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

CYBERCRIME: ISSUE AND THREATS

AUTHOR - SAQUIB ZUBAIR, STUDENT AT AMITY UNIVERSITY, LUCKNOW

BEST CITATION - SAQUIB ZUBAIR, CYBERCRIME: ISSUE AND THREATS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 5 (4) OF 2025, PG. 837-841, APIS – 3920 – 0001 & ISSN - 2583-2344.

Abstract

Cybercrime has emerged as a critical issue in the digital age, posing significant threats to individuals, corporations, and national security. This paper explores various types of cybercrime, including hacking, phishing, ransomware, and financial fraud, highlighting their evolution and impact. It also examines major cyber threats such as data breaches, cyber espionage, AI-driven attacks, and vulnerabilities within the Internet of Things (IoT). The paper discusses the far-reaching economic, psychological, corporate, and national security impacts of cybercrime. Current strategies to combat these crimes, including cybersecurity laws, technological advancements, and awareness initiatives, are evaluated. However, evolving threats, global coordination challenges, and a lack of awareness remain substantial obstacles. This paper emphasizes the necessity for proactive measures, international cooperation, and continuous technological innovation to effectively counter cybercrime. A forward-looking approach is vital as cyber threats continue to grow in sophistication and complexity.

Keywords: Cybercrime, Hacking, Phishing, Ransomware, Data Breaches, Cyber Espionage.

1. Introduction

In 2023, global cybercrime damages topped $8 trillion, highlighting the scale of digital hazards in today's connected world. Cybercrime—"the unlawful acquisition, alteration, or destruction of data or systems in cyberspace" (see figure)—is rising rapidly. The volume and sophistication of cyberattacks increase with technological dependence. Once limited to individuals, these crimes increasingly attack businesses, governments, and national security. Cybercrime exploits digital infrastructure weaknesses to cause rapid money losses, privacy invasions, and service outages[1392]. Organisations struggle to secure private data, countries worry about safety, and consumers are vulnerable to frauds and identity theft. No one is immune to these attacks because thieves continuously find new ways to exploit digital flaws[1393]. This study examines phishing, ransomware, identity theft, and hacking and its effects. Cybercrime methods and their consequences on the economy, psychology, and corporations will also be discussed. The paper will conclude that stopping these crimes is difficult and that stronger digital security is needed.

2. Types of Cybercrime

Hacking

In order to steal, alter, or damage data, hackers unlawfully access computer systems or networks. Curious individuals who wanted to play around with system security were the first hackers. It started off as a simple crime but has evolved into a complicated crime driven by politics, business, and violence[1394]. In order to take advantage of newly discovered software

[1392] Rani, S., Kataria, A., Sharma, V., Ghosh, S., Karar, V., Lee, K., & Choi, C. (2021). Threats and corrective measures for IoT security with observance of cybercrime: A survey. Wireless communications and mobile computing, 2021(1), 5579148.

[1393] Sharma, M., & Kaur, S. (2019). Cyber crimes becoming threat to cyber security. Academic Journal of Forensic Sciences ISSN, 2581, 4273.

[1394] Giri, S. (2019). Cyber crime, cyber threat, cyber security strategies and cyber law in Nepal. Pramana Research Journal, 9(3), 662-672.

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

vulnerabilities before they are patched, modern hackers employ distributed denial of service (DDoS) attacks, brute force attacks, and zero-day vulnerabilities. The world's digital infrastructures are under risk from these assaults, which can aim at individuals, companies, or even governments.

Phishing & Social Engineering

Phishing and social engineering try to get personal information from people. Most phishing efforts use emails, websites, or texts posing as respectable firms. Social engineering employs psychological tactics to encourage people to give money or expose sensitive information, unlike phishing. High-profile phishing attacks like the 2016 US presidential election email account hack demonstrate their widespread impact[1395]. Phishing remains a popular and successful cybercrime, even as people become more aware of it.

Ransomware & Malware

Ransomware and malware encrypt data and assault machines to steal money. Ransomware demands money to decrypt the victim's data. WannaCry, which infected hundreds of thousands of computers worldwide, including those in hospitals, wanted Bitcoin for the decryption keys in 2017. Malware includes a larger spectrum of programs that damage or harm systems, spy on users, or steal data[1396]. Malware and ransomware are used by hackers to take over computers and extort money from individuals, corporations, and governments.

Identity Theft

Cybercriminals steal personal information like Social Security numbers, bank account information, and credit card numbers to commit fraud. This can cost victims a lot of money and destroy their credit and reputation[1397]. Due to online storage and sharing of personal information, identity theft has expanded considerably. Data breaches, such as the massive Equifax breach in 2017, have exposed the personal details of millions of individuals, making identity theft one of the fastest-growing cybercrimes globally.

Financial Frauds & Scams

Online thieves often use schemes and frauds to steal money from people and companies who don't know what's going on. All of these crimes are different, from complicated investment plans to credit card fraud and fake e-commerce sites. Phishing and other forms of social engineering are common ways for thieves to get private financial information. Cybercriminals use private information to buy things without permission, empty victims' bank accounts, or trick them into investing in fake businesses or Ponzi scams[1398]. People and businesses alike need to put safety first because of the growing risk of financial fraud that comes with doing business online.

3. Major Cyber Threats

Data Breaches

As data breaches have increased dramatically over the last decade, some well publicised incidents have affected millions of people and businesses worldwide. Unauthorised access to personal, financial, medical, or proprietary company data causes a data breach. These breaches may cost money and reputation. Credit damage and fraud can result from lost or stolen financial and personal data. Businesses face steep fines, customer hesitancy, and lengthy repair after a data breach[1399]. Cyberattacks are devastating; the 2017 Equifax hack exposed 147 million consumer records.

[1395] Sumadinata, W. S. (2023). Cybercrime And Global Security Threats: A Challenge In International Law. Russian Law Journal, 11(3), 438-444.
[1396] Atta Ul Haq, Q. (2021). Cyber crime and their restriction through laws and techniques for protecting security issues and privacy threats. Securiaty Issues and Privacy Threats in Smart Ubiquitous Computing, 31-63.
[1397] Tok, Y. C., & Chattopadhyay, S. (2023). Identifying threats, cybercrime and digital forensic opportunities in Smart City Infrastructure via threat modeling. Forensic Science International: Digital Investigation, 45, 301540.
[1398] Andini, N. K. T., Damayanti, N. M. A. N. P., Sari, N. K. W. P., Fkun, E., & Erkamim, M. (2023). Cybercrime and Threats to the Electoral System. Journal of Digital Law and Policy, 3(1), 26-37.
[1399] Rao, S., Verma, A. K., & Bhatia, T. (2021). Evolving cyber threats, combating techniques, and open issues in online social networks. In Handbook of research on cyber crime and information privacy (pp. 219-235). IGI Global.

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

Cyber Espionage

Some governments or businesses use digital technologies to spy on or steal sensitive information from other groups in order to get a political, military, or economic edge. This is called cyber espionage. Hackers can get to a lot of data from afar, which makes cyber spying quick and secret. Cyberattacks paid for by governments are on the rise as countries try to learn more about their rivals or damage important infrastructure. It is said that Russian hackers tried to change the outcome of the 2016 US election[1400]. In 2014, North Korean hackers may have gone after Sony Pictures to get back at them for a highly charged movie. These cases show how cyber espionage can affect countries around the world and make political conflicts worse.

AI-Driven Attacks

Artificial intelligence (AI) is rapidly transforming the landscape of cyber threats, enabling cybercriminals to conduct more sophisticated and effective attacks. AI can be used to automate attacks, identify vulnerabilities faster, and even create more convincing phishing scams or malware that adapts in real-time. For instance, AI-driven malware can evade traditional security defenses by learning how these systems operate and adjusting its behavior to avoid detection. AI also facilitates large-scale attacks, allowing criminals to carry out highly targeted operations with minimal human intervention[1401]. Looking ahead, the potential for AI to be weaponized in cyber warfare is a growing concern, as it could lead to highly autonomous and devastating cyberattacks that are difficult to anticipate or counter.

IoT Vulnerabilities:

The growth of IoT devices has created new security vulnerabilities. Industrial sensors, smart home systems, and wearable health monitoring are examples. Due to their weak security, cybercriminals attack networked devices. Many IoT devices have outdated software and inadequate encryption, making them ideal targets for hackers who can access wider networks. In 2016, the Mirai botnet attack took down Twitter and Netflix by hijacking thousands of IoT devices like routers and cameras to conduct a huge DDoS attack. The development of Internet of Things (IoT) devices makes it crucial to prepare for large-scale attacks that could damage infrastructure and threaten people.

4. Impact of Cybercrime

Economic Impact

Cybercrime has done a lot of damage to the world economy. By 2025, costs are expected to be more than $10.5 trillion per year. In this amount, both the direct and indirect costs of cyberattacks are included. These include fines, legal fees, ransoms, and things like missed productivity and problems with business operations. Some well-known companies that have lost a lot of money because of data hacks are Target, Marriott, and Equifax. Think about the hundreds of millions of dollars that Equifax had to pay out in settlements, fees, and recovery costs after the breach[1402]. This shows how much damage cyberattacks can do to profits. Hackers are mainly going after banks and other financial institutions, which is causing the world's financial system a lot of problems and big losses. The finance business is especially at risk.

Psychological Impact

People who are victims of cybercrime may go through a lot of mental and physical pain. People who have been abused online, scammed, or had their identities stolen often

[1400] Dumchykov, M., Utkina, M., & Bondarenko, O. (2022). Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis. International Journal of Safety and Security Engineering, 12(4), 481-490.

[1401] Cascavilla, G., Tamburri, D. A., & Van Den Heuvel, W. J. (2021). Cybercrime threat intelligence: A systematic multi-vocal literature review. Computers & Security, 105, 102258.

[1402] Baranovska, T., Savitskyi, V., Serbov, M., Stoliar, Y., & Krutik, Y. (2024). The Impact of Cybercrime on State and Institutional Security: Analysis of Threats and Potential Protection Measures. Economic Affairs, 69, 33-42.

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

feel deeply violated, unsure, and helpless. People whose identities have been stolen may feel anxious, stressed, or scared as they try to fix their financial and emotional problems[1403]. A lot of mental pain can happen when people lose their life savings in fraud or financial scams like phishing. Because of the stress of these events, victims may always feel like their privacy and safety are at risk. This can have long-lasting psychological effects like sadness and a stronger sense of being vulnerable.

Corporate Impact:

Cybercrime undermines consumer confidence and brand image, threatening organisations' long-term viability in addition to short-term financial losses. Data breaches and ransomware attacks erode customer trust in a company's data security. If reputation harm is severe, customers may leave and companies may face years of litigation[1404]. Cyberattack recovery increases a company's financial burden. New security measures, legal fees, and customer compensation programs are costly. Example: Target. The 2013 data breach cost the company about $200 million in legal bills, settlements, and infrastructure improvements. Additionally, shoppers lost trust in the brand's security, lowering revenues.

National Security:

World governments worry more about cybercrime, cyberwarfare, and cyberespionage. Nation-states try to compromise key infrastructure like power grids, financial systems, healthcare facilities, and communication networks to disable or interrupt vital services. The 2020 SolarWinds breach, carried out by Russian hackers, exposed sensitive national security information and demonstrated the dangers of cyber espionage by compromising several US business and government entities[1405]. Ukraine's 2015 infrastructure attacks interrupted electricity to hundreds of thousands, highlighting cyberwarfare's growing threat. These events demonstrate the need for strong cybersecurity to protect national interests and maintain global stability.

6. Challenges in Combating Cybercrime

Evolving Threats

Cybercriminals are always changing and adapting their methods, which makes it harder for law enforcement and cybersecurity experts to stay ahead. Cybercriminals are always coming up with new ways to take advantage of weaknesses in technology. Cybercrime is no longer just hacking efforts. It includes high-tech malware and ransomware as well as attacks powered by AI. Security experts are facing problems that have never been seen before because of how quickly new attack routes are appearing, like deepfakes, IoT flaws, and the use of quantum computing to break encryption. Because these dangers are always changing, even the best security measures can become useless very quickly. This means that cybersecurity practices need to keep getting better. Unfortunately, cybercrime is always changing, which makes it harder to come up with long-term answers.

Global Coordination

Because cybercrime happens all over the world, it is very hard to bring cybercriminals to justice across countries. Unfortunately, it is often hard to enforce laws or catch hackers whose home countries are different from those of their victims. Different legal systems, conflicting cybersecurity rules, and problems with jurisdiction make it hard to successfully pursue hackers on a global scale[1406]. Criminals online may also find safe places to work in countries that don't want to pursue cybercrime or don't

[1403] Cristea, L. M. (2020). Current security threats in the national and international context. Journal of accounting and management information systems, 19(2), 351-378.
[1404] Tanwar, S., Paul, T., Singh, K., Joshi, M., & Rana, A. (2020, June). Classification and imapct of cyber threats in India: a review. In 2020 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO) (pp. 129-135). IEEE.
[1405] Furnell, S., & Dowling, S. (2019). Cyber crime: a portrait of the landscape. Journal of Criminological Research, Policy and Practice, 5(1), 13-26.
[1406] Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. Journal of International Studies (2071-8330), 17(2).

have the money to do so. These issues show how important it is to fight cybercrime more systematically, which calls for more international cooperation, such as deals between nations. Because cyber threats are global, it is important to arrange treaties that cover multiple borders, make it easier for people to share information, and set up joint cyber defence measures.

Lack of Awareness:

Cybercrime is rising, yet many people and corporations don't grasp the risks or don't prioritise threats. Lack of understanding makes them more vulnerable to ransomware, phishing, and identity theft. Due to the belief that they are immune to cyberattacks, many SMEs underfund cybersecurity. Unfortunately, ignorance creates key vulnerabilities attackers exploit. People who don't know how to use secure passwords, two-factor authentication, and avoid phishing are more vulnerable to crooks. Education and understanding of cybercrime hazards reduce vulnerabilities and improve cybersecurity resilience.

7. Conclusion

In conclusion, cybercrime continues to threaten individuals, businesses, and nations worldwide. Cybercrime is huge and changing, from hacking and phishing to AI-driven attacks and cyber espionage. These crimes involve massive economic costs, psychological harm, company reputation damage, and national security risks. Governments, organisations, and individuals must be proactive to address these issues. Cyber dangers evolve quickly, therefore cybersecurity legislation, technology, and education and awareness must evolve too. Preventative tactics and international cooperation will help combat cybercrime globally. The threat landscape will evolve as cybercriminals adopt more advanced and targeted approaches. To keep ahead of cybercrime, we must be vigilant and adaptable in our defence against these digital dangers. The future of cybersecurity is a safer digital world through collaboration.