately impacts children and teenagers. Internet anonymity allows cyberbullies and online harassers to behave without consequence. Many victims of these crimes suffer from anxiety, depression, and self-harm or suicide. Online settings, especially social media, are hard to govern, making cybercrime prevention and prosecution challenging. Even though governments and internet companies have created reporting mechanisms and stricter content standards, online abuse persists.

Malware, Ransomware, and Denial-of-Service Attacks

A wide range of damaging programs meant to interrupt, damage, or gain unauthorized access to systems are called "malicious software," a cybercrime. Malware includes viruses, worms, trojans, and spyware. These malware programs use diverse methods to infiltrate computers. Ransomware encrypts user data and demands money to unlock it. The global rise in ransomware assaults has affected businesses hard, notably those in healthcare, energy, and banking (Kagita et al., 2022). One of the most prominent ransomware attacks, WannaCry, infected hundreds of thousands of workstations in over 150 countries in 2017. Another common cybercrime is Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS), in which offenders flood a network or website with traffic to crash or disable it. These assaults on critical websites, banks, and governments often cause massive disruption and financial damage. These attacks seldom result in data theft, but operational and reputation damage can be significant.

3. Reasons for Cyber Crimes

Multifaceted cybercrime has numerous reasons. Understanding the causes of these crimes is essential to prevention. Cybercriminals are motivated by money, grudge, or ideology and come from many backgrounds. Its anonymity, global accessibility, and legal flaws make the internet a prime location for illegal behavior. The following are frequent cybercrime motivations.

Financial Gain

Cybercriminals often want financial benefit. Cybercrimes like ransomware, fraud, and identity theft aim to profit the offenders. Fraudsters use phishing to steal sensitive information like bank account or credit card details. Criminals also steal corporate data, including client information, and sell it on underground marketplaces or use it for extortion. Recent years have seen more fraudsters encrypting victims' data and demanding payment to unlock it. This is called ransomware (Goni et al., 2022). Financial cybercrime may have severe impacts on enterprises worldwide, as the WannaCry ransomware attack of 2017 showed. The huge potential rewards and low operational costs make financial cybercrime alluring. Cybercriminals may operate from anywhere without detection, unlike traditional crimes that need physical presence and resources. Bitcoin

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

and other cryptocurrencies have made criminality more profitable by simplifying financial transactions and erasing traces.

Revenge or Personal Vendettas

Vengeance or personal grudges may drive cybercrime. Cyberstalking, cyberbullying, and doxxing—unlawful exposure of private information—come to mind. If a supervisor, coworker, or business partner has wronged them, they may turn to cybercrime for revenge. People use these strategies when they're furious with someone, whether over a breakup, a professional dispute, or a social media dispute. Internet anonymity helps them harass, threaten, and humiliate victims. Cyberbullying, when people harass, humiliate, and spread false information to get revenge, is a serious issue among today's youngsters. Such crimes can cause severe emotional and psychological trauma and lifelong scars (Goni, 2022). Workers or ex-business partners who are disgruntled with the company's treatment may access its systems or release secret information in revenge, which can damage its finances and reputation.

4. Profiles of Cyber Criminals

Cybercriminals of many backgrounds have various aims and methods. Others work alone or in larger, more organized networks with tremendous resources. New hackers with different interests and tactics have developed as cybercrime has increased in popularity. We need to know cybercriminals' traits to identify them and their methods. Here are several typical cybercriminals.

Organized Crime Syndicates

Organized crime syndicates are increasingly committing huge, well-coordinated crimes online. These criminal groups' intricate and damaging cyberattacks target businesses, banks, and government entities. These gangs commonly deploy ransomware attacks. Syndicates hack a company's network, encrypt critical data, and demand money to unlock it. One of the most famous ransomware attacks was the 2021 Colonial Pipeline hack. DarkSide, a criminal gang, extorted millions from a major US energy supplier, causing gasoline shortages. Global and scattered organized cybercrime groups make it difficult for law enforcement to track and capture (Boussi&Gupta, 2020). These syndicates include hackers, programmers, money launderers, and ransom negotiators. They can launch complex and prolonged attacks due to their professionalism and wealth. Transnational cybercrime makes prosecuting foreign cybercriminals difficult for law enforcement.

Individual Hackers

Another big cybercrime category is "lone wolves," or solo hackers. Hackers usually hack for academic curiosity, celebrity, or the thrill of tricking security systems. Possibly amateurs or semi-pros. Many new hackers are "script kiddies," using existing hacking tools or programs to target system holes without knowing how. Hackers may start by defacing websites or hacking small businesses, but they may become deadly criminals with expertise. Hackers often seek recognition on hacker communities. These forums allow hackers to brag, sell tools, and steal data. Many adolescent hackers like breaking into secured systems to prove their technological prowess. As they improve, fraudsters may steal personal information, impersonate legal firms, or sell their services to criminal groups. Hackers may do it for money or to help hacktivist organizations

Insiders and Employees

Dissatisfied employees and insiders are one of the biggest cybersecurity dangers. These individuals abuse business network access to commit cybercrimes for personal grudges, vengeance, or financial gain. Because they already have access to sensitive data or systems, insiders may commit crimes without suspicion more easily than outsider attackers. Insider risks include discreetly sharing knowledge, disrupting systems, and stealing IP (Grispos, 2021). Cybercriminals or outside competitors may pay cash to employees to

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 5 AND ISSUE 4 OF 2025
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

reveal critical information. Businesses might suffer catastrophic losses since these criminals typically have access to sensitive data including bank records, customer data, unique technology, and essential operations. To combat insider cybercrime, organizations must establish strict monitoring and security rules without alienating or distrusting their employees.

Nation-States and Political Actors

Cyber espionage, political disruption, and assaults on key infrastructure are all carried out by nation-states and politically motivated individuals, who make up another notable profile of cybercriminals. The government agencies, companies, or vital infrastructure of other countries are frequently the targets of these cybercriminals, who are frequently funded or aided by these governments. The usual goals of nation-state cyberattack include obtaining strategic advantages, disrupting enemies, or collecting key military or political information. For example, governments employ hacking tactics to acquire intelligence, steal IP, or meddle in elections; this practice has evolved into cyber espionage, a weapon of contemporary warfare. There has been much worry about the role of cybercrime in geopolitics, with accusations that nation-state actors employed cyberattacks to influence the 2016 U.S. election being one example. The Stuxnet malware, which attacked Iran's nuclear facilities, is only one example of how government-sponsored cybercriminals may do catastrophic damage. Cybercriminals from nation-states typically have access to sophisticated technology, intelligence networks, and a lot of money (Anjum, 2020). Their governments support these actors' operations, making it hard to prosecute or hold them responsible. The frequency and complexity of cyberattacks claimed by nation-states have increased, endangering the stability and security of the whole world.

5. Psychological and Sociological Factors

Psychological and societal factors often drive hackers. Understanding these dynamics is essential to creating comprehensive cybercrime prevention and protection measures.

Psychological Factors

Cybercriminals often behave due to mental health and personality disorders. For instance, narcissism may fuel cybercrime. Narcissists may commit cybercrime to show off their self-importance and expertise. They may brag about their hacks in online communities or break into secured systems to steal data. Psychological disorders like antisocial personality disorder, which causes a person to lack empathy, integrity, and morality, are common in cybercriminals. Cybercriminals with this condition may see victims as a means to a goal, not victims. These people may crave revenge, financial gain, or personal pleasure through cybercrime, including fraud and hacking (Parikh, 2023). Furthermore, some hackers seek power or control. For reasons they may not have elsewhere, individuals feel powerful manipulating digital systems, interrupting services, or stealing important information. When people approach a breaking point, dissociation may cause them to explain their online activity and minimize their mistakes.

Sociological Factors

Socioeconomic factors also influence cybercrime. People who struggled in the real world may succeed online. Many perceive cybercrime as a way to earn money fast without the difficulties of work or school. Cybercrime may appeal to economically disadvantaged or career-stalled people due to the availability of hacking tools and the growing dark web market for stolen data. In hacker networks, peers may encourage crimes. Online communities often laud and reward system breakers and fraudsters (Aftab et al., 2022). These locations glorify cybercrime, which

encourages illegal behavior. After becoming prominent among their acquaintances, hackers may feel driven to expand their illegal actions beyond exploiting software holes. Cybercrime is also driven by rapid cash. Many find cybercrime enticing since it's low-risk, high-reward. Scams like ransomware, identity theft, and internet fraud promise fast money to many, especially young people. Since the internet is global, fraudsters may hide their identities and erase their digital footprints.

6. Challenges in Addressing Cyber Crimes

Despite growing awareness, cybercrime prevention, detection, and fight face several hurdles. Due to shifting cyber threats and technological advances, law enforcement and enterprises protecting themselves from cybercriminals confront significant problems.

Anonymity in the Digital World

Internet anonymity makes cybercrime difficult to fight. Cybercriminals may work remotely with VPNs, Tor, and many encryption layers. These technologies allow criminals to hide their names and whereabouts, making them tougher to catch. While legitimate internet activity should stay private and safe, cybercriminals utilize encryption to escape discovery. Cryptocurrencies like Bitcoin and encrypted communication channels make hackers hard to track (Assarut et al., 2019). Cybercriminals may stay anonymous and conduct cybercrimes without fear of prosecution since even the most modern investigation methods cannot penetrate their multiple layers of camouflage.

Lack of Awareness and Preparedness

Cybercrime is a major issue, yet people and companies are unprepared. Many businesses and individuals still don't grasp the need of strong cybersecurity, leaving them vulnerable to attacks. Many consumers still fall for phishing scams and give hackers important information because they can't spot suspicious emails or websites. Some firms, especially SMBs, lack the people, training, or knowledge to design and maintain adequate cybersecurity processes. Many organizations are vulnerable to cybercriminals due to poor password habits, outdated software, and inadequate data backups. Employees' inexperience of cybersecurity best practices makes them easy candidates for social engineering and other types of social engineering, and they are less likely to follow security measures, which help cybercrimes succeed (Vaishy& Gupta, 2021). Since technology evolves quickly, many people and businesses are unprepared for the latest cyber threats. Cybercriminals find new ways to exploit holes in emerging technologies like IoT, cloud computing, and AI. Inability to respond to shifting threats worsens the problem as fraudsters exploit security architectural flaws.

Weak Legal Frameworks

Lack of international coordination and outdated laws hinder cybercrime prevention. Many nations' cybercrime laws are weak and fail to penalize highly experienced hackers. Because cybercrime laws vary by country and jurisdiction, hackers crossing borders present problems. When crimes in one country affect people or organizations in another, law enforcement authorities struggle to collaborate and pursue justice. Hackers can also operate from nations with weak cybercrime legislation or law enforcement due to the global nature of the internet (Kipane, 2019). Because there is no worldwide pact or extradition convention, a cybercriminal in one country may attack a corporation in another without fear of prosecution. Cybercriminals go unpunished because governments don't cooperate. Cybercrime is always developing; thus, legal frameworks must change. International coordination is needed to identify, locate, and prosecute cybercriminals worldwide.

7. Conclusion

In conclusion, cybercrime has become a global issue for psychological, sociological, and pragmatic reasons. Most cybercriminals commit fraud, theft, and extortion for financial gain by exploiting digital network vulnerabilities. Cyberstalking, cyberbullying, and hacktivism

are motivated by personal grudges and retribution, whereas cyberterrorism and hacktivism are political or ideological. Intellectual challenge and peer groups in hacker networks also matter, especially for younger or amateur hackers. Cybercriminals take advantage of the internet's perceived impunity and ineffective law enforcement and jurisdictional barriers. The rising threat of cybercrime requires multifaceted preparation. First, nations must cooperate to enforce the law. Since cybercrime transcends borders, states must collaborate to discover, capture, and punish cybercriminals. Cybercriminals exploit gaps that may be closed by treaties, harmonised legislation, and better extradition. The second major concern is upgrading cybersecurity infrastructure across all industries. Organizations should utilize firewalls, encryption, and frequent software updates to prevent cyberattacks. Provide personnel with cybersecurity best practices training and audit security procedures often to reduce risks. Third, personal and organizational awareness is needed to reduce hackers' success rates. Public awareness campaigns, worker cybersecurity education, and increased transparency about cyber threats like phishing and identity theft may help anybody see and avoid them. Education and awareness can reduce the likelihood of people unknowingly aiding hackers by not using proper security. Finally, cybercrime prevention requires education, law enforcement collaboration, and enhanced cybersecurity. While cybercrime is ever-changing, we can all help make the internet safer by being proactive.

Reference

1. Al-Suwaidi, N., Nobanee, H., & Jabeen, F. (2018). Estimating causes of cyber crime: evidence from panel data FGLS estimator.
2. Datta, P., Panda, S. N., Tanwar, S., & Kaushal, R. K. (2020, March). A technical review report on cyber crimes in India. In *2020 International conference on emerging smart computing and informatics (ESCI)* (pp. 269-275). IEEE.
3. Deora, R. S., & Chudasama, D. (2021). Brief study of cybercrime on an internet. *Journal of communication engineering & Systems*, *11*(1), 1-6.
4. Okutan, A. (2019). A framework for cyber crime investigation. *Procedia Computer Science*, *158*, 287-294.
5. Kagita, M. K., Thilakarathne, N., Gadekallu, T. R., Maddikunta, P. K. R., & Singh, S. (2022). A review on cyber crimes on the internet of things. *Deep Learning for Security and Privacy Preservation in IoT*, 83-98.
6. Goni, O., Ali, M. H., Alam, M. M., & Shameem, M. A. (2022). The basic concept of cyber crime. *Journal of Technology Innovations and Energy*, *1*(2), 16-24.
7. Goni, O. (2022). Cyber crime and its classification. *Int. J. of Electronics Engineering and Applications*, *10*(1), 17.
8. Boussi, G. O., & Gupta, H. (2020, June). A proposed framework for controlling cyber-crime. In *2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1060-1063). IEEE.
9. Grispos, G. (2021). Criminals: Cybercriminals. In *Encyclopedia of Security and Emergency Management* (pp. 84-89). Cham: Springer International Publishing.
10. Anjum, U. (2020). Cyber crime in Pakistan; detection and punishment mechanism. *Časopis o društvenom i tehnološkom razvoju*, *2*(2).
11. Parikh, R. (2023). An Introduction to Cybercrime and Cybersecurity: The Whys and Whos of Cybersecurity. In *Cybersecurity for Decision Makers* (pp. 57-70). CRC Press.
12. Assarut, N., Bunaramrueang, P., & Kowpatanakit, P. (2019). Clustering Cyberspace Population and the tendency to Commit Cyber Crime: A Quantitative Application of Space

Transition Theory. *International Journal of Cyber Criminology*, *13*(1).

13. Vaishy, S., & Gupta, H. (2021, September). Cybercriminals' Motivations for Targeting Government Organizations. In *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)* (pp. 1-6). IEEE.
14. Kipane, A. (2019). Meaning of profiling of cybercriminals in the security context. In *SHS Web of Conferences* (Vol. 68, p. 01009). EDP Sciences.
15. Aftab, R. M., Ijaz, M., Rehman, F., Ashfaq, A., Sharif, H., Riaz, N., ... & Maqsood, H. (2022, December). A Systematic Review on the Motivations of Cyber-Criminals and Their Attacking Policies. In *2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS)* (pp. 1-6). IEEE.