ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

"Tracing The Evolution of Cyber Crimes: From Early Incidents to AI-Powered Threats and Their Impact"

Rachel Ann Marngar, Abhinaya, Vismaya SR

Kristu Jayanti Deemed to be University, India

DOI: https://doi.org/10.51583/IJLTEMAS.2025.1408000150

Abstract: From the initial rise of technology, mobile devices and the widespread use of the internet, which has also given a head start to the spreading of fraudulent cyber-crimes and online scams. With individuals being dependent on mobile devices from simple communication to totally being dependent for various primary purposes such as online shopping, online gaming, online payment and providing personal information on social media platforms more than ever before have given way for criminals to take advantage of this opportunity for their illegal and deceitful activities ("The_Global_Rise_of_Online_Devi," n.d.). This paper stresses on the rise and evolution of cybercrimes and how it has affected many people with their day to day livelihood. The concept of "going virtual for everything" has been one of the main reasons for the ever increasing cybercrimes and the growth of artificial intelligence has rapidly changed the entire view of cybercrimes. These fraudulent activities aim to deceive and defraud individuals and organizations, resulting in financial loss and identity theft. The impact of online frauds and scams goes beyond financial losses, they can also cause emotional distress and erode trust in online platforms and transactions.

The evolution of cybercrimes from the first ever reported cybercrime to the recent crime will be discussed along with the advancements of different cybercrimes including the detection method. It also stresses upon the different methods sorted during the first ever cybercrime that had taken place and the differences of the newly found methods for modern cybercrimes.

Keywords: Cybercrime, cyberspace, evolution, internet, virus attack, scam, cyberterrorism, machine learning.

I. Introduction

Cybercrime is described as the unlawful actions that manage using digital devices or computers and refers to all criminal activities with the medium of computers. Crimes can vary from individuals, organization, government, a cyberattack, causing disorder, or taking advantage of the vulnerability. Some types of cybercrimes are hacking, identity theft, phishing, cyber-pornography, software piracy, online drug trafficking, email spoofing, cyber stalking, cyber terrorism, spamming, web jacking, and cyberbullying. Cybercrime emerged when there was a rational development in digital technology and it led to the drastic change in the digital world. The technological revolution and hooked up to the internet had discovered opportunities for a threat actor to exploit vulnerabilities in computer systems. Some of the impacts that lead to cybercrime are financial losses, data leakage, critical infrastructure failures, repercussions on business, and social effects. These made society more vulnerable to cybercrimes. In recent years there has been a rise in the number of online frauds and scams This is mainly due to the drastic spread of the internet and digital technology, which provide new opportunities for criminals to take advantage of individuals and organisations. In 1834, two thieves broke into the French telegraph systems and stole financial market data, which is considered the first cyberattack in history.

As cybercrimes traced back to the late 20th century, where criminals regularly committed crimes via telephone lines. The modern technologies are persistently increasing cybercrimes as new technologies bring new online crimes, and various preventive measures have been taken to combat these cybercrimes. "CYBERSPACE" is a new term for the environment where individuals communicate through computer networks, which is a faster mode of communication as compared to the traditional ways of communication. This in turn has made people even more vulnerable to face cybercrimes and adds to the ever-evolving forms of cybercrimes(Malik et al., 2019). The reason for the commission of computer crime and cybercrime is money. People commit cybercrimes to make money quickly and easily and to revenge other people, organisations, castes, or religions by causing them physical harm or damaging their reputation, or to get recognition if they hack a very secure network like a defence site or network. The natural security in cybersecurity and cyberspace11 is used to refer to the security offered through anti-services to protect your online information and about cyberspace to form a global computer network to facilitate online communication, so threats in cyberspace are hacking, cybercrime, cyberterrorism, etc. One of the recent cybercrimes that involved one of the most notable phishing attacks was the OCBC bank phishing case in Singapore in December 2021, where approximately 420 OCBC bank customers fell victim to SMS phishing scams. The use of forensic software tools for drive imaging was designed to facilitate efficient analysis and gathering and compilation of the phishing evidence that helped to conclude the case.(Azam et al., 2023). Meanwhile, with the continuous development in computer system technology, the increase of cybercrimes has also improved its pace accordingly.

II. Background

The paper includes the introduction and definition of cybercrime and its types and how it has impacted the entire world as a whole. It includes the initiation of cybercrime from the olden period starting with traditional crimes that evolves strategically with the founding of the internet which adversely introduces to new and sophisticated cybercrimes. This paper stresses on the

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

evolution of cybercrime and the use of forensic science in this field. The introduction of forensic science which aids in the investigation method and preservation of evidence has played a major role in the process of cybercrime investigation. This paper also mentions the importance of knowledge and awareness of these cybercrimes and how to prevent the effects and damages of these crimes. The improvement of the law and the working of enforcement agencies which adds to the solving of cybercrimes.

Objectives and Scope

The objective of this study is to compare the differences between olden stages of cybercrime and modern cybercrime which has gradually upgraded over the years. The study includes the significance of the coming of the internet which is the main reason for the evolution of cybercrime and the need for people to be informed about the extreme aftereffects of cybercrimes and to be aware of the laws which are related to such crimes. This paper is mainly for the purpose of understanding how cybercrimes have evolved and how it is continuing in recent years with even more advanced technologies and the intricate challenges which law enforcement agencies face to combat against cybercrime.

III. Methodology

This review addresses the basic learning of cybercrime and how it came into existence and the extensive major approach throughout the years. The topics related were sourced from available review papers directed from google scholar, Research gate and PubMed. Only resources from sources deemed reliable by the publication community have been added to the collection; this includes publications with established publication names, web sites, and potential DOI numbers. It did not contain any content from unreliable sources. A direct search on Google is conducted using the previously mentioned sources. The papers were thoroughly read by the writers of this review paper and have provided our opinions and thoughts and dwell on many new changes. A qualitative review methodology was employed, relying on an in-depth analysis of existing literature from credible academic approach to ensure accuracy, relevance, and scholarly integrity. The commonly used web browsers, Google Chrome and Mozilla Firefox, to extract and compile the abstracts and titles of published publications. The procedures adopted are listed below:

1. Choosing a relevant topic and name for the paper- The first step involved identifying a topic of relevance and interest and scope definition. The topic on cybercrime was selected due to its growing impact across the digital world and increasingly significance in both law enforcement and cybersecurity domains. The scope of this paper include the historical emergence and evolution of cybercrime, its types and classifications. It also includes the emerging national and international laws governing cyber offences. This paper also embraced and encourage public awareness, education and preventive measures to reduce the events of cybercrimes. Technological tools and systems which are used in cybercrime detection by forensic experts have been done.
2. Selection of online sources- A comprehensive literature search was conducted using academic databases such as Google scholar, PubMed and Research Gate. Only peer-reviewed journal articles, conference papers and institutional reports were considered. Unreliable or non- academic sources or unverified websites were excluded to maintain the integrity and accuracy of the review.
3. 3. All sources of information were appropriately cited and no data was being misrepresented. The review was conducted in accordance with ethical research practices. Forensic applications were also added and was based on scientific researches on how forensic experts are involved in cybercrimes to solve, preserve and analyse evidences.

Absence Of The Law In The Olden Period, Which Led To Increase Of Cyber Crimes

At the beginning of the first stage of cybercrimes, there were no laws and regulations to govern or combat such crimes. In the early 20th century, the term cybercrime was virtually non-existent and the legal framework did not account for such crimes. It only began in the early 1930s after the invention of computers and the development of cryptographic techniques during World War II, that laws and interventions regarding such digital crimes began to kick start. Cybercrimes pose significant threats and challenges due to the easy wide range accessibility of the internet, its portability and its global reach. with billions being active and connected, offenders can operate and attack anonymously evading any sort of detection. Law enforcement agencies and legislature bodies face a lot of difficulty in surveilling these issues and call for immediate action, legal measures and technological safeguards. Before such digital laws were implemented, the government mainly focused on making laws pertaining to protection of physical property and the traditional forms of communication. In the early 20th century, laws against wiretapping were one of the earliest laws relating to electronic devices. As law enforcement agencies and legislation bodies lack the potential and expertise to tackle cybercrimes, the focus remains on solving traditional crimes with the lack of understanding of cybercrimes and electronic vulnerabilities being very limited which led to the rise and increase of more digital crimes. Initially the focus on computer manipulation and telecommunication theft, cybercrime has expanded with technology to include hacking, botnets, and network-based crimes. The increasing connectivity and the Internet of Things introduce new vulnerabilities, continually presenting fresh challenges for cybersecurity. The evolution of the internet has evolved to widespread cybercrime laws for example the 2001 EU convention on Cybercrime. Laws were implemented by the United States such as Computer Fraud and Abuse Act (CFAA), enacted in 1986 and the Electronic Communications Privacy Act (ECPA), passed in 1986 which serves as

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

primary statutory mechanism for prosecuting cyber criminals and providing penalties, punishments, fines and imprisonment with severity depending on the nature of the crime.

The second half of the 20th century laid the groundwork for modern cybersecurity practices. Through early legislation, specialized law enforcement units, international cooperation, CERTs, public education, and technological advancements, significant strides were made in combating the growing threat of cybercrime. These efforts provided the foundation for the more sophisticated and coordinated approaches used today. (Chimchiuri, 2024) As cybercrime grows more sophisticated and harder, the need for specialized units is required. These units were equipped with the technical skills and knowledge required to investigate and prosecute cybercrimes. Cybercrime legislation is evolving rapidly to tackle new cybercrimes and digital threats.

Early stages of cybercrime

The origin of cybercrime traced back to the beginning of the 19th century with the materialization of the telegraph to obtain information based on financial reports. In 1834, a nefarious incident about two individuals trying to penetrate the French telegraph system to acquire unlawful data. This marks the beginning of one of the first known cybercrimes. Incidents of hacking telecommunications began to surface and positioned the foundation for the different types of network invasion and exploitation of innovation which sums up to modern cybercrime.(Allahrakha, n.d.)

Cybercrime was essentially unheard of in the 1940s due to the lack of restricted availability of digital devices and when these devices were developed later on were not directly connected to the network system which reduces the potential threats of cyberattacks and cybercrimes at that period of time. Though cybercrimes were not prevalent in the early years, this period stood as the prime occurrence before the prevalence of cybercrime. In the late fifties, another sect which is referred to as 'phone phreaking' to trigger telephone systems by exploiting telecom protocols to avoid long distance charges and to make free calls. Regardless of efforts taken to take down 'phone phreaking' activities and devising methods to eradicate such activities, it then continued till the 1980s. Phone phreaking laid the platform for hacking culture in the technological landscape. ("The Convention on Cybercrime_ A Harmonized Implementation of Inte," n.d.)The emergence of malicious hacking started during the 1960s mainly by curious students and programmers even though computers were provided in a safe and secure environment like schools or colleges. With the advancement of technology and computers, the need for physical security decreased and password security system acts as a primary method to system access.(Monteith et al., 1920)

The 1980s occurred to be the significant evolutions of cybercrime which is marked with high profile attacks and the rise of antivirus solutions. The public became more aware of the nature of cybercrime and its potential threats. In developed countries like the United States, The US Department of Defence started publishing books and articles highlighting security concerns and vulnerabilities in relation to cyber security. Commercial antivirus software were the early solutions which reflected a need for the growing awareness and active defence against evolving cyber threats.(Ige, 2023)

However, cybercrime entered a rapid process of globalization in the 1990s. Computer networks gained public interest and their utmost attention in commercial use and limited to academic and official uses. As the growth of the internet was surprisingly fast, users acquiring access to the network faced threats from globalized cyberspace which became more complicated. The cyberspace where perpetrators indulged with the knowledge they gained, the networks they had crashed had provided them with different degrees of sophistication with new incentives. Personal information could be retrieved during voluntary surfing of the internet. Web sites could not only be tools by which attacks were carried out, but could also be targets for attacks.(Hunton, 2011)Malicious code were publicly released by attackers for the means of hobbyists but later monetized malicious for profit. The funds earned were put into research and development to create more advanced malicious software. As attackers found a reliable way to make money through cyberspace, incidents of such crime inevitably rise and devised business models that are low risk of being apprehended.

A different trend of cyberattack in the early 20th century involves 'phishing' emails where an attacker pretends to be from a trusted organization or from an individual sending emails to people that aims to deceive users to disclose personal information or installing malicious software. Attackers also use emails to trick people into surfing certain websites to harvest data for identity theft. Spear phishing is also a type of phishing attack which when users click a certain link that will allow attackers to exploit the user's browser and install a bot in their computer devices. An attacker also sends emails using mobile devices leaving phone numbers or voicemails for users to call back. Computer attacks began widespread internationally in the early 2000s where worms were being spread by citizens of different countries. For example, a love bug virus was spread by a student in the Philippines and in 2005, the Zotob bot was made public by a developer from Morocco. Most international attacks were prevalent in the United states and across Europe. Now attacks come simultaneously from different countries or from a single individual using bot-assisted machines in different countries to mask the source of origin. Some attacks are motivated by political or national propaganda between two or more countries. The rise in online communities where individuals in cyberspace sharing common interests bring together ideas and sharing of data to achieve certain goals. They provide detailed personal information and such data are being misused. High profile stalkers are using this information to target children and women.(Malik et al., 2019) Children with complete access to the internet face potential dangers of cyberbullying and other cyber threats leading to the deterioration of their well-being. Elderly people are especially vulnerable and prone to cyber scam due to their lack of knowledge and skills. People of many age groups are victims of online scams, phishing and email frauds which had an adverse effect on their livelihood.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

III. Modern stages of cybercrime

Modern cybercrime has evolved quite significantly with the advancement of technology and categorized into numerous stages or phases. These relate to illegal activities carried out using computers, networks and the internet. This is getting more sophisticated and widespread. the key modern stages of cybercrime are reconnaissance, initial access, establishment of foothold, privilege escalation, system exploitation, operational impact and evasion. Modern crime origins, therefore, are complex and multi-faceted, interplaying with historical, economic, social, and technological factors. To be able to understand how contemporary crime began, there is need to look at significant changes in society, governance, and technology that created a platform for criminal behaviour as is known today.

During industrialization and urbanization, society would experience a turning point away from their original forms as agrarian societies transformed into industrial ones. Then came the mass migrations towards different centres in the cities where this gave rise to an immensely populous city with all related bad living conditions, enormous economic disparities, and stretched scant resources of law enforcements within these cities. The basis was fertile for a newly born form of crimes with varieties like organized thefts and frauds and exploitative services.

Economic and social inequality: with the development of capitalism as well as its class divisions that accompanied it, there became increased inequality in wealth as well as opportunity. Often, inequality would push away the marginalized group toward criminality as a survival mechanism as well as a form of resistance. Labour dispute crimes such as sabotage and strikes also rose during this period.

During the 19th and 20th centuries Advancement of Technology Introduced innovations that had a positive impact on daily life but also opened up the avenues for criminal activity. The building of railroads allowed transporting goods over long distances but opened up opportunities for train robberies. The development of telecommunications paved the way for cybercrimes in this digital age.(Li, n.d.) Globalization and International Crime. The expansion of trade and travel connected distant parts of the world, enabling the rise of transnational crimes such as drug trafficking, human smuggling, and arms trading. During the initial periods of globalization, enhanced transportation systems and laxer international regulations enabled the flourishing of these activities. Organized Crime: Its Evolution The late 19th and early 20th centuries saw the institutionalization of organized crime groups such as the Italian Mafia and American gangster syndicates. They seized on such social transformations as Prohibition in the United States to create large, illegal markets. Legal and Political Developments. Changes in legal and political systems also contributed to modern crime. For example, colonialism imposed new legal systems that criminalized indigenous practices, which often led to resistance and rebellion. The rise of nation-states also brought more systematic approaches to policing and punishment, sometimes inadvertently creating professional criminal adept at avoiding these systems.

Cultural Changes and Media Influence. The mass media explosion of the 20th century brought crime into the public eye, shaping perceptions and behaviours. Sensationalized accounts of criminals and their exploits often romanticized unlawful behaviour, influencing both would-be offenders and societal attitudes toward crime. The Digital Revolution over the past few decades, the rise of the internet and digital technologies has fundamentally changed the face of crime. Cybercrime, including identity theft, hacking, and online fraud, has become one of the defining features of modern criminal activity. The anonymity and universal reach of the internet empower it as a tool in illicit activities that are often beyond the methods of traditional law. Modern crime stems from historical processes and recent developments. A combination of economic shifts, technological advancements, and social changes has birthed a dynamic and shifting criminal landscape. Understanding origins is essential in developing useful strategies to fight crime for the present and future.(TKALICHENKO et al., 2021)

Impacts of cybercrime

Modern cybercrime has caused deep impacts on individuals, businesses, and society at unprecedented levels of financial, emotional, and social disruption. With the widespread development of digital technology and the internet, cybercriminals have devised new ways to exploit vulnerabilities in their pursuit of personal data, financial systems, and even critical infrastructure. Data breach involving personal details such as social security numbers, banking details, and personal correspondence has led to a widespread problem of identity theft, where millions have become victims. Most people have suffered huge financial loss through this, including the deterioration of their credit scores, followed by lengthy litigation cases aimed at restoring stolen identities.(Hemraj Saini, 2012) The problem also presents a scenario of phishing and ransomware attacks targeting users with a lack of cyber security awareness. In addition to extortion, ransomware also cripples life in general, locking people out of important systems and data. Apart from monetary damage, cybercrime takes psychological tolls, including fear, tension, and helplessness.(Professor, 2019) Cyberbullying and online harassment have increased dramatically, particularly with the emergence of social media, impacting mental health and, at worst, pushing some individuals into depression or even suicidal thoughts. On a wider level, cybercrime reduces trust in digital systems and discourages people from adopting technologies that could enhance their lives. Societal impact is also quite disturbing because cybercrime siphons resources into fighting online threats, affecting governments, businesses, and individuals. The further advance of technology is expected to bring about increased reach and sophistication of cybercrime, emphasizing the need for comprehensive cybersecurity education, legislation, and global cooperation in order to curb its effects.(Chevers, 2019)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Types of modern cybercrime

1. Phishing

Attacks Phishing involves attacks by cyber-crooks, who send faked communications, mostly email-based, that attempt to confuse people into providing sensitive data like passwords, credit card number or social security information. Sometimes the messages are from known establishments like banks or companies of computing and technology, laced with urgent words that can spur people into action promptly. Phishing scams take several sophisticated forms, most importantly spear-phishing (aimed attacks) and other ways, such as using decoy websites that almost duplicate their real counterparts.(Manky, 2013)

2. Ransomware

Ransomware is a form of malware that encrypts the victim's data and demands money in some sort of cryptocurrency for the unlock key. The attackers can lock essential systems and data in businesses, hence disrupting the operations. Well-known ransomware attacks targeted hospitals, schools, and government agencies. Other ransomware attackers also double extortion by threatening to leak data stolen in case the ransom is not paid**.**

3. Identity Theft

Identity theft involves stealing one's personal information, like names, social security numbers, or financial information, for fraud. Such data is often obtained through breaches, phishing, or spyware by cyber criminals. These stolen identities may be used to open a bank account, apply for loans, or make purchases without permission, which will cause considerable financial and emotional stress for the victims

4. Cyberstalking

Cyberstalking uses digital means to harass or intimidate individuals. Offenders may monitor victims through social media, send threatening messages, or spread false information online. This crime often escalates into offline threats, making it particularly dangerous. Victims of cyberstalking often feel violated and may face difficulties proving the harassment due to the anonymity the internet provides

5. Online Fraud

Online fraud comprises auction fraud, online retail scams, as well as fake investment schemes. In auction fraud, for example, criminals misrepresent items or fail to deliver them after payment. Online fraud further includes fake websites or emails that mislead victims in giving money or sensitive information under false pretends.(.Lee, 2017)

6. Hacking

Hacking relates to unauthorized access to computers or networks with the intent of stealing or altering data or destroying them. Hackers enter this way by exploiting weaknesses within software, weak passwords, or unpatched systems. While some hackers come with ethical intentions, generally known as white-hat hackers, malicious hackers, sometimes referred to as black-hat hackers, intend to disrupt operations, steal information, or demand ransoms.

7. Cyberterrorism

Politically or ideologically motivated attacks against digital infrastructure to create fear or disrupt critical systems characterize cyberterrorism. Its target is power grids, transportation systems, and communication networks. Catastrophic in its impact, this will have implications on the public safety and national security of a country.(Georgi et al., 2020)

Recent case study of cybercrime

Real-World Case Studies: The Deepfake CEO Scam

Countering AI-Powered Social Engineering Attacks: An unusual instance of audio deepfake cybercrime surfaced in early 2019 when a sophisticated voice-cloning scheme scammed a UK-based energy company out of $243,000 (about €220,000). One of the first instances of AI-generated deepfake technology being used in business fraud was this occurrence. The scam showed how threat actors can use artificial intelligence, which was initially created for benign use cases like accessibility or entertainment, to mimic human voices convincingly and take advantage of trust in corporate hierarchies. On trusting the voice which the authority it conveyed, one of the employee made the transfer and the company later discovered the scam only after the funds had been quickly moved offshore, making the recovery process a huge task at the most impossible for the company. The amount lost was around $243,000 and was being transferred to a Hungarian bank account which quickly funnelled through additional foreign accounts. The company was unable to recover the funds which they apparently face a huge loss. Follow-up emails were sent to the company which appeared to come from a legitimate company accounts and realistic transaction instructions were being provided to execute the fraud. The technology which was used was a text-to-speech deepfake generator trained on publicly available samples.

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Application of Forensics in Cybercrime

Cybercrime can be drastically complex and intricate, and it can be challenging to unravel for first responders, investigators, forensic experts, and administrators of criminal justice to combat cybercrime. The police department has been revolutionised to use digital forensics, which is a branch of forensic science when it comes to the discovery, acquisition, and investigation of cybercrimes. It is significantly very important to spread awareness of cybercrimes and to explore the factors relating to investigating and exposing these offences. The community needs to be aware of the impact of cybercrime and require special knowledge and education about these crimes and to reduce the occurrence of cybercrimes. Forensic services play an important role and act as a core function to analyse and investigate cybercrimes, which aid in the criminal justice system. Forensics acts upon the collection, preservation of digital evidence, removal of any tampering devices, and tracing and tracking of IP addresses or the digital footprints of the cyber attacker. As technology is a major factor that facilitates the commission of traditional cybercrimes, including offences against property or offences regarding personal harm, already existing investigation methods may sometimes be incapable; hence, the need to update certain investigation processes is mandatory, and forensic experts dealing in digital crimes need to be aware of new methods or modus operandi that cyber attackers use to manipulate other individuals. Forensics adds value to the investigation process by establishing facts and blending investigative and technical methodologies, which are utilised by digital forensics investigators. Forensics investigators developed certain skills to swiftly assess and apprehend cybercrimes. This can include communicative, rational, intuitive, and resilience to effectively attend to the rigorous nature of a cybercrime inquiry. These skills are coupled with experience to apply such crimes in real and virtual environments. Other investigative skills involve research to gain insights from various sources and strict compliance when handling electronic evidence while conducting digital forensic investigations. Logical and practical methods to forensically acquire data and verify various sources of information. Data retrieval and extraction of metadata, deleted files, and formatted information are basic skills that aid in investigation. Digital forensic investigators also abide by certain rules and regulations for the admissibility of evidence in the court of law.(Brown, 2015)

Education of modern cybercrime

Education for contemporary cybercrime is the ability to understand its changing character, methods, and overall implications on society. Once mostly an activity of secluded hackers, cybercrime has transformed into a sophisticated and complex threat that transcends national borders and encompasses numerous activities ranging from financial fraud to intellectual property theft and even cyber espionage and cyberterrorism. Modern cybercriminals use advanced malware and phishing campaigns, ransomware, and APT to breach systems, compromise information, and disrupt service offerings. With the diffusion of digital technologies, for instance, IoT, cloud computing, and AI, criminals have found new windows through which to exploit other vulnerable parties. These innovations have created more entry points for attacks while simultaneously making it more difficult for individuals and organisations to secure their systems. Moreover, the anonymity of the internet, coupled with the decentralised nature of cryptocurrencies, has allowed cybercriminals to operate with relative impunity, evading traditional law enforcement mechanisms. Cybercrime has become an organised activity in many cases and is often linked to transnational crime syndicates or even state-sponsored actors who engage in politically motivated cyberattacks. With the development of cybercrime, the importance of effective education in cybersecurity is increasingly felt. This includes not only technical training for professionals but also awareness campaigns for the general public, emphasising safe online behaviours, recognising phishing scams, and understanding the risks associated with the digital world. On a larger scale, governments and international organisations are working to strengthen legal frameworks, improve cross-border cooperation, and develop proactive defence mechanisms. However, the dynamic and borderless nature of cybercrime is unique and poses challenges requiring constant adjustments in educational and operational strategies to stay ahead of the malicious actors. In this context, public education, students, and cybersecurity professionals need to be educated in order to build resilience against the growing threat of modern cybercrime.(Wall, n.d.)

Detection of cybercrime

Modern cybercrimes are detected through a multi-faceted approach. While traditional forensic methods such as log analysis, network monitoring, and system auditing are essential, these need to be supplemented by more advanced techniques such as machine learning and artificial intelligence (AI) for detecting anomalies in real-time. (Fluchs et al., 2023)For instance, behavioural analysis may help identify unusual patterns of activity that may indicate a security breach or the presence of malware. Forensic investigators rely on digital footprints such as IP addresses, metadata, and transaction logs in tracing criminal activities back to their source. The increased usage of cybercrime-as-a-service platforms has given the possibility of buying hacking tools and services.(Sanjay Goel, 2023) Thus, cybersecurity professionals must be alert about the new threats and tactics emerging in this regard. This demands constant training on the newest cybercrime detection technologies and collaboration on threat intelligence across organisations and even among private and public institutions and law enforcement agencies. It is also increasingly deploying honeypots to capture cybercriminals and employing block-chain technology to trace transactions.(Thomas Holt, 2015)

Cybercrime detection and prevention continue to present ongoing challenges in an endeavour that needs proactive and collaborative measures. Effective detection systems rely on real-time monitoring, pattern recognition, and a robust response mechanism to mitigate the impact of cybercriminal activities. Moreover, educating individuals and organisations about cybersecurity hygiene—such as regular software updates, the use of strong passwords, and phishing awareness—remains one of

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

the most critical defences against cybercrime. These changes require law enforcement agencies to transform by utilising specialised cyber units and international cooperation in tracing cyber criminals that work from across the borders.(N Kshetri, 2013)

Cybercrime Detection Using Machine Learning

Machine Learning: Machine learning (ML) is a system that is engaged by feeding a large amount of data to an algorithm. The final product is a model that may be used to manage intelligent activities that go beyond the realm of traditional programming. Automatic learning frequently makes use of statistical, probabilistic, and other optimisation techniques. It enables the creation of models that use patterns identified in a formation dataset to classify new data after a formation. In the last ten years, machine learning (ML) has become one of the key components of artificial intelligence (AI) solutions used to prevent and detect cybercrimes like denial-of-service attacks, child pornography, cyberbullying, cyberterrorism, phishing, and other risks to the community and the business. There are numerous studies that address the use of machine learning (ML) to predict cyber threats, attacks, and other illegal online activities.

Blowfish- Blowfish, which was developed to replace the Data Encryption System, is another algorithm to fight cybercrime. This symmetric utility divides the messages into 64-bit blocks and then encrypts each message independently. During the tests, Blowfish proved to be quite effective and quick to implement. During this time, businesses have fully benefited from free access to the public domain in order to tackle cybercrime. It is possible to investigate Blowfish technologies in electronic commerce systems, particularly those pertaining to password management and payment security.(Wadha et al., 2020)

Researchers have used a number of algorithms that fall into the category of supervised algorithms, including KNN and naïve Bayes, as well as the category of unsupervised algorithms, like K-means, to detect cybercrimes uninformed. A simple member of the whole Bayesian learning machine is known by the name of Bayes. Consequently, the probabilistic obstacle it has been exposed to is that the Bayes network faces equally. It will be referred to as "naive" because its assumption that any variables are actually independent of another is wrong.

Cybercrime Detection Using Neural Networks

A neural network mimics the functioning of the human brain. The learning neurons that make up the brain are represented by the neurons in the neural network. Because of their prior experience, these neurons are able to create themselves again. This enables a neural network that has not been specifically designed to find a workable solution for problems of the same kind. In contrast to automatic learning methods, neural networks are thought to have a greater capacity to handle large amounts of material.(Chinedu et al., 2021) Among the technologies used to detect cybercrimes include software development, agent-based techniques, integrated programming, and artificial intelligence methods. Raiyn (Raiyn, 2014) has highlighted specific forms of cyberattacks. The researcher came up with the concept of using IP addresses to identify users' geographic location (i.e., country, city, and street) and to detect real-time cyberattacks. She also discusses cloud cybersecurity detection, highlighting some research that has been done on the topic.

Forensic tools: Cybercrimes have also been identified by analytical techniques based on forensic tools; for instance, Meera and colleagues (V Meera et al ., 2013) attempted to analyse cybercrimes committed through a virtual computer known as VMware. These days, disks with hard drives are used to simulate evidence. The researchers used the VMware files to locate criminal evidence on a virtual disc by using direct internal data collection and the extraction of raw data from many grains. A grain is a collection of sectors that contain data on a hard disc. The raw data is recovered and analysed using various forensic techniques in order to extract valuable information. The files recovered include the "vmdk" extension, which stands for VMware disc file. The main focus of the forensic investigation model (SRDFIM) is cybercrime and cyber fraud investigations (Dimitriadis et al., 2020). Among its ten steps are examination and analysis. The goal of the examination step, according to SRDFIM, is to locate relevant evidence, make it visible, and get it ready for analysis. For this reason, SRDFIM advises filtering the data, validating the patterns, looking for strategies, retrieving both ASCII and non-ASCII data, identifying cached files or documents, detecting incompatible extensions and signatures, etc. The analysis phase consists of a technical analysis of the material gathered and extracted from the examination tape in order to create connections between the data, assess their significance, reconstruct the events, and draw conclusions. In this opinion, SRD FILM suggests analysing the cycle time, analysing the cached data, analysing the apps, and files, analysing the relationships between the data fragments, and analysing the cached data. Therefore, it is clear that the model is technique-centered and does not offer a systematic method or approach to effectively manage the inspection and analysis steps. The Cyber Forensic Field Triage Process Model (CFFTPM) offers a way to quickly review, assess, and interpret digital evidence. The main goal of the model is to shorten the time required for an investigation into a crime scene, which is seen as a crucial component. The model suggests a number of steps to do in order to gather data from a Windows system. Among the processes are planning, triage, user and usage profiles, deadlines, online activity, and case-specific evidence. The CFFTPM does not specify how the objects and their classification can be used to further a research project. In the end, the steps seem to specify what needs to be examined rather than how an issue may be investigated using them.(Rogers et al., 2006)

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Detection of cybercrime using AI

Detection of cybercrime has vastly expanded by using AI driven tools and system detection in user behaviour and network traffic. By combining ideas from human–computer interaction research with adversarial machine learning approaches, detection accuracy can be improved and model robustness against manipulation and evasion strategies strengthened. AI-based cybercrime detection combines cutting-edge methods from data mining, behavioural analysis, natural language processing (NLP), and machine learning (ML) As an illustration, UEBA (User and Entity Behaviour Analytics) employs machine learning (ML) to identify anomalous activities, such as huge data transfers or login attempts made at unusual hours. Dynamic analysis of malware AI and sandboxing enable real-time file or application simulation in a controlled setting while keeping an eye out for harmful trends. Polymorphic malware, which alters its signature with every attack, is easier to detect with AI. Using Natural Language Processing (NLP) to identify phishing even if new variations are employed, AI can analyse internal and external interactions (email, Slack, etc.) to identify linguistic trends linked to social engineering or phishing. Natural Language Processing(NLP) can also be in use for the purpose to extract and analyse cyber threat information from unstructured sources such as dark webs, emails, forums etc. (Mulahuwaish et al., 2025)

AI- powered malware detection to identify and block malware which is firmly based on patterns in code or behaviour. The techniques used to identify malware are binary/ static analysis using Machine Learning and dynamic analysis consists of using sandbox and behaviour modelling. An example of this is using a neural network to detect polymorphic malware that can evade signature based detection. Another type of cybercrime which can be detected by AI is fraud detection in financial systems by using anomaly detection on transaction patterns, graph based detection of fraud rings and sequential pattern mining. Botnet Detection which is used to detect and disrupt networks of infected machines used for cyberattacks can be detected by network traffic analysis using ML. (Feily et al., 2009)

Future Directions

Since cybercrime is becoming widespread and more imperative to improve measures to counteract these threats. There are a number of gaps in the research on cyber security, as well as several approaches used to enhance and address network security issues. This area of research may present numerous opportunities to advance justice, raise awareness, improve cyberspace security, and establish a new security-based business sector. An increasing reliance on technology in criminal investigations has resulted from the complexity of risk actors. A variety of tools and techniques are available to researchers to aid them in their work. None of these tools are able to perform all of the tasks that researchers require. Therefore, familiarizing oneself with the various tools, their capabilities, and the data they may offer researchers is essential.(Horan and Saiedian, 2021)The field of digital forensics has been around for a while, yet it is constantly changing. The four primary areas of digital forensics remain essential for digital investigations even when new methods are developed. In mobile forensics, data can be extracted in a variety of ways. The most effective methods are logical extraction and hex dumps. With the increasing number of services moving to the cloud, the field of digital forensics is primarily expanding. The automation and automatic learning have advanced the field's technology, and they have an effect on online investigations as well. While machine learning enables researchers to identify and categorize this evidence, automation enables investigators to gather evidence more quickly. Furthermore, automation presents challenges for this profession in terms of underlying legal assumptions and their implications. There are numerous opportunities for additional research in this expanding field. As these technologies develop, automation and automatic learning present interesting opportunities for future research. The insufficiency of open intelligence methods in the sector has revealed another avenue for research.(Završnik, 2020)

IV. Conclusion

This study has highlighted the many types of cybercrimes. Additionally, an extensive analysis of cybercrime detection and prevention models over the past ten years using various multilevel marketing platforms and other intelligent systems has been provided in order to assess the effectiveness of multilevel marketing. After identifying the strengths of detection and prevention models and the challenges of applying them to real-world scenarios where threats, attacks, and violations are common, this review concludes that ML and most of the forensic tools being mentioned can be used to develop and implement intelligent systems aimed at reducing or combating cybercrimes in cyberspace. Important issues include determining whether dataset is suitable for analysis and assessing the study's cybercrime detection method. The lack of cooperation between researchers and law enforcement in gathering cybercriminals' data always results in the loss of reference data. The variety of cybercrimes is another matter, which can occur on various platforms like Instagram, YouTube, Twitter, or networks and include various datasets. Despite the advancements in cyber security, there are still many issues. Because cyber threats are dynamic, detection and response protocols must be continuously improved. Maintaining the ability of computer security systems to expand, interact, and confront new threats is a challenge for researchers and experts.

References

1. Kshetri, N. (2022). The global rise of online devices, cybercrime and cyber defense: Enhancing ethical actions, counter measures, cyber strategy, and approaches (Publication No. 29165177) [Doctoral dissertation, University of Missouri–St. Louis]. ProQuest Dissertations & Theses Global. https://www.proquest.com/openview/f5504834b2980c4808671dfad212f354/1?pq-origsite=gscholar&cbl=18750&diss=y

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

2. Ottis, R., & Lorents, P. (2010). Cyberspace: Definition and implications. In Proceedings of the 5th International Conference on Information Warfare and Security (pp. 267–270). Academic Publishing Limited. https://scholar.google.com/scholar?cluster=739456875908443413
3. Azam, H., Dulloo, M. I., Majeed, M. H., Phang Hui Wan, J., Tong Xin, L., & Sindiramutty, S. R. (n.d.). Cybercrime unmasked: Investigating cases and digital evidence. Semantic Scholar. https://pdfs.semanticscholar.org/9d91/d55029a4ebbe92e52602b0f4185eb0e4a27d.pdf
4. Chimchiuri, L. (2024). The evolution of cybercrime legislation. Scientific Works of National Aviation University: Series Law Journal "Air and Space Law," 2(71), 221–227. https://doi.org/10.18372/2307-9061.71.18813
5. AllahRakha, N. (2024). Transformation of crimes (cybercrimes) in digital age. International Journal of Law and Policy, 2(2). https://doi.org/10.59022/ijlp.156
6. Miquelon-Weismann, M. F. (2005). The Convention on Cybercrime: A harmonized implementation of international penal law: What prospects for procedural due process? John Marshall Journal of Computer and Information Law, 23(4), 329. https://repository.law.uic.edu/cgi/viewcontent.cgi?article=1057&context=jitpl
7. Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., & Glenn, T. (2021). Increasing cybercrime since the pandemic: Concerns for psychiatry. Current Psychiatry Reports, 23(4). https://doi.org/10.1007/s11920-021-01228-w
8. Ige, O. (2023). Trends of cybercrime from 2001 to 2021: Cybersecurity action plan for Papua New Guinea. Discover Global Society, 1(1). https://doi.org/10.1007/s44282-023-00007-7
9. Hunton, P. (2011). The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Computer Law & Security Review, 27(1), 61–67. https://doi.org/10.1016/j.clsr.2010.11.001
10. Malik, J. K., & Choudhury, S. (n.d.). A brief review on cyber crime – Growth and evolution. ResearchGate. https://www.researchgate.net/profile/Jitender-Malik-2/publication/340756419
11. Brown, C. S. D. (2015). Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55–119. https://doi.org/10.5281/zenodo.22387
12. Tkalichenko, S., Khotskina, V., & Solovieva, V. (2021). Cybercrime: The comparative analysis of the modern information space. Computer Systems and Information Technologies, 1, 56–62. https://doi.org/10.31891/csit-2021-3-8
13. Li, J. X. (2017). Cyber crime and legal countermeasures: A historical analysis. International Journal of Criminal Justice Sciences, 12(2), 196. https://doi.org/10.5281/zenodo.1034658
14. Renu. (2019). Impact of cyber crime: Issues and challenges. International Journal of Trend in Scientific Research and Development, 3(3), 1569–1572. https://doi.org/10.31142/ijtsrd23456
15. Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202–209. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=6b41f80de9a314af67b909b509d7119d0d29c787
16. Chevers, D. A. (2019). The impact of cybercrime on e-banking: A proposed model. CONF-IRM 2019 Proceedings, Article 11. https://aisel.aisnet.org/confirm2019/11
17. Manky, D. (2013). Cybercrime as a service: A very modern business. Computer Fraud & Security, 2013(6), 9–13. https://doi.org/10.1016/s1361-3723(13)70053-8
18. Lee, J. H., & Kim, S. J. (2017). Analysis and security evaluation of security threat on broadcasting service. Wireless Personal Communications, 95(4), 4149–4169. https://link.springer.com/article/10.1007/s11277-017-4056-z
19. Tsochev, G., Trifonov, R., Nakov, O., Manolov, S., & Pavlova, G. (2020). Cyber security: Threats and challenges. In 2020 International Conference Automatics and Informatics (ICAI) (pp. 1–6). IEEE. https://doi.org/10.1109/ICAI50593.2020.9311369
20. Cybercrime Magazine - page one for the cybersecurity industry. (2025, January 29). Cybercrime Magazine. https://cybersecurityventures.co/m
21. Fluchs, S., Taştan, E., Trumpf, T., Horch, A., Drath, R., & Fay, A. (2023). Traceable security-by-design decisions for cyber-physical systems (CPSs) by means of function-based diagrams and security libraries. Sensors, 23(12), 5547. https://doi.org/10.3390/s23125547
22. Digital forensics and cyber crime. (2024). In Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering. https://doi.org/10.1007/978-3-031-56583-0
23. Holt, T., & Bossler, A. (2015). Cybercrime in progress. https://doi.org/10.4324/9781315775944
24. Cybercrime and cybersecurity in the global South. (n.d.). Google Books. https://books.google.co.in/books?hl=en&lr=&id=SepWfACNTgQC&oi=fnd&pg=PP1&dq=Kshetri,+N.+(2018).+Cybercrime+and+cybersecurity+in+the+global+south.+Springer.&ots=BFHEp2vFZO&sig=pDiWYfG2EM-l002jEsVpDxBSPr4&redir_esc=y#v=onepage&q&f=false
25. Wall, D. S. (2017). Crime, security and information communication technologies: The changing cybersecurity threat landscape and its implications for regulation and policing. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.3005872
26. Al-Khater, W. A., Al-Maadeed, S., Ahmed, A. A., Sadiq, A. S., & Khan, M. K. (2020). Comprehensive review of cybercrime detection techniques. IEEE Access, 8, 137293–137311. https://doi.org/10.1109/ACCESS.2020.3011259
27. Chinedu, P. U., Nwankwo, W., Masajuwa, F. U., & Imoisi, S. (2021). Cybercrime detection and prevention efforts in the last decade: An overview of the possibilities of machine learning models. Review of International Geographical

ISSN 2278-2540 | DOI: 10.51583/IJLTEMAS | Volume XIV, Issue VIII, August 2025

Education Online, 11(7). https://www.researchgate.net/profile/Paschal-Chinedu/publication/355668267_Cybercrime_Detection_and_Prevention_Efforts_in_the_Last_Decade_An_Overview_of_the_Possibilities_of_Machine_Learning_Models/links/61792620a767a03c14bbc798/Cybercrime-Detection-and-Prevention-Efforts-in-the-Last-Decade-An-Overview-of-the-Possibilities-of-Machine-Learning-Models.pdf

28. Raiyn, J. (2014). A survey of cyber attack detection strategies. International Journal of Security and Its Applications, 8(1), 247–256. https://doi.org/10.14257/ijsia.2014.8.1.23
29. Meera, V., Isaac, M. M., & Balan, C. (2013). Forensic acquisition and analysis of VMware virtual machine artifacts. In Proceedings of the International Multi-Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s) (pp. 255–259). IEEE. https://doi.org/10.1109/iMac4s.2013.6526418
30. Agarwal, A., Gupta, S., Gupta, S., & Gupta, M. (2011). Systematic digital forensic investigation model. International Journal of Computer Science and Security, 5(1), 118–130. https://www.researchgate.net/profile/Yatendra-Gupta/publication/228410430_Systematic_Digital_Forensic_Investigation_Model/links/56ea8cd208ae95bddc2bcc6b/Systematic-Digital-Forensic-Investigation-Model.pdf
31. Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2019). D4I - Digital forensics framework for reviewing and investigating cyber attacks. Array, 5, 100015. https://doi.org/10.1016/j.array.2019.100015
32. Rogers, M. K., Goldman, J., Mislan, R., Wedge, T., & Debrota, S. (2006). Computer forensics field triage process model. Journal of Digital Forensics, Security and Law, 1(2). https://doi.org/10.15394/jdfsl.2006.1004
33. Horan, C., & Saiedian, H. (2021). Cyber crime investigation: Landscape, challenges, and future research directions. Journal of Cybersecurity and Privacy, 1(4), 580–596. https://doi.org/10.3390/jcp1040029
34. Završnik, A. (2020). Criminal justice, artificial intelligence systems, and human rights. ERA Forum, 20, 567–583. https://doi.org/10.1007/s12027-020-00602-0
35. Feily, M., Shahrestani, A., & Ramadass, S. (2009, June). A survey of botnet and botnet detection. In 2009 third international conference on emerging security information, systems and technologies (pp. 268-273). IEEE. DOI: 10.1109/SECURWARE.2009.48
36. Mulahuwaish, A., Qolomany, B., Gyorick, K., Abdo, J. B., Aledhari, M., Qadir, J., Carley, K., & Al-Fuqaha, A. (2025). A survey of social cybersecurity: Techniques for attack detection, evaluations, challenges, and future prospects. Computers in Human Behavior Reports, 100668. https://doi.org/10.1016/j.chbr.2025.100668