International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 10 Issue 1, Jan-Feb 2026 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Internet Crime: An Overview

Paul A. Adekunte[1], Matthew N. O. Sadiku[2], Janet O. Sadiku[3]

[1]International Institute of Professional Security, Lagos, Nigeria
[2]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[3]Juliana King University, Houston, TX, USA

ABSTRACT

Internet crime, commonly known as cybercrime, refers to a spectrum of illegal acts committed through the use of computers, networks, and Internet technologies. Most of these activities range from unauthorized access and data theft to financial fraud, identity theft, cyberstalking, and system disruption. Just as digital connectivity is expanding globally, so is the scale and sophistication of cybercrime, challenging traditional legal, technical, and social frameworks. Some of the characteristics that distinguish cybercrime include its transnational nature, anonymity of perpetrators, and rapid evolution alongside technological innovation. Cybercrime does not only result in substantial economic losses for individuals, businesses/organizations, and governments but raises critical questions and concerns about privacy, security, and legal accountability. Addressing cybercrime therefore will require multidisciplinary strategies, that must include robust legal frameworks, international cooperation, advanced cybersecurity practices, and public awareness initiatives. This paper looks at the pervasive impact of cybercrime, how to combat it, strengthening national and international cooperation among countries, legal, and policy development in the digital age.

KEYWORDS: *Cybercrime, advanced cybersecurity practices, public awareness initiatives, internet technologies, cyberstalking, identity theft, technological innovation, legal frameworks, international cooperation, cyberwarfare, espionage, malware, ransomware.*

How to cite this paper: Paul A. Adekunte | Matthew N. O. Sadiku | Janet O. Sadiku "Internet Crime: An Overview" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-10 | Issue-1, February 2026, pp.996-1002, URL: www.ijtsrd.com/papers/ijtsrd100160.pdf

IJTSRD100160

INTRODUCTION

In today's highly interconnected digital world, cybercrime has emerged as one of the most significant and rapidly evolving threats to individuals, organizations, and national security. Cybercrime is said to refer to illegal acts that involve the use of computers, networks, or internet technologies to commit crimes or facilitate unlawful activities, including fraud, identity theft, intellectual property violations, and violations of privacy – underscoring its wide scope and dynamic nature, as shown in Figure 1. Cybercrime also involves the unauthorized access, use, disclosure, disruption, modification, or destruction of computer systems, networks, or data. Common types of cybercrime include hacking, phishing, identity theft, and ransomware attacks, as shown in Figures 2, 3 and 4. At its core, cybercrime exploits digital technologies to achieve objectives such as financial gain, privacy invasion, data theft, system disruption, or harassment. The pervasive adoption of the internet and digital services has made cybercrime a ubiquitous challenge, which transcends geographical boundaries and complicating efforts to detect, prevent, and prosecute offenders.

Some of the key characteristics of cybercrime include:

- It often involves the use of computers and networked systems as both tools and targets of criminal behavior.
- It has a high degree of anonymity.
- It frequently operates across national and jurisdictional boundaries, making enforcement particularly challenging.

Cybercrime as discovered by researchers encompasses a diverse set of behaviors, ranging from

technical attacks on systems to traditional criminal acts that are facilitated by digital means. The impact of cybercrime is profound and far-reaching as this results in significant economic/financial losses, undermines privacy and trust, disrupts critical infrastructure, and could pose as threats to national security. This has led to international initiatives and treaties aimed at enhancing cooperation and legal frameworks to combat cybercrime globally, such as the United Nations Convention against cybercrime (also known as the Hanoi Convention) signed in 2025. As technology evolves, so too do the tactics and sophistication of cybercriminals, hence necessitating the constant advancements in cybersecurity practices and legal frameworks designed to mitigate these threats.

The global nature of technology means that state and non-state actors can engage in cybercrimes which may include espionage, and financial theft, and offenses that cross international borders may be referred to as cyberwarfare [1-8], as shown in Figure 5.

HISTORY

Cybercrime evolved from early 1960s password theft to sophisticated modern attacks, with notable milestones including the 1971 Creeper virus, 1980s hacking of defense systems, and the 1999 Melissa worm, which encompasses profit-driven scams, state sponsored espionage, and ransomware, with significant high-profile breaches rising sharply in the 2000s. The key phases and incidents in history of cybercrime are:

- 1960s-1970s: Early Origins: Early computer crimes, like phone phreaking and unauthorized access emerged. The first cyberattack is often cited as Allen Scherr's 1962 theft of password data at MIT via punch cards. The first computer virus, "Creeper," was detected on ARPANET in 1971.
- 1980s: Hacking and "Phreaking": Ian Murphy ("Captain Zap") was convicted in 1981 for hacking AT&T, while the "414s" group of teenagers was prosecuted in 1984 for breaching high-profile systems. First computer virus (Elk Cloner, 1982) and hacking groups formed.
- 1990s: Rise of the Internet: Malware proliferated, exemplified by the Melissa worm in 1999. Cybercrime grew with the internet's expansion; hacking and malware became more sophisticated.
- 2000s: DDoS and Organized Crime: MafiaBoy launched massive DDoS attacks against major sites like CNN and Yahoo! in 2000 (Yahoo! Data Breach 2013-2014: 3 billion accounts were compromised). This era saw the rise of botnets and massive data breaches. Phishing, identity theft, and ransomware attacks increased.
- 2010s-Present: Advanced Persistent Threats (APTs): High-profile breaches included the 2014 Sony Pictures hack and increased state-sponsored activity/hacking, and cryptocurrency-related crimes rose. Ransomware became a major threat, with 82% of Indian companies experiencing attacks in 2020. Worthy of note is the WannaCry 2017 global ransomware attack.
- Legal Response: The UN adopted resolutions against computer crime in 1990, 2000, and 2002. Key figures like Kelvin Mitnick got a 68-month sentence in 1999, and while Albert Gonzalez received a 20-year sentence [9-12].

Some Key Milestones are [13-15]:

- 1986: US Computer Fraud and Abuse Act
- 1990: First international hacking competition
- 2000: "I Love You" virus (global malware attack)
- 2017: WannaCry ransomware attack (global attack)

INDIRECT BENEFITS OF CYBERCIME

Even though as cybercrime is illegal and harmful, its prevalence has forced rapid advancements in technology and digital safety. Some of its key indirect benefits include [16, 17]:

- Accelerated development of robust cybersecurity measures via accelerated development of encryption, AI-driven threat detection, and more secure network protocols.
- Creation of specialized jobs (Job Market Growth) which has resulted in creating a high demand for cybersecurity professionals, ethical hackers, and forensic investigators
- Increased public awareness of data protection by individuals and organizations to adopt better digital hygiene such as multi-factor authentication (MFA) and regular security updates.
- Strengthening of digital infrastructures – the threat encourages governments and businesses to improve, patch, and harden critical infrastructure against future attacks.
- Better Legal Frameworks: Cybercrime has forced the development of specialized laws (e.g., GDPR) to protect data and privacy.
- Ethical Hacking Advancement: The need to defend against criminals has spurred the growth of the cybersecurity industry, helping to identify vulnerabilities before they are exploited.

All of these are indirect benefits arising from the fight against cybercrime, the actions themselves cause significant damage, financial loss, and privacy breaches. The followings are the types of cybersecurity:

- Network security
- Application security
- Cloud security
- Information security
- Endpoint security
- Mobile security
- Identity and access management
- Internet of Things (IoT) security
- Data security
- Operational security

CHALLENGES TO CYBERCRIME

Combating cybercrime faces some key challenges – that is, the major difficulties law-enforcement agencies, governments, courts, organizations, and societies encounter when trying to prevent, investigate, prosecute, and mitigate cybercrime. Some of which are:

1. **Jurisdictional & Legal Framework Challenges**: Cyber frequently crosses national borders, but legal frameworks and enforcement vary widely between countries:

- Jurisdictional conflict: Cyberattacks may originate in one country, target another, and use servers in a third, making it hard to determine which nation's law apply [18, 19].
- Inconsistent or outdated cyber laws: Many jurisdictions lack modern cybercrime legislation or have differing definitions of what constitutes a cybercrime, creating loopholes criminals exploit [20].
- Extradition and international cooperation hurdles: Varying legal standards, domestic procedures, and political issues can delay or block effective cross-border investigations [21].

The resulting impact is that these challenges slow prosecution, frustrate law enforcement coordination, and often result in cybercriminals avoiding justice by exploiting legal gaps, as shown in Figures 6 and 7.

2. **Limited Resources & Technical Capacity**: Effective cybercrime response demands specialized skills, tools, and infrastructure:

- Shortage of skilled personnel: There is a global deficit of trained cybersecurity experts and digital forensic investigators, especially in developing countries [18].
- Underfunded enforcement agencies: Many police units lack modern tools, advanced forensic labs, and budget allocations to keep pace with sophisticated cyber threats [19].
- Inadequate cybersecurity infrastructure: Organizations and governments often do not invest enough in detection, monitoring, and defensive systems [22].

The impact is such that resource constraints hinder detection, evidence collection, timely investigation, and prosecution of cyber offenses.

3. **Technological Complexity & Anonymity**: Advances in technology create new attack vectors while enabling criminals to hide their identity:

- Encryption and anonymity tools: Technologies like VPNs, TOR, and strong end-to-end encryption protect privacy but also shield cybercriminals from identification [23].
- Rapid evolution of cyber threats: The pace of innovation (e.g., IoT, cloud services, AI-driven tools) often outstrips law enforcement capabilities and regulatory responses [22].
- Dark web and obfuscation tactics: Criminals make use of hidden networks and sophisticated techniques to conceal activities, making it difficult to trace operations [19].
- Cybercriminals use advanced tactics like encryption, anonymity tools, AI evasion, and zero-day exploits, making detection and response difficult.

The above factors complicate attribution, slow investigations, and enable criminal to adapt faster than prosecutors or security systems.

4. **Digital Evidence Challenges**: Collecting, preserving, and presenting digital evidence poses unique legal and technical hurdles:

- Volatile nature of digital data: Digital evidence can be easily altered or destroyed, hence requiring precise forensic procedures [24].
- Chain of custody and admissibility issues: Courts may reject digital evidence if proper forensic standards are not followed [25].
- Lack of standardization: There is often no unified procedure for handling digital evidence across jurisdictions, creating legal uncertainties [24].

All of these issues make convictions harder to secure and can result in lengthy trials or dismissed cases.

5. **Underreporting & Public Awareness Shortfalls**: Cybercrime is often underreported, and many victims lack the knowledge to recognize or act on cyber threats:

- Low reporting rates: Victims may fear reputational harm, distrust authorities, or simply be unaware of reporting mechanisms, making it hard for law enforcement to assess the threat landscape [22].

- Lack of cybersecurity literacy: Many individuals and some organizations are still unaware of basic cyber risks and safety measures, hence increasing vulnerability [22].

The impact leads to gaps in data on cybercrime prevalence, hindering effective policy or response strategies.

6. **Coordination & Institutional Fragmentation**: Effective anti-cybercrime efforts require synchronized action across sectors and agencies:
- Fragmented institutional responses: Multiple agencies with overlapping mandates can duplicate effort or work in silos, reducing overall effectiveness [26].
- Weak public-private collaboration: Cybercrime investigations often require cooperation with private sector firms, but standardized protocols and mechanisms are often lacking [27].

The impact leads to coordination gaps slowing investigations, impede intelligence sharing, and weaken deterrence. Need for well organized and funded organizations/institutions like the Federal Bureau of Investigation (FBI) to investigate cybercrime, terrorism, violent crimes involving gangs, crimes against children etc., as shown in Figure 8.

7. **Ethical and Human Rights Considerations**: Balancing cybercrime enforcement with privacy and civil liberties is challenging:
- Privacy vs. surveillance: Strong privacy protections can limit law enforcement access to critical data, while invasive surveillance poses risks to civil rights [23].
- Global human rights norms: Some proposed international arrangements aimed at strengthening cybercrime enforcement (e.g., international conventions) have been criticized for potential misuse or overreach [28].

These concerns complicate legislation, enforcement policies, and international cooperation.

SOLUTIONS TO CHALLENGES FACED BY CYBERCRIME

Cybercrime is tough because it evolves very fast, crosses borders, and exploits both technology and human behavior. There is no single fix, but a combination of technical, legal, organizational, and social solutions works best. Some of the solutions to the challenges are as outlined below [15, 29-37]:

1. Rapidly evolving cyber threats

Challenge: Attackers constantly adapt using new malware, ransomware, AI-driven phishing, and zero-day exploits.

Solutions would include:
- Use AI- and machine-learning-based security systems to detect abnormal behavior in real time.
- Continuous patch management and system updates.
- Threat intelligence sharing between organizations and governments.

2. Lack of cybersecurity awareness

Challenge: Human error (weak passwords, phishing clicks, social engineering) is one of the biggest causes of cyber incidents.

Solutions to this are:
- Regular cybersecurity awareness training.
- Simulated phishing exercises.
- Strong password policies and multi-factor authentication (MFA).

3. Weak legal and regulatory frameworks

Challenge: Cybercrime most often crosses national borders, making enforcement difficult,

Solutions involve:
- International cooperation through treaties (e.g., Budapest Convention on Cybercrime).
- Harmonization of cyber laws across countries.
- Strengthening digital forensics and cyber law enforcement units.

4. Inadequate security infrastructure

Challenge: Many organizations, especially SMEs, lack resources to implement robust cybersecurity.

Solutions would include:
- Adoption of cloud-based security services.
- Government incentives and cybersecurity grants
- Implementation of baseline frameworks like ISO/IEC 27001 or NIST Cybersecurity Framework.

5. Data privacy and identity theft

Challenge: Cybercriminals steal personal and financial data for fraud and identity theft.

Solutions:
- Strong data encryption (at rest and in transit).
- Privacy-by-design principles.
- Compliance with data protection regulations (e.g., GDPR).

6. Shortage of skilled cybersecurity professionals

Challenge: The global demand for cybersecurity experts far exceeds supply.

Solutions:
- Investment in cybersecurity education and certification programs,
- Public-private partnerships.
- Automation of routine security tasks using AI.

7. Poor incidence response and recovery

Challenge: Many organizations are unprepared to respond quickly to cyberattacks.

Solutions:

- Develop and regularly test incident response plans.
- Maintain secure and tested data backups.
- Use cyber insurance to mitigate financial losses.

CONCLUSION

Cybercrime has become one of the most significant challenges of the digital age, affecting individuals, organizations/businesses, and governments globally. As technology continues to advance, so are cybercriminals are becoming more sophisticated, exploiting vulnerabilities in systems, networks, and human behavior. The consequences – financial losses, data breaches, identity theft, and threats to national security – highlight that cybercrime is not just a technical issue, but a social, economic, and legal one. Combating it will therefore require a collective effort that includes stronger cybersecurity measures, effective legislation, international cooperation, and increased public awareness. Ultimately, reducing cybercrime depends not solely on technology, but on responsible digital behavior and continuous adaptation to merging threats. More information on Cybercrime can be obtained in books in [38-45] and the following related journals:

International Journal of Cybersecurity Intelligence & Cybercrime (IJCIC)

International Journal of Cyberlaw and Cybercrime (IJCLCC)

International Journal of Information Security and Cybercrime (IJISC)

Global Journal of Information security and Cyber Criminology

IJRDO Journal of Law and Cyber Crime

IEEE Security & Privacy

IET Information Security

Commonwealth Cyber Journal

REFERENCES

[1] M. A. Dennis (ed.) (December 31, 2025), "Cybercrime," https://www.britannica.com/topic/cybercrime

[2] New world Encyclopedia, "Cybercrime," https://www.newworldencyclopedia.org/entry/Cybercrime

[3] UNDOC, "Cybercrime Module 1 Key Issues: Cybercrime in Brief," https://www.undoc.org/e4/en/cybercrime/module-1/key-issues

[4] ITU, "Understanding cybercrime: Phenomena, challenge and legal response."

[5] "Cybercrime," Wikipedia, the free encyclopedia, https://en.wikipedia.org/cybercrime

[6] Cybersecurity Ventures: "Cybercrime Report 2020."

[7] FBI Internet Crime Complaint Center (IC3)

[8] Interpol: Cybercrime.

[9] Artic Wolf (April 19, 2024), "A brief history of cybercrime," https://www.articwolf.com

[10] K. Chadd (November 30, 2020), "The history of cybercrime and cybersecurity, 1940-2020," Cybercrime Magazine, https://www.cybersecurityventures.com

[11] "International cybercrime," Wikipedia, the free encyclopedia, https://en.wikipedia.org

[12] BlueVoyant, "Cybercrime: History, global impact & protective measures [2025]," https://www.bluevoyant.com

[13] B. Landreth, "The Cracker."

[14] K. Poulsen, "Kingpin."

[15] Verizon Data Breach Investigations Report, "FBI IC3 Reports."

[16] "Cyber crime: Advantages, disadvantages, merits, and demerits," https://askfilo.com

[17] T. W. Renish (May 09, 2025), "Top 20 advantages and disadvantages of cybersecurity," https://webandcrafts.com

[18] The Law Institute (December 3, 2025), "Preventive strategies against cybercrimes: A multi-faceted approach – Law Notes by TheLaw.Institute," https://www.thelaw.institute/regulation-of-cyberspace/preventive-strategies-against-cybercrimes-multi-faceted-approach

[19] This Nation (July 11, 2024), "Cybercrime trends and its challenges to modern law enforcement," https://www.thisnation.com/politics/world/cybercrime-trends-and-its-challenges-to-modern-law-enforcement

[20] Cyber and Technology Law, "What are the challenges in cyber law enforcement? L Law4u" https://www.law4u.in/top-

answer/15513/what-are-the-challenges-in-cyber-law-enforcement

[21] Md. R. Islam et al. (October 2024), "Legal and ethical challenges in combating international cybercrime," International Journal of Progressive Research in Science and Engineering, vol. 5, no. 10, pp. 15-24.

[22] "Cybercrime – Meaning, types, challenges, solutions – Inclusive IAS," https://www.inclusiveias.com/cybercrime-meaning-types-challenges-solutions

[23] "Legal challenges in cybercrime investigations impeding justice and enforcement – LexJuris Vista," https://www.lexjurisvista.com/legal-challenges-in-cybercrime-investigations-impeding-justice-and-enforcement

[24] "Cybercrime and the law: Addressing the challenges of digital forensics in criminal investigations l Mexican Law Review," https://www.ijpc245.juridicas.unam.mx/index.php/mexican-law-review

[25] "Legal challenges in combatting cybercrime in Nigeria: regulations versus enforcement – Record Of Law," https://www.recordoflaw.in/legal-challenges-in-combatting-cybercrime-in-nigeria-regulations-versus-enforcement

[26] D. Young (December 15, 2025), "Nigeria's fight against cybercrime: Institutional challenges and the path to unified response," https://www.linkedin.com/pulse/nigeria's-fight-against-cyberrcrime-institutional-path-

[27] "Setting the scene on cybercrime: Trends and new challenges l Eurojust l European Union Agency for Criminal Justice Cooperation," https://www.eurojust.eu/news/setting-scene-cybercrime-trends-and-new-challenges

[28] "United Nations Convention against Cybercrime," Wikipedia, the free encyclopedia, https://en.wikipedia.org/wiki/United_Nations_Convention_against_Cybercrime

[29] R. Anderson et al. (2019), *Measuring the cost of cybercrime*, Journal of Cybersecurity, vol. 5, no. 1.

[30] Europol (2023), *Internet Organized Crime Threat Assessment (IOCTA).*

[31] National Institute of Standards and Technology (NIST) (2018), *Framework for Improving Critical Infrastructure Cybersecurity.*

[32] United Nations Office on Drugs and Crime (UNODC) (2021), *Comprehensive Study on Cybercrime*.

[33] ISO/IEC (2022), *ISO/IEC 27001: Information Security Management Systems*.

[34] Gartner, "Top security and risk trends 2022."

[35] FBI IC3, "2020 Internet Crime Report."

[36] Cybersecurity and Infrastructure Security Agency, "Cybersecurity Awareness Training."

[37] NIST, "Multi-Factor Authentication."

[38] T. J. Holt & A M. Bossler (eds.) (2019), "The Palgrave Handbook of international Cybercrime and Cyberdeviance," Springer.

[39] B. H. Schell & C. Martin, "Cybercrime: A reference handbook: Contemporary World Issues," Bloomsbury Publishing.

[40] N. E. Marion & J. Twede, "Cybercrime: An encyclopedia of digital crime," Apple Books.

[41] M. Yar & K. Steinmetz (4th edition), "Cybercrime and society," SAGE India.

[42] J. Bandler & A. Merzon, "Cybercrime investigations: A comprehensive resource for everyone."

[43] P. Stephenson & K. Gilbert, "Investigating computer-related crime," 2nd Edition.

[44] Akhgar & Brewster, "Combatting cybercrime and cyberterrorism: Challenges, trends and priorities," Springer Nature Link.

[45] Y. Jewkes & M. Yar, "Handbook of internet crime," Apple Books.

Figure 1. Cybercrime
Source: https://en.wikipedia.org/wiki/Cybercrime

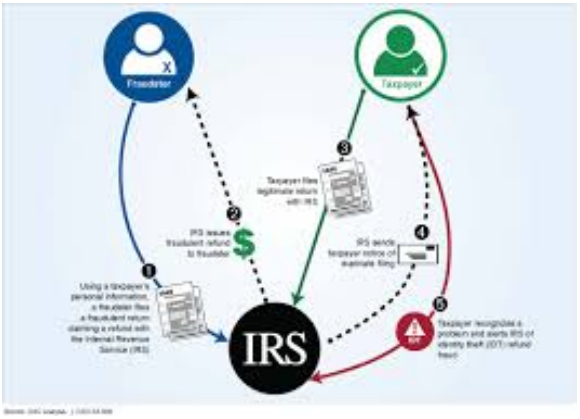

Figure 2. Identity theft
Source: https://en.wikipedia.org/wiki/Identity_theft

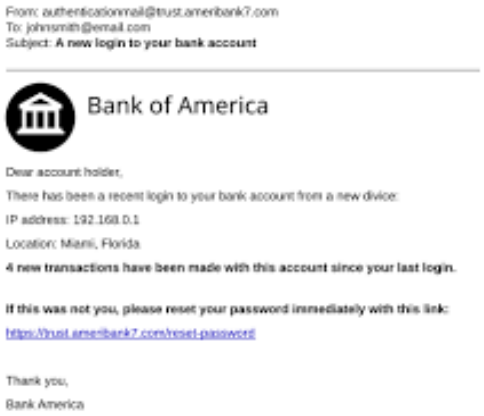

Figure 3. Phishing
Source: https://en.wikipedia.org/wiki/Phishing

Figure 4. Hacker
Source: https://en.wikipedia.org/wiki/Hacker

Figure 5. Cyberwarfare
Source: https://en.wikipedia.org/wiki/Cyberwarfare

Figure 6. International cybercrime
Source:
https://en.wikipedia.org/wiki/International_cybercrime

Figure 7. List of cybercriminals
Source:
https://en.wikipedia.org/wiki/List_of_cybercriminals

Figure 8. Federal Bureau of Investigation
Source:
https://en.wikipedia.org/wiki/Federal_Bureau_of_Investigation