Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts January-June 2026 7(1), 90-96

CRIMINAL JUSTICE SYSTEM POLICY ON CYBER CRIME: CAUSES AND PREVENTIVE MEASURES

Mahendra Kumar [1], Dr. Upendra Grewal [2]

[1] Research Scholar, School of Law, IFTM University, Moradabad, India
[2] Assistant Professor, School of Law, IFTM University, Moradabad, India

Received 24 March 2026
Accepted 23 April 2026
Published 27 May 2026

Corresponding Author
Mahendra Kumar,
mahendrakumar318@gmail.com

DOI
10.29121/shodhkosh.v7.i1.2026.8405

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

The emergence of cybercrime due to the development of computer technologies has become a significant issue in recent years. Cyber-crime mainly involves activities that use internet and computers as a tool to extract private information of an individual either directly or indirectly and disclosing it on online platforms without the person's consent or illegally with the aim of degrading the reputation or causing mental or physical harm. The recent shift in criminal activities includes organized crime, white-collar crime, and cybercrime. The increased use and access to digital space have influenced the prevalence of cyber-criminal behavior over time. Therefore, using electronic equipment to get access to prohibited or unlawful information is one sort of criminal cyber activity.

The research examines the evolving policies within the criminal justice system aimed at addressing cyber-crime, focusing on underlying causes such as anonymity, technological vulnerabilities, and socioeconomic factors, while proposing preventive measures like enhanced legislation, international cooperation, and public awareness campaigns. Drawing from recent developments, including the 2024 UN Cybercrime Convention and 2025 U.S. state cyber security legislation, the paper highlights gaps in current frameworks and recommends integrated strategies to mitigate risks. Additionally, it explores the inadequacies of existing laws and the necessity for legislative reforms to adapt to the digital age effectively.

Keywords: Cyber Crime, Criminal Justice System, Internet, Advancement of Technology, Legislative Framework Etc

1. INTRODUCTION

Cybercrime is a criminal act that utilizes computer technology and internet networks as its target. Cybercrime itself appears along with the incessant digital technology, information and communication that is growing. Cybercrime encompasses illegal activities conducted via digital means, such as hacking, identity theft, and ransom ware, posing significant challenges to the criminal justice system. With the proliferation of internet usage, incidents have surged, necessitating robust policies. Cybercrime encompasses any criminal act dealing with computers and networks. [1] It

includes crime conducted through the Internet. The Internet is basically the network of networks used across for communication and sharing of data.

It is evident that cyber criminals will stop at nothing to gain unauthorized access to confidential information. To effectively combat malware attacks, strict cyber laws are necessary, and the use of malware is punishable in many countries. Criminals have found ways to exploit technology to commit various crimes, including theft, fraud, and even terrorism. [2] Law enforcement agencies have been working tirelessly to combat this growing threat, but investigating cybercrime is not an easy task. [3] However, this digital transformation has also given rise to a parallel phenomenon – the escalating threat of cybercrime. As cyberspace becomes an increasingly fertile ground for criminal activities, the legal landscape grapples with multifaceted challenges, necessitating a meticulous review of contemporary issues within the criminal justice system. The challenges of digital forensics in criminal investigations are numerous and resolving these challenges requires a unique set of skills and tools. [4]

The cyber offender can infect or damage or steel data from the targeted computer system. Cybercriminals use various techniques, such as hacking, phishing, and malware, to steal personal information, financial data, and intellectual property. [5] Cybercriminals exploit vulnerabilities across borders, the criminal justice system encounters obstacles in attributing and prosecuting these offenses, underscoring the urgency for a harmonized, global approach. Cybercrime has had a significant impact on criminal investigations because traditional methods of collecting and analyzing evidence are no longer sufficient. [6]The advent of digital evidence, such as email records, social media posts, and digital documents, has created a new challenge for law enforcement agencies, prosecutors, and defense attorneys. [7]

Cybercrimes are crimes committed through Internet. They are just "a change in the modus operandi of conventional acts". [8] Computer crime involves any illegal activity carried out using a computer or networked device. This can include a variety of actions such as hacking, computer fraud, identity theft, cyber stalking, online harassment, and the spread of malicious software.

Some of the most common types of computer crime include:

1) **Hacking:** Gaining unauthorized access to computer systems, networks, or websites.
2) **Computer fraud:** The use of technology to deceive individuals or organizations for financial gain, including phishing scams, credit card fraud, and identity theft.
3) **Malware:** Malicious software used to harm or interfere with computer systems, networks, or devices.
4) **Cyberstalking:** Using technology to harass or threaten people, often via social media or other online platforms.
5) **Cyberbullying:** Using technology to harass, intimidate, or bully people, usually via social media or other online platforms.

There are five elements that characterize cybercrime that should be recalled. First is the change of the scena criminis, which becomes intangible; second, the emergence of completely new types of crime (i.e. phishing); [9] third, the impact on law enforcement procedures, requiring international co-operation between law enforcement agencies and a multi-stakeholder approach; [10] fourth, the decentralization of the control over digital networks, which has major consequences for the identification of the country, company or place where the evidence is transmitted or stored; fifth, the openness and interdependence of the Internet, which creates shared vulnerabilities affecting all people accessing a specific digital network. Computer crime is an increasing issue as more individuals and organizations depend on technology for their daily routines. To fight this type of crime, law enforcement and cyber security experts must collaborate to identify and prosecute offenders, while also putting proper security measures in place to prevent future breaches.

2. CAUSES OF CYBERCRIME

Hacking, identity theft, online fraud, cyber bullying, cyber terrorism, and other things are all considered forms of cybercrime. It is challenging to create a comprehensive definition that encompasses all of them because they each entail distinct approaches, motivations, and legal concerns. Cybercrime can have many different motivations, including as espionage, political action, financial gain, or just plain malevolence. These motivations may change over time and don't necessarily align with the conventional criminal goals.

2.1. SIMPLE ACCESS

The problem with protecting a computer system from unauthorized access is that due to the complexity of technology, there are numerous ways for a breach to occur. Hackers can steal access codes, retina images, advanced voice recorders, and other devices that can easily fool biometric systems and circumvent firewalls, allowing them to circumvent many security systems.

2.2. NEGLIGENCE

Because most people do not like to use strong passwords on their computers, it is easy to hack them.

2.3. TECHNOLOGICAL VULNERABILITIES

The internet's borderless and anonymous nature enables remote, hard-to-trace attacks. Emerging technologies like AI, IoT, crypto currency, and social media create new attack vectors (e.g., ransom ware, crypto jacking).

2.4. HUMAN FACTORS

Poor cyber security practices, such as weak passwords, unpatched software, or unsecured Wi-Fi, provide easy entry points. Social engineering (e.g., phishing) exploits trust in digital communications. Victims' reluctance to report incidents due to embarrassment or reputational concerns enables further crimes.

2.5. ORGANIZED CRIME AND ACCESSIBILITY

Organized groups use sophisticated, persistent techniques for large-scale attacks. "Crime-as-a-Service" platforms on the dark web lower barriers, enabling less-skilled individuals to commit cybercrimes.

2.6. GLOBALIZATION AND JURISDICTIONAL CHALLENGES

Cross-border operations complicate law enforcement due to differing legal systems. Dark web markets facilitate illegal trade, amplifying cybercrime's reach.

Cyber laws in India

There are certain laws, acts, and rules in India to prevent cybercrime. Such cyber laws are:

1) The IT Act of 2000
2) BNS, 2023
3) Information Technology (Certifying Authorities) Rules, 2000
4) Information Technology (Security Procedure) Rules, 2004
5) Information Technology (Certifying Authority) Regulations, 2001.

3. EMERGING TRENDS AND CHALLENGES IN CYBER CRIME

As technology continues to evolve, many new trends and a lot of challenges are emerging in this field of cybercrime. As well as, Cybercriminals are constantly evolving their strategies to harm and to exploit susceptibilities. They won't

leave any chance to take advantage of new technologies. Understanding these trends and emerging issues is critical to staying one step ahead of cyber threats.

3.1. CRYPTO CURRENCY RELATED CRIMES

The rise of crypto currencies like Bit coin has given rise to new forms of cybercrime. Criminals use the anonymity and privacy of crypto currencies for criminal activities, including money laundering, ransom ware payments, and illegal online transactions.

3.2. SOCIAL ENGINEERING TECHNIQUES

Cybercriminals are increasingly using social engineering techniques to manipulate people and gain authorized access to systems. Techniques such as sensitive texting, bitexting, and spear phishing are used to trick and trick people into disclosing sensitive information or taking security-related actions.

3.3. ARTIFICIAL INTELLIGENCE (AI)

The proliferation of AI devices presents new opportunities for cybercriminals. They can exploit susceptibilities in AI systems, such as using competitor attacks to manipulate AI algorithms or using deep AI-generated scams to commit fraud. Internet devices with weak security measures can be compromised, leading to massive botnet attacks or privacy breaches.

3.4. STATE-SPONSORED CYBER-ATTACKS

State-sponsored cyber-attacks pose a threat to national security and critical infrastructure. Governments engage in cyber espionage by intercepting or disrupting the communications of conflicting nations with the aim of stealing sensitive information, influencing public opinion, or disrupting procedure.

3.5. INSIDER THREATS AND INSIDER ATTACKS

Insider threats are still a challenge for cyber security. Insiders with access to systems can do harm, intentionally or unintentionally, by stealing data, disclosing sensitive information, or disrupting systems within an organization.

3.6. CYBERCRIME AS A SERVICE

Cybercriminals are increasingly acting as service providers, offering malevolent tools, botnets, or hacking services to rent or buy on the dark web. This leads to the participation of individuals with special skills in cybercriminal activities, resulting in an increase in the total number and intelligence of cyber-attacks.

3.7. ADVANCED PERSISTENT THREATS

Persistent threats are complex, persistent cyberattacks carried out by an organized group, often well-funded with government support. These attacks often target organizations such as governments, corporations, or critical systems for the purpose of unauthorized access, extraction of sensitive information, or to affect performance.

3.8. DATA BREACHES AND PRIVACY CONCERNS

Massive data breaches continue to emerge that put the personal information of millions of people at risk. Privacy concerns arise when cybercriminals exploit susceptibilities in data storage and transmission, raising questions about data protection and legal compliance.

3.9. EMERGING MALWARE

Cybercriminals are constantly developing new types of malware with advanced features and hijacking techniques. This includes in-memory file less malware, polymorphic malware that changes the code structure to avoid detection, and zero-day attacks targeting previously unknown susceptibilities.

3.10. CLOUD SECURITY CHALLENGES

As the widespread of cloud computing, the security of the cloud environment has become important. Incorrect cloud configuration, insecure APIs, and data breaches in cloud storage create serious problems for organizations as well as individuals.

4. CYBER CRIME PREVENTIVE MEASURES

Cybercrime is addressed by criminal justice systems across the world using a mix of preventative, enforcement, and legislative measures. In order to lessen vulnerabilities and stop threats before they become more serious, these policies place a strong emphasis on deterrence, risk mitigation, and capacity building. National laws, international treaties, and interagency collaborations are important frameworks that frequently draw from agencies such as the FBI, UNODC, INTERPOL, and the U.S. Department of Justice. To tackle problems like ransomware, hacking, and data breaches, preventive approaches emphasize technology protections, public awareness campaigns, legislative reforms, and international collaboration.

4.1. LEGAL AND REGULATORY COUNTERMEASURES

Enacting and revising laws to criminalize cyber activity often includes preventive measures aimed at minimizing data breaches. Key legislation like the African Union Convention on Cyber Security and Personal Data Protection and the EU General Data Protection Regulation mandates secure practices. The Computer Fraud and Abuse Act in the U.S. prohibit unauthorized access and deter further offenses. National strategies focus on aligning domestic laws with international standards, such as the Budapest Convention on Cybercrime, to facilitate cross-border collaboration. Additionally, preventive laws encourage mandatory incident reporting to enhance data collection and response, addressing issues of under-reporting.

4.2. CAPACITY BUILDING AND PUBLIC EDUCATION

Raising awareness and enhancing skill levels are key preventative measures in managing cyber investigations. National policies advocate for specialized training for criminal justice personnel, including police, prosecutors, and judges. Public education initiatives, such as Safer Internet Day, aim to promote cyber hygiene and reduce risks for vulnerable groups. In the U.S., the Justice Department enhances private-sector defenses through information sharing and public education on fraud and swatting. Policies also emphasize the development of forensic tools and guidelines for covert operations to mitigate investigation hazards.

4.3. CYBER SECURITY AWARENESS AND EDUCATION

There are initiatives that teach people how to spot phishing, create secure passwords, and report instances to sites such as IC3. Programmes organized for raising public awareness, education, and training assist people and organizations in adopting security procedures, understanding risk, and improving their capacity to recognize and address cyber threats.

4.4. STRONG AUTHENTICATION MECHANISMS

Strong authentication methods like biometrics and multi-factor authentication (MFA) provide an extra degree of protection to shield individuals and systems from unauthorized access. Robust authentication improves your overall security and lowers the chance of identity theft.

4.5. REGULAR SOFTWARE UPDATES AND PATCH MANAGEMENT

Adopting the most recent security patches and upgrades for software and systems will help minimize Frequent domain maintenance guarantees prompt resolution of vulnerabilities, which lowers the number of crooks stopped.

4.6. INTERNATIONAL COOPERATION

Assist multinational organizations in the fight against transnational cybercrimes. Engage in treaties and agreements aimed at preventing and prosecuting cybercrimes. Globally, exchange best practices and intelligence.

5. CONCLUSION

The fundamental principles of societies—human rights, democracy, and the rule of law—are seriously threatened by cybercrime, and this threat is only going to get worse every day. Cybercrime's dynamic environment poses a difficult and ever-evolving problem that calls for constant adaptation and preventative actions. Since cybercriminals are quick to take advantage of new vulnerabilities and sophisticated actions due to the rapid advancement of technology, it is crucial that people, organizations, and governments remain attentive and proactive in their cyber security efforts.

History has demonstrated that no strategy has ever been able to totally eradicate crime on a global scale. Laws should be more strictly enforced as they are the sole means of preventing crime, and people should be made aware of their rights and responsibilities, such as the significance of reporting crimes to the authorities as a duty to society. Act represents an important turning point in the development of cyberspace. Furthermore, I believe that changes to the Information Technology Act are necessary to better combat cybercrime. To sum up, I would want to caution those who support legislation: it's critical to keep in mind that the limitations of the cyber law shouldn't be so onerous as to impede the expansion of the sector and make it ineffective.

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Ahlberg, P., and Stedt, J. (2010). Digital Evidence in Criminal Cases: An Overview of Challenges and Opportunities. Computer Law and Security Review, 26, 105–106.

Arsawati, I., Darma, I., and Antari, P. (2021). A Criminological Outlook of Cyber Crimes in Sexual Violence Against Children in Indonesian Laws. International Journal of Criminology and Sociology, 10, 219–223. https://doi.org/10.6000/1929-4409.2021.10.26

Chatterjee, B. B. (n.d.). Last of the Rainmacs? Thinking About Pornography in Cyberspace. In D. S. Wall (Ed.), Crime and the Internet (74). Routledge.

Council of Europe. (2001). Convention on Cybercrime (ETS No. 185). Council of Europe.

Hayes, J., and Shenoi, S. (2010). Impact of Cybercrime on Digital Forensics: Threats, Challenges, and Future Directions. In Handbook of Digital Forensics and Investigation (1–4).

Holt, T. J., and Bossler, A. M. (2021). Cybercrime and Digital Criminology: An Introduction. Routledge.
Holt, T. J., and Holt, T. B. (2013). Examining the Social Organization and Structure of Digital of Fending in Hacking Groups. Deviant Behavior, 34(1), 67–69.
Munoz, J. K., and Sanders, R. H. (2022). Digital Forensics: The Challenges of Operating in a Digital Landscape. Digital Evidence and Electronic Signature Law Review, 12, 1–3.
United Nations Office on Drugs and Crime. (2013). Comprehensive Study on Cybercrime (Draft). UNODC.
Wall, W. E. (2021). Cybercrime: The Investigation, Prosecution and Defense of a Computer-Related Crime (2nd ed.).