International Journal of Innovations & Research Analysis (IJIRA)
(An International Quarterly Multidisciplinary Peer Reviewed Refereed Journal)
e-ISSN :2583-0295, Impact Factor: (Cosmos 7.662 & I2OR 5.105), Volume 06, No. 02(I), April- June, 2026, pp 01-06

Recent and Emerging Trends in Cyber Crime

Dr. Omkar Sonawane*

Assistant Professor, Department of Defence and Strategic Studies, Savitribai Phule Pune University.

*Corresponding Author: dromkarphd@gmail.com

Citation: Sonawane, O. (2026). Recent and Emerging Trends in Cyber Crime. International Journal of Innovations & Research Analysis, 06(02(I)), 01–06.

ABSTRACT

The global landscape of cybercrime is rapidly evolving as cyber offenders continue to deploy sophisticated cyber technologies to scale their operations. Technically sophisticated criminal environments will develop fast. Despite India's rapid digitalization and improvement in its digital services accessibility, it has opened new avenues for cybercrime. Cybercriminals are now impersonating law enforcement and government officials with interactive scams such as Digital Arrest. Individuals and society are being defrauded by these new security challenges in cyberspace. Based on the precedence of such digital crimes, the article discusses how globalization, technology and society are embracing such challenges, while discussing new trends and future developments in the spectrum of digital landscape. This research is intended to promote deep understanding amongst intellectuals, public officials, financial institutions and law enforcement by providing a clear outlook on emerging trends in cybercrime. Criminal activities are constantly evolving and it is essential to be aware of its new patterns. Globalization and technological changes are driving these factors, which pose a serious threat to economic stability, public safety and national security. The article also highlights how technology allows criminals to maintain high level of anonymity and conduct illicit activities across the globe. It showcases how the development of society and technology have made these intersections for such crimes to take effect.

***Keywords**: Cyber Security, Cyber Crime, National Security, Data Privacy.*

Introduction

With the advent of computer technology, the internet is at the crossroads of radical changes that have impacted on how we connect and experience the world around us. Technological advancements also bring in increased vulnerability to cyberspace. The globalization of digital trade has been enabled by a new generation of cybercriminals who abuse vulnerabilities found in digital space for fraudulent monetary transactions and defraud individuals through innovative deceptive techniques. Therefore, mitigating the threat of cybercrime is a required necessity for individuals, society, businesses and nations. Today, cybercrime carries far-reaching effects that not only covers online crimes but also focus upon the technology used in such digital environments to commit financial fraud, deepfakes, malvertising, disinformation and espionage.

As cybercrime continues to advance, it poses serious risk to online safety, law enforcement and cyber jurisdictions. An urgent adaptive legal framework along with digital guidelines is imperative to address such security challenges. As technology advances, so do the methods employed by cybercriminals. This necessitates the need for effective vigilance in cyber space. Cybercrime today has become a worldwide problem that needs to be tackled by all means necessary. Today no nation is immune to cybercrime, neither can it protect its cyberspace by its own in isolation. Cyber-attacks today

are no longer confined to physical boundaries but require a transnational coordinated response, which does not adhere to national or international regulations.

In the initial days of the World Wide Web[1], cybercrime was only limited to the defacement of websites and pulling harmless pranks. Fast forward to today, cybercrime has evolved into sophisticated and multi-layered deception strategy, which has become hard to detect, posing serious to the internet. Fraudsters are constantly evolving new techniques to deceive individuals with high net worth and target millions of unsuspecting victims worldwide. The internet is one of the social infrastructures that is increasingly becoming popular with cutting-edge technology and is responsible for the transformation of humanity. Social networking sites are increasingly becoming popular targets for cybercriminals, which has made it difficult to protect personal information. Thus, protecting individual data and protection of data centers is essential. This calls for a wide spectrum of security measures to protect information in the age of cybersecurity and national security.

Definition of Cyber Crime

Understanding the complex web of digital crimes starts by stating what cybercrimes are. Cybercrimes, also known as computer crimes, represent numerous illegal activities that govern computers, digital networks and cyberspace. They exploit gaps in the digital systems and information networks in order to steal data, breach privacy and inflict damage on people, businesses and governments. At its core, cybercrime is the transformation of everyday criminal activities in cyber space with information technology serving both as its instrument and focus. Thus, the adaptability of cybercrimes is clear, as they can take many shapes and forms such as identity theft, cyberbullying, hacking, spread malware, install spyware and spreading disinformation.

According to National Cyber Crime Reporting Portal, cybercrime can be defined as "any unlawful act where a computer or communication device, or computer network is used to commit or facilitate the commission of a crime".[2]

As technology and crime evolve so does the definition of cybercrime. In the initial stages of cybercrime, much of it was attributed to unauthorized access in computer networks. But as cyber environment grew, so did cybercrime, which broadly referred to the variety of crimes that utilize electronic systems for malicious purposes. In order to provide appropriate context to cybercrime, defining digital acts as crimes is essential. Among these actions include unauthorized access, stealing data, hacking, online phishing, distribution of malware, viruses, worms and trojans to undermine digital integrity. Certainly, the definition of cybercrime is not only limited to cybercrime alone but also focuses upon its ramifications on individuals, business and people. Cybercrimes can cause financial harm, damage reputations, erode trust and reduce confidence in information security and national security.

Classification of Cyber Crime

Cybercrimes can be classified into three distinct categories based upon its targets, which includes; People (Digital Harassment[3], Cyber Bullying[4], Phishing, Vishing, Smishing), Businesses (Website Hacking, Website Defacement, Virus, Worms, DDOS, Ransomware[5]), Governments (Denial of Service, Malware, Identity Theft, Email Spoofing[6], Espionage[7]). Through computer and cyber networks, these malevolent operations aim to acquire data, inflict harm and impede digital systems.

Crime Against People

Any assault on an individual's private information, privacy or well-being through cyberspace or computers can be considered as crime. Criminals employ fake advertisements to establish misleading sense of security while requesting personal information. Classifying social networking sites and online chat groups as major cybercrimes is now possible.

Crime Against Business

Businesses can suffer catastrophic consequences from cybercrime. Several cybercrimes have the power to shut down businesses permanently. Business continuity plans suggested by industry experts complement disaster management plans, and here is the reason why. To obtain sensitive and proprietary business data on the server, hackers compromise company's defense systems. They illegally access confidential information, divert funds, leading to companies' financial ruins.

Crime Against Government

Committing a crime against the government involves any illegal action taken against the state, its legitimate authority or how it functions. Such crimes put nation's territorial integrity, sovereignty and

digital stability at risk. When hackers illegally access government databases to misuse personal information, it is considered cybercrime. This erodes public's trust in government. Cybercrimes against government include; malicious attacks on information centers, critical infrastructure, stealing sensitive data, disrupt operational stability and commit acts of cyberterrorism.

Emerging Trends in Cyber Crimes

The swift development of information technology is leading to rapid changes in cybercrime. Criminals are leveraging cyber space with advanced cyber tools to victimize people, businesses and government. Below are the key developing trends.

- **Misinformation**

Incorrect or misleading information is known as misinformation.[8] Misinformation can be unintentional, but disinformation[9] is spread on purpose with the aim of deceiving. The unintentional nature of misinformation is often a result of ignorance, judgement error and misunderstanding. Misinformation encompasses a range of inaccuracies including; incomplete details, deceptive statements, outright falsehoods and carefully chosen half-truths. Misinformation is defined as content that once thought to be correct but later disproven, which is commonly seen in developing scenarios where verified information is missing or scientific understanding is absent. Digital networks like Facebook[10], Instagram[11], and X[12] are built to facilitate rapid sharing of information at a pace unmatched by other communication networks.

- **Disinformation**

Disinformation[13] is the product of individuals or groups of individuals who intentionally try to mislead their audiences. By eroding trust and blocking effective communication, disinformation inflicts harm and creates a direct impact on the masses. Fabricated, out-of-context, exaggerated and incomplete details can all be treated as active components of disinformation. False information can be found in various forms such as written words, sounds and pictures. The difference between misinformation and disinformation is rather unclear as it is tough to determine the intention behind sharing such falsehoods. While Mal information[14] refers to the use of true information with the intention of harm. Selective disclosure of information is carried out to manipulate opinions.

- **Deepfakes**

The term deepfake originates from its creation using deep learning techniques. Deep learning is a subset of machine learning, which is itself a part of artificial intelligence. A model is created for specific tasks by training machine learning models on data. Enhanced model performance is achieved through extensive and thorough data training. For classification or parsing, deep learning models can automatically identify data features. They are trained at a more profound level. Utilizing AI/ML based deepfakes[15] are a developing threat under the wider synthetic media umbrella.It is capable of producing realistic fabricated content like videos, pictures, audio and text. While synthetic media can be used for harmless entertainment, some of its applications carry serious security risks. The real threat posed by deepfakes and synthetic media does not lie in technology itself, but in the natural inclination to believe what one sees. This indicates that even simple counterfeit items can efficiently disseminate disinformation.

- **WhatsApp Impersonation Scams**

In WhatsApp[16] impersonation scams, cybercriminals often pose as unsuspecting individuals by utilizing unfamiliar phone numbers to create fabricated scenarios, such as; lost phone in order to extract funds or seek confidential information. Such scams leverage a sense of authority and urgency to deceive individuals into providing sensitive information or making urgent bank transfers. Messages will originate from an unknown number, with impersonator claiming to be a family member or friend. The conversation will convey a pressing need, prompting requests for quick money. In reality, these are scamsters using stolen credentials to defraud individuals.

Most common types of WhatsApp Scam Include;

- Family Emergency Scam[17]
- Account Takeover Scam[18]
- Fake Jobs Offer[19]
- Call Forwarding Scam[20]
- Tech Support Impersonation[21]

- **Facebook Scams**

Facebook scams are fraudulent schemes that employ sophisticated social engineering tactics, use of fake profiles or compromised social media accounts to pilfer money, access personal account and steal login credentials. Recently, AI developments have made these scams even more difficult to identify. Scamsters seek to defraud individuals, leading them to surrender funds or reveal confidential information. Consider receiving emails promotingget-rich-quick schemes, urgent texts from friends asking for help or fake emails requesting immediate action to restore your account suspension via malicious links as attachment.

Most common types of Facebook Scams Include;

- Marketplace Scams[22]
- Fake Friends Request[23]
- Fake Prizes Scam[24]
- Account Suspension Alerts
- Malware Downloads[25]

- **AI Powered Phishing**

Artificial Intelligence powered phishing is a scam that leverages AI to craft convincing messages and deceive individuals. They are difficult to identify compared to previous phishing methods. Phishing scams in the past frequently used copied templates and contained easily noticeable errors, such as bad spelling and grammar. With contemporary methods, the widely used AI generative tools have now been leveraged to compose phishing messages as and when needed by scamsters. Attackers are capable of rapidly producing new messages that are more human-like and believable. Current techniques go far beyond just bad spelling or awkward paraphrasing. Messages now refer to real-time events and current scenarios that match communication styles of trusted companies or colleagues. AI phishing has become a significant threat with messages been personalized effectively, resulting in clear and natural tone which doesn't seem suspicious.

- **AI Powered Hacking**

Artificial Intelligence powered hacking involves using AI to automate cyber-attacks. Such tools enable threat actors to produce code, examine systems and circumvent cyber defense with ease. AI models particularly LLMs, are accelerating attack developments, reducing costs and lowering the entry barrier for armature hackers. This results in cyber-attacks that are much quicker, faster and frequent. Cybercriminals are now leveraging AI to automate cyber tasks in order to amplify cyberattacks. AI hackers leverage machine learning tools, generative AI and autonomous agents to overcome security measures to exploit cyber vulnerabilities. AI is now being utilized to execute faster, smarter and more versatile cyberattacks unlike before. Cybercrime has now become a scalable operation with use of Artificial Intelligence. It is capable of creating harmful code, crafting phishing messages and assisting hackers with complete attack sequences.

Criminal use of Artificial Intelligence includes:

- Payload Generation
- Social Engineering
- Reconnaissance and Planning
- Autonomous Cyber Attacks[26]

- **Digital Arrest**

Digital Arrest[27] refers to digital fraud where scamster pose as national security officials, accusing victims of crimes and demand financial compliance. The notion of “digital arrest" is purely imaginary and lacks legal or constitutional mandate. Rather than genuine authority, its appearance is used to manipulate, intimidate and coerce individuals. In South Asia,[28] and notably in India,[29] this term has gained significance since 2023. In digital arrest scams, individuals are deceptively told they are under active investigation for committing serious crimes, which includes; money laundering, drug trafficking and child pornography. Scammers often pose as representatives from law enforcement agencies like the CBI,[30] ED,[31] and NCB.[32] Digital Arrest stands out compared to other cybercrimes as it employs psychological manipulation tactics via carefully structured and scripted impersonation. In many such

instances, victims are informed that a non-bailable warrant has been issued against them and subsequently been put under digital surveillance.

Scammers deploy deceptive tactics. This includes; phone calls, video chats, instant messages, emails, along with fake official documents, government seals, notices in order to support the narrative. Fake law enforcement uniforms, government ranks, badges, insignia and virtual backgrounds resembling actual police stations or courtrooms are established to create false sense of authority during such video calls. Victims of digital arrest find it psychologically taxing to inform people about their situation. Subsequently, individuals are forced to remit significant sums of money to resolve such situations and procure (false) digital bail by verifying their identities. In serious instances, victims are compelled to remain on video calls for extended periods (days or weeks), fostering an environment of total control, observation and fear. It is crucial to understand that digital arrest is not recognized within the Bharatiya Nyaya Sanhita.[33]

- **Mule Accounts**

Illegally obtained money through crime proceedings is processed via money mules accounts for cyber criminals.[34] Digital scammers rely upon mule accounts as a crucial conduct, allowing hackers to successfully steal money and evade capture. Cyber criminals can't immediately deposit proceeds of crimes into their bank accounts. Should they proceed, the transaction would eventually be traced by law enforcement officials, leading to arrests. Instead, money mules are employed to layer financial transactions. Initially, the illicit money goes into the mule's account. Then money mules are informed to relocate the funds. This leads to a complex trail of financial transactions, which makes it difficult to identify and locate the origins of crimes.

Money mules can be divided into two distinct categories;

  - **Unwitting Mule:** Individuals are often clueless that they are subject to violation of law**.** They may be hired by a cybercriminal under the guise of fake jobs. Funds are deposited into the victim's bank account, with instructions given to send them to clients in exchange for salary.[35]
  - **Complicit Mules:** Career criminals who purposefully open bank accounts with fabricated identities to facilitate money laundering for criminal organizations.[36]

- **Malvertising**

Malvertising is where online ads are used to distribute malware. Malvertising is the practice of inserting harmful ads into legitimate online advertising websites, intending to drive and attract users via advertisement products that serve as a strong vector for malware dissemination. By injecting malicious ads into prominent websites, malvertising allows attackers to target web users who are protected from standard firewalls. Hackers favor malvertising as it allows for bypass detection. It can install spyware to track user keystrokes to steal financial credentials or introduce ransomware virus that can lock computer.[37]

Conclusion

While the Internet has proven to be a vital asset, it should not be treated as a hotbed of cybercriminals. A perfect society with the absence of complete crime cannot be established. However, in order to keep criminality at its bare minimum, cyber rules must be followed, with regular law enforcement and cyber vigilance. The explosion in cybercrimes indicates the persistent rise in computer crimes in cyberspace, which is caused by rapid industrialization, globalization, internet penetration and increased dependence on cyberspace. Cybercriminals have significantly grown in numbers and have become impactful because of the growing digitalization of cyberspace that has far-reaching consequences. The sheer complexity of the Internet has resulted in sophisticated cyber-attacks, followed by a lack of awareness, weak cyber safety protocols and lack of digital hygiene. As technology continues to advance, so do cybercriminals. Hence, effective management of cyber security and national security is essential.

References

1. https://info.cern.ch/hypertext/WWW/TheProject.html
2. https://cybercrime.gov.in
3. https://reportandsupport.durham.ac.uk/support/what-is-online-harassment
4. https://www.missingkids.org/netsmartz/topics/cyberbullying

5. https://www.ibm.com/think/topics/ransomware
6. https://cybernews.com/secure-email-providers/email-spoofing
7. https://googledictionary.freecollocation.com/meaning?word=espionage
8. https://guides.library.iit.edu
9. ibid.
10. https://transparency.meta.com/policies/community-standards/misinformation
11. https://about.instagram.com/blog/announcements/combatting-misinformation-on-instagram
12. https://help.x.com/en/rules-and-policies/x-rules
13. https://guides.library.iit.edu
14. https://thesaurus.altervista.org/dict/en/malinformation
15. https://www.proofpoint.com/us/threat-reference/deepfake
16. https://faq.whatsapp.com/2286952358121083
17. https://www.globalsecuritymag.fr/Experts-warn-of-WhatsApp-family-emergency-scam-targeting-Brits-across-the.html
18. https://faq.whatsapp.com/479314433984258
19. https://faq.whatsapp.com/2286952358121083
20. https://bprd.nic.in/uploads/pdf/1716805963_bc3c2af8914f27cfc38f.pdf
21. https://www.leapxpert.com/impersonation-threats-in-whatsapp-are-real-how-to-prevent-them/
22. https://www.facebook.com/help/www/1295340050874305
23. https://www.youtube.com/watch?v=bnK8LPppT6M
24. https://www.which.co.uk/news/article/five-ways-to-spot-a-fake-freebie-on-facebook
25. https://www.facebook.com/help/389666567759871
26. https://inspiraenterprise.com/autonomous-ai-attacks-unlock-new-cybersecurity-nightmares-for-enterprises-yourstory/
27. https://www.niti.gov.in/sites/default/files/2025-04/Digital_Arrest_The_Modern_Day_Cyber_Scam.pdf
28. https://www.bbc.com/news/articles/cdrdyxk4k4ro
29. https://www.livemint.com/money/rbi-moves-to-prevent-banks-from-mis-selling-financial-products-how-will-it-protect-customers-11773835360854.html
30. https://frontline.thehindu.com/social-issues/ai-deepfake-digital-arrest-scams-india-cybercrime/article70587955.ece
31. ibid.
32. https://www.facebook.com/icicibank/posts/digital-arrests-are-a-lie-real-authorities-never-make-arrests-or-demand-money-on/1079706700851506/
33. https://www.indiacode.nic.in/handle/123456789/20062
34. https://www.acfe.com/acfe-insights-blog/blog-detail?s=what-you-should-know-about-money-mules
35. https://hyperverge.co/blog/money-mule/
36. ibid
37. https://www.geeksforgeeks.org/ethical-hacking/what-is-malvertising.

❑❑❑