CYBER-SECURITY TACTICS IN MITIGATING CYBER-CRIMES: A REVIEW AND PROPOSAL

Adeniyi Phillips, Ibraheem Ojelade, Esther Taiwo, Callistus Obunadike and Kunle Oloyede

Department of Computer Science and Quantitative Methods, Austin Peay State University, Tennessee.

ABSTRACT

This article underscores the urgent need for a global response to cyber threats, discusses the risks associated with increasing reliance on technology, and sets the stage for a review focused on understanding and mitigating cybercrimes. In summary, the passage discusses the internet's impact on national development and the growing problem of cybercrime. It calls for a deeper understanding of the characteristics and motivations of cybercriminals and highlights several questions that need to be addressed to effectively combat cybercrime and its detrimental effects on society. The classification of cybercrime is summarized into five categories: Cybercrimes against Persons (including cyber pornography, cyber stalking, financial cybercrimes, phishing, and vishing), Cybercrimes against Property (involving intellectual property violations, data theft, and "Man in the Middle" attacks), Cybercrimes against Government, Denial of Service (DOS) Attacks, and Other Cybercrimes (comprising data diddling, salami attacks, email bombing, email spoofing, logic bombs, internet time theft, and mobile and wireless technology-related cybercrimes). This classification helps understand the diverse nature of cybercrimes, their attack methods, and tools used in their commission. This article discusses cybercrimes against government and the importance of cybersecurity. It highlights key cybercrimes against governments, including cyberterrorism and hacking/cracking activities. The text emphasizes the need for a cybersecurity culture and presents goals and prevention strategies to enhance cyber protection. It also mentions crime detection steps, tools, and defense methods to safeguard against cybercrimes. The passage emphasizes the importance of protecting electronic evidence and using software and hardware tools for digital forensic investigations. It also mentions various cybersecurity technologies and methods, such as network access control, honeypots, encryption, and intrusion detection systems, to prevent cyberattacks. Overall, the passage underscores the significance of cybersecurity in protecting critical information infrastructure and reducing cybercrime risks. Essentially, the need for comprehensive cybersecurity measures to protect against cybercrimes and the importance of detecting, preventing, and mitigating cyber threats against governments and critical information infrastructure.

KEYWORDS

Cybercrimes, cyber-security, information, and communication technology (ICT), cyberspace, Cyber-Terrorists

1. INTRODUCTION

Over the past two decades, the significance of the Internet has grown significantly, playing a pivotal role in enhancing a nation's competitiveness, fostering innovation, advancing globalization, and simplifying daily life[1], [2]. In today's interconnected world, the menace of cyber-attacks and cyber-threats has evolved into a pervasive global problem. These threats can wreak havoc on a massive scale within minutes, transcending borders, and necessitating a comprehensive, collaborative solution that involves all stakeholders. Governments, businesses,

and individuals have become increasingly reliant on the vast amounts of information stored and transmitted across advanced communication networks. The costs associated with cyber-attacks are staggering, encompassing revenue losses, sensitive data breaches, equipment damage, denial-of-service attacks, and network outages. The future growth and potential of our online information society hang in the balance as cyber-threats continue to escalate. Over the past few decades, computers have transformed society beyond all expectations, bridging social, economic, and cultural gaps and ushering in unprecedented convenience.

However, this reliance on information and computer technology (ICT) has exposed society to the ever-looming threat of cybercrime. The internet's growing significance and our increasing dependence on it have given rise to a plethora of new criminal opportunities. Cybercrime is a global phenomenon and an evil bedeviling the world, causing lots of losses and damage to human resources and lives [3]. Cybercrime is any criminal action which occurs on or over the vehicle of computers or internet or other technology acknowledged by the Information Technology Act [4]. In other words, it is any unlawful activity where either a tool or target are towards computer or internet. Despite cybercrime is an uncontrollable evil, however, it can be curbed [5], [6].

In our pursuit of a crime-free society, we are met with a harsh reality – crime is an ever-present companion of society, shaped by its very nature. Furthermore, the complexity of society dictates the complexity of the crimes that emerge within it. Understanding prevalent crime and seeking effective solutions requires a deep dive into the socio-economic and political structures that underpin society. When studying the nature and scope of crime, it is essential to consider the preventive and corrective measures adopted by societal mechanisms to control crime and delinquent behavior. One of the most profound challenges of our time is cyber security. The rapid expansion of information and communication technology (ICT) networks has created new opportunities for criminals to exploit online vulnerabilities and target critical infrastructure of nations.

This review aims to provide an in-depth exploration of cybersecurity strategies for mitigating cybercrimes. We will delve into the motives behind individuals engaging in cybercrime, the reasons driving their involvement, the various types of cybercrimes, and examine cybersecurity tactics. Furthermore, proposes recommendations to curb the rising tide of cybercrimes and cybercriminals.

1.1. Research Problem

The internet has undoubtedly contributed to national development, but it has also given rise to a new wave of cybercrime that threatens to undermine this progress. Cybercrime has transcended geographical boundaries, becoming a pervasive and persistent issue that afflicts nations worldwide. The alarming increase in cybercrimes can be attributed to a lack of security awareness and underreporting of incidents. Geopolitical boundaries hold no sway when cybercrimes are committed, as individuals with access to computers and the internet can perpetrate criminal acts from virtually anywhere on the globe. The speed, ease, and potential damage of cyber-criminal activities are amplified by the internet's reach. Considering these realities, cybercrime must be viewed as a global issue that demands a comprehensive understanding of its root causes and viable solutions.

Efforts by governments and international organizations to combat cybercrime have yielded limited results due to the elusive nature of cybercriminal identities. There is a pressing need to identify additional attributes of cybercriminals and explore the motivating factors behind their actions. The queries that easily come to mind include: What are the socio-economic characteristics of those involved in cybercrime? What drives youth to engage in cybercrime?

What techniques do cybercriminals employ to execute their acts? What measures have law enforcement agencies implemented for cybercafe operators to combat cybercrime? What are the broader societal impacts of this menacing phenomenon? This study seeks to address these critical questions and contribute to our collective understanding of the complex landscape of cybercrimes and their control.

2. LITERATURE REVIEW

The Internet is a global network which connects several computers located in numerous countries and openswide-rangingchances to obtain and exchange information. Ithas now been abused for criminal purposes due to the economic factors. It has created a geometric growth and accelerated openings of opportunities for businesses and the elimination of economic obstacles hitherto faced by nations of the world. Cybercrimes differ from most terrestrial crimes in four ways which are: They are easy to learn; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present and they are often not clearly illegal. Cybercrime is one of the major security issues for law enforcement agencies and the world in general. Some of the possible adverse effects of cybercrime could include the destruction of the country's image both at home and abroad, insecurity of both life and properties, fear of doing business, economic loss of spending substantial amount of money on the prevention and control of cybercrime amongst others.

Over the past two decades, the Internet has become an integral part of global communication, with over 3 billion users worldwide [7]. It has not only facilitated connectivity but has also contributed significantly to the global economy, generating billions of dollars annually [8]. Today, cyberspace serves as the primary arena for economic, commercial, cultural, social, and governmental activities at all levels, encompassing individuals, non-governmental organizations, and government institutions [9]. Crucial infrastructures and systems either reside in cyberspace or are controlled through it, while vital information is stored and exchanged within this realm [10]. Moreover, most media activities, financial transactions, and citizen interactions now occur in cyberspace [11]. The income generated by cyberspace businesses has become a significant component of a country's Gross Domestic Product (GDP), and cyberspace metrics play a substantial role in measuring development [12]. Consequently, a considerable portion of a nation's resources and its citizens' material and spiritual achievements are intertwined with cyberspace, making any instability or insecurity in this domain directly impact various aspects of citizens' lives [13].

However, cyberspace has introduced new security challenges to governments. Its low entry cost, anonymity, geographical uncertainty, and lack of transparency have attracted various actors, including governments, organized groups, terrorists, and individuals, leading to threats like cyber warfare, cybercrime, cyber terrorism, and cyber espionage [14]. These threats differ from traditional national security threats, which are typically transparent and associated with identifiable governments and nations within specific geographical areas. Consequently, traditional national security measures have proven ineffective in the cyber domain [15].

Analysts have been contemplating the potential consequences of cyber-attacks for over a decade, envisioning scenarios involving severe physical or economic damage. These scenarios range from financial systems being targeted by viruses to disruptions in stock markets, power plants, and even air traffic control systems (Snehi and Bhandari, 2021; Ahmed Jamal et al., 2021). However, addressing these complex and diverse aspects of cyber-attacks and providing legal advice and analysis remains challenging until there is a universally accepted definition of what constitutes a cyber-attack [16].

This raises the fundamental question of what precisely defines a cyber-attack and whether every action within cyberspace qualifies as a traditional-style attack [17]. Establishing a comprehensive definition of a cyber-attack would significantly impact the legal framework for addressing and assessing the consequences of such attacks (Furnell et al., 2020). Without a clear and universally accepted definition, legal interpretations and practices vary, sometimes leading to conflicting legal conclusions [18].

Therefore, it is imperative to develop an agreed-upon definition, especially as a starting point for understanding, adapting, and analyzing this subject. In this study, we first delve into the nature of cyber-attacks, followed by an examination and classification of different types of cyber-attacks. Subsequently, we explore existing definitions as proposed by international experts and organizations. Finally, we present the conclusions drawn from this paper.

2.1. Characteristics of Cybercrime

Cybercrime is different from traditional crime with the following peculiar characteristics:

1. Experts are involved – Cybercrimes are perpetrated by well-educated information and computer technology (ICT) experts.
2. Geographical challenges – The geographical confines shrink to zero in cyberspace this implies that a cybercriminal sitting in any part of the world perpetrate crime in other location of globe in other words there are no geographical boundaries.
3. Virtual World – Each action of the criminal while perpetrating the crime is done over the computer-generated world.
4. Difficulty in Proving Collected Evidence – This is occasioned by the fact that cybercriminals cite jurisdiction of several countries while committing cybercrime.
5. Inconceivable Crime Magnitude – Cybercrime can cause injury and loss of life to a magnitude which cannot be envisaged.

2.2. Categories of People Involved in Cybercrime

Those involved in committing cyber-crimes are in three categories and they are[19]:

1. The Idealists (Teenager):These are mainly youngsters between the ages of ≤ 13 and <40 years who seek social recognition, they are usually not highly trained or skillful (Trend Micro and Interpol, 2017). Their actions are globally damaging but individually negligible.

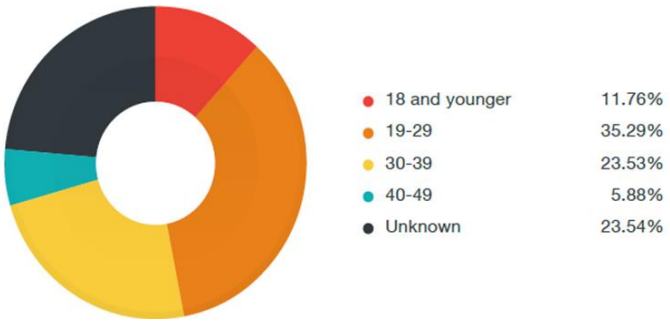

Figure 1: Cybercriminal age range (Trend Micro and Interpol, 2017)

2. The Greed – Motivated: This type of cyber-criminals is dangerous because they are usually unscrupulous and are ready to commit any type of crime if it brings money to them. They are usually very smart and organized and they know how to escape the law enforcement agencies.
3. The Cyber-Terrorists: They are the newest and most dangerous group. Their primary motive is not just money but also a specific cause they defend. They usually engage in sending threat mails, destroying data stored in mainly government information systems just to score their point. This disheartening issue is that they have no state frontiers; can operate from anywhere in the world and this makes it difficult for them to get caught.

2.3. Cybercrime Victims

Four levels of cybercrime victims have identified [20].They are:

1. The Gullible: These victims are easy to deceive. On a more obvious level, phishers are best able to fool such people into buying their scams or being drawn into legal traps. Spammers send multiple e-mail messages to harvested email addresses and the gullible fall prey to the contents of the email. Usually, older people are prone to being scammed as they are more trusting and helpful towards others.
2. Desperados and greedy people: Many internet users are desperate for easy ways to make money. Greedy and desperate people will always fall into the ploy of scammers by following the instructions in the emails which most others are likely to treat as junk. They are almost definitely being led to legal and financial entanglements out of which only the perpetrator will make profits. There are others who are attracted to advertisements related to improving one's physical image.
3. Unskilled and Inexperienced: These are victims who are ignorant of the fact that most people they meet online are criminals who hide under the shades of the internet to perpetrate different crimes. Lots of people have been raped by sex seeking individuals on the internet.
4. Unlucky people: These are victims who are just unlucky enough to be at the wrong place at the wrong time, in cyberspace that is,these categories of victims believe they are meeting legitimate business associates only to be deceived by the variants.

Millions of victims have been shortchanged in the United State, leading to loss of several millions of Dollars as shown in Figure 2.

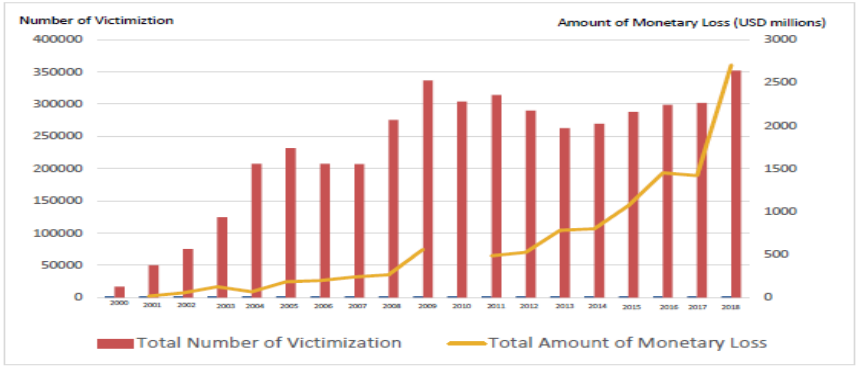

Figure 2: Cybercrime Victimization and monetary loss in the United State (2000-2018) Internet crime report (2023)

2.4. Causes of Cybercrime

Cybercrime aims rich people or rich organizations like casinos, banks, and financial firms where a terrific amount of money comes daily, and hackers can easily hack sensitive information. It is an easy way to make big money. Catching these criminals is difficult. The number of cybercrimes across the globe is increasing daily. Various laws are required to safeguard the use of computers against various vulnerabilities. The following are various reasons listed for the helplessness of computers:

1. Ability to store data in comparatively small space- one unique characteristic of a computer is that it can store your data in a considerable small space. This makes it easy for the criminal to steal data from the system and use it for their own profit.
2. Negligence- This is a characteristic of human conduct. While protecting the computer system we can make any negligence which makes it easy for the criminal to have access and control over your computer system.
3. Easy to access- Due to the complex technology used, it is difficult to protect a computer system from unauthorized access. Hackers can steal information that can fool biometric systems easily and bypass firewalls need to be used to get past many security systems.
4. Loss of evidence- The data with the crime can be destroyed easily. Loss of evidence has become a very common problem that paralyzes the system behind the investigation [21], [22].

2.5. Classes of Cybercrime, Nature of Offence, Attack Methods, and Tools

There are different classes of cybercrime perpetrated in different parts of the world with different nature of offence. Cybercrimes can be basically divided into 3 major categories namely: cybercrimes against persons, cybercrimes against property and cybercrimes against government [4], [23].

2.5.1. Cybercrimes Against Persons

1. Cyber Pornography: Itis the exploit of employing cyberspace to create, display, distribute, import, or publish pornography or obscene materials [24]. The rise of pornography websites offering photos, video clips and streaming media including live web cam access allowed greater access of pornography [23], [25].
2. Cyber stalking - Cyber stalking is the act of using the Internet or other electronic means such as e-mail, chat rooms etc. in harassing or threatening an individual, a group of individuals or an organization. It includes the making of false accusations or statements of fact (as in defamation), monitoring, making threats, identity theft, damage to data or equipment, the solicitation of minors for sex, or gathering information that may be used to harass. Cyber stalking is conducted by E-mail, Internet, and Computer. Social networking sites such as Facebook, Twitter, Google plus, Instagram and many more are media used for cyber stalking in the modern world [25], [26].
3. Financial Cyber Crimes: The financial cybercrime also known as economic crime in cyber world is a crime committed with the use computers and the internet, it includes cheating, credit card frauds, money laundering, forgery, online investment frauds distributing viruses, illegally downloading files, phishing, and pharming, and stealing personal information like bank account detailsetc. it is an act of cyber-deceptions and thefts[26].One potential reason that may explain this sudden rise in cybercrime is the rise in the volume of e-business, greater penetration of internet and e-commerce. The reason for low levels of awareness can be attributed to an extent, to the frequency of performing fraud risk assessment [25].

4. Phishing: Phishing is a form of social engineering, characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication, such as an e-mail or an instant message and Domain Name Server (DNS) manipulation[23],[25]. The term phishing arises from the use of increasingly sophisticated lures to "fish" for 'users' financial information and passwords[26]. The act of sending an e-mail to a user falsely claiming to be established legitimate enterprises in an attempt to scam the user into surrendering private information that will be used for identity theft[22].
5. Vishing: Vishing is also like phishing; it is the criminal practice of using social engineering and Voice over IP (VoIP) to gain access to private, personal, and financial information from the public for the purpose of financial reward. The term is a combination of "voice" and phishing. Vishing exploits the public's trust in landline telephone services, which have traditionally terminated in physical locations which are known to the telephone company and associated with a bill-payer. The victim is often unaware that VoIP allows for caller ID spoofing, inexpensive, complex automated systems, and anonymity for the bill payer. Vishing is typically used to steal credit card numbers or other information used in identity theft schemes from individuals [27].
6. Denial of Service (DOS) Attack: In this criminal act, the bandwidth of the victim's network or e-mail box is flooded or filled with spam mail depriving him of the services he is entitled to access or provide Short for denial-of-service attack, a type of attack on a network that is designed to bring the network to its knees by flooding it with useless traffic[25]. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

   A DoS attack can be perpetrated in several ways. There are three basic types of attack:
   - Consumption of computational resources such as bandwidth, disk space or CPU Time.
   - Disruption of configuration information, such as routing information.
   - Disruption of physical network components[28].

   A system may also be compromised with a Trojan, allowing the attacker to download a zombie agent[25], [29].

7. Data Diddling: Data diddling involves changing data prior or during input into a computer[30]. In other words, information is changed from the way it should be entered by a person typing in the data, a virus that changes data, the programmer of the database or application, or anyone else involved in the process of having information stored in a computer file. The culprit can be anyone involved in the process of creating; recording, encoding, examining, checking, converting, or transmitting data. This is one of the simplest methods of committing a computer-related crime, because it requires almost no computer skills whatsoever. Despite the ease of committing the crime, the cost can be considerable [31].
8. Salami Attacks: A salami attack is a series of minor data security attacks that together result in a larger attack. For example, a fraud activity in a bank, where an employee steals a small amount of funds from several accounts, can he consider a salami attack. Crimes involving salami attacks typically are difficult to detect and trace. These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely unnoticed. A bank employee inserts a program into the bank's servers, that deducts a small amount of money from the

account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month [31].

9. E-mail Bombing: An e-mail bomb is a form of net abuse consisting of sending huge volumes of e-mail to an address in an attempt to overflow the mailbox or overwhelms the server in other words, e-mail bombing refers to sending a large number of e-mails to the victim resulting in the victim's e-mail account (In case of Individual) or mail servers (in case of a company or an e-mail service provider) crashing. [30]. Mail bombing is sometimes accomplished by giving the victim's e-mail address to multiple spammers. E-mail spamming is a variant of bombing; it refers to sending e-mail to hundreds or thousands of users. E-mail spamming can be made worse if recipients reply to the e-mail, causing all the original addresses to receive the reply. It may also occur innocently, because of sending a message to mail lists and not realizing that the list explodes to thousands of users [31].
10. E-mail Spoofing: E-mail spoofing is a fraudulent e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source [22]. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message. By changing certain properties of the e-mail, such as the From, Return-Path and Reply-To fields (which can be found in the message header), ill-intentioned users can make the e-mail appear to be from someone other than the actual sender[32]. It is often associated with website spoofing which mimics an actual, well-known website but is run by another party either with fraudulent intentions or as a means of criticism of the organization's activities.

    E-mail spoofing is possible because Simple Mail Transfer Protocol (SMTP), the main protocol used in sending e-mail, does not include an authentication mechanism. Although an SMTP service extension allows an SMTP client to negotiate a security level with a mail server, this precaution is not often taken. If the precaution is not taken, anyone with the requisite knowledge can connect to the server and use it to send messages. To send spoofed e-mail, senders insert commands in headers that will alter message information. It is possible to send a message that appears to be from anyone, anywhere, saying whatever the sender wants it to say. Thus, someone could send spoofed e-mail that appears to be from you with a message that you didn't write [31].
11. Logic Bombs: A logic bomb is a programming code, inserted surreptitiously or intentionally, that is designed to execute (or "explode") under circumstances such as the lapse of a certain amount of time or the failure of a program user to respond to a program command. Software that is inherently malicious, such as viruses and worms, often contain logic bombs that execute a certain payload at a pre-defined time or when some other condition is met. A logic bomb, when "exploded," may be designed to display or print a spurious message, delete, or corrupt data, or have other undesirable effects. Logic bombs are event dependent programs. This implies that these programs are created to do something only when a certain event also known as a trigger event occurs. E.g., even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date, for example the Chernobyl virus[33].
12. Internet Time Theft: Theft of Internet hours refers to using somebody else's internet hours. Normally in these kinds of thefts of the Internet another person uses up surfing hours of the victim. This is done by gaining access to the login ID and the password[23].
13. Cybercrime with Mobile and Wireless Technology: As it is clear that at present the mobile is so developed that it becomes somewhat equivalent to personal computer, as we can do a lot of work on our mobile phones which were earlier possible on the computers only, such as surfing, sending e-mails etc. there is also increase in the services which were available on the mobile phones such as Mobile Banking, mobile wallet and other economic transaction done over the phone through internet which is also prone to

cybercrimes on the mobile. Due to the development in the mobile and wireless technology day by day, the commission of cybercrimes on the mobile is becoming a major threat along with other cybercrimes on the net [29].

2.5.2. Cybercrimes Against Property

1. Cyber Crime related to Intellectual Property Rights: Cybercrimes related intellectual property rights include [29]:

a. Domain Name violations: A domain name identifies a computer or a sub-Network of computers on the Internet. In other words, a domain name is a name-cum-address on the Internet of any person or entity. A computer or device that is attached to the Internet has an address popularly known as Domain name. With the advancement of internet communication and growing e-commerce and its future potential, domain names today are serving as trade names or brands and carry with them the goodwill and reputation of the websites they represent. Domain names being used as business identifiers have attained importance and legal sanctity as a means of differentiation between e-players since e-commerce is conducted in the absence of personal interaction or the opportunity to inspect the goods.

b. Software Piracy: universally, copyright subsists in the following classes of works, original literary, dramatic, and musical, artistic works, computer Programme, cinematograph films and sound recording etc. Some common methods of copyright infringement in relation to computer software are: reproducing the original owner's software and packaging of that software, so that purchasers are deliberately misled into believing that the product they are buying is genuine software; reproducing or 'burning' the original owner's software onto a blank CD, where no attempt is made to represent that the copy is genuine; reproducing a number of the owner's programme on a single CD- ROM, known as a 'compilation' CD. Another form of piracy that is assuming alarming shape in the information technology age is that of internet piracy when software is downloaded from the Internet or distributed via internet without the permission of the copyright owner.

c. Copyright and Digital Music: The rapid Increase of the internet has made it possible to transfer huge amounts of data of all types over the internet in a simple and cost-effective way. Further compression technology has also played a very important role in transferring data at fast speed and in less time.

d. Rights of reproduction and Database: A database is a collection of data in cyberspace, which is organized so that its contents can easily be accessed, managed, and updated. It is important to note that reproduction rights are equally affected if copyright material of the author is reproduced in an electronic form without his consent and made part of a database.

2. Data Theft - Data and information are valuable assets in this digital age. Business secrets, technical know-how, designs, music, films, books, personal data including usernames, credit card numbers and passwords, are some forms of property that drive the information economy. Money, time, effort, and creativity go into the creation and compilation of data and information. Stealing of data and information through hacking and other means is the most prevalent cybercrime [22], [34]. Data/information theft can be said to be committed in six ways; this includes:

- The first unauthorized copying of data / information;
- Making unauthorized subsequent copies.
- Making a copy and dishonestly sending the data/information online.
- Unauthorized copying of data / information in a floppy, C.D. or pen-drive and dishonestly taking it away.

- Stealing the computer itself.
- Data / Information already resides in a movable storage medium (floppy, C.D., or pen-drive) that is dishonestly taken away.

3. "Man in the Middle" (MitM) attack**:** Where an attacker establishes a position between the sender and recipient of electronic messages and intercepts them, perhaps changing them in transit. The sender and recipient believe they are communicating directly with one another. A MitM attack might be used in the military to confuse an enemy [25].

2.5.3. Cybercrimes Against Government

1. Cyber Terrorism: Cyber terrorism is the combination of cyberspace and terrorism. Cyber-terrorism is a criminal act perpetrated using computers and telecommunications capabilities [22]. Cyber-terrorism involves highly targeted efforts made with the intention of terrorism. It is an emerging threat that has the potential to cause serious damage. A prolonged and targeted terrorism campaign against a country has the potential to render it weak in the long run-in terms of it economic, finance and even psychology [35]. Cyber Terrorism becomes an international threat to the global population as through the terrorism, the terrorist is spreading false propaganda in line with political and religious ideologies [25].
2. Hacking/Cracking: Hacking a computer merely means gaining unlawful or unauthorized access to another's computer without permission or Cyber-trespass [26]. It is equivalent to phone-tapping. Hacking is identified amongst the most serious of all cybercrimes. It is said that hacking wears away the confidence of people in information technology and the Internet. A person who enjoys exploring computer systems is also a hacker. Hacking is also committed to damage the business of competitors and enemies. Hacking is also done to spy into others computer systems, steal information/data residing therein [25], introduction of computer viruses and contaminants and disruption of critical information infrastructure. Hacking is also used as a Weapon to commit other crimes such as cheating and misappropriation of funds electronically from the bank account of another [22]. Cracking is unauthorized access to a computer with the aim of causing damage. A Person who attains unauthorized access to a computer with the aim of causing damage is a cracker [36].

The European crime protection network-EUCPN observed that the most common cybercrime acts encountered by national police are as reflected in Figure 3 below with computer related fraud and forgery rated as highly common in the European, Americas, Asia, and Oceania as well as in Africa (EUCPN, 2015).

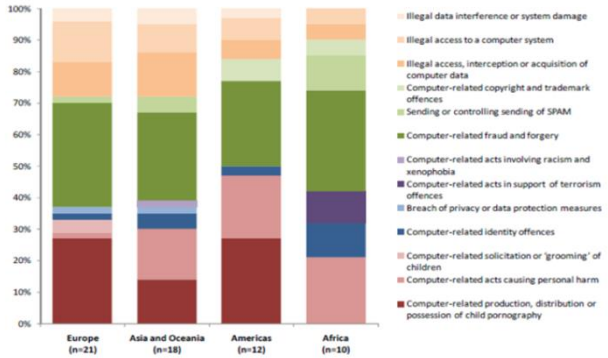

Figure 3: The most common cybercrime acts encountered by national police (EUCPN, 2015)

The cybercrime wing of Pakistan in 2020, received eighty-four thousand seven hundred and sixty-four (84,764) complaints. Most of the complaints were related to financial fraud (20,218); fake profile/identity theft (4,456); defamation (6006); hate speech (892); hacking (7,966); cyber harassment/threats (6,023) and cyber blackmail (3,447) [37]

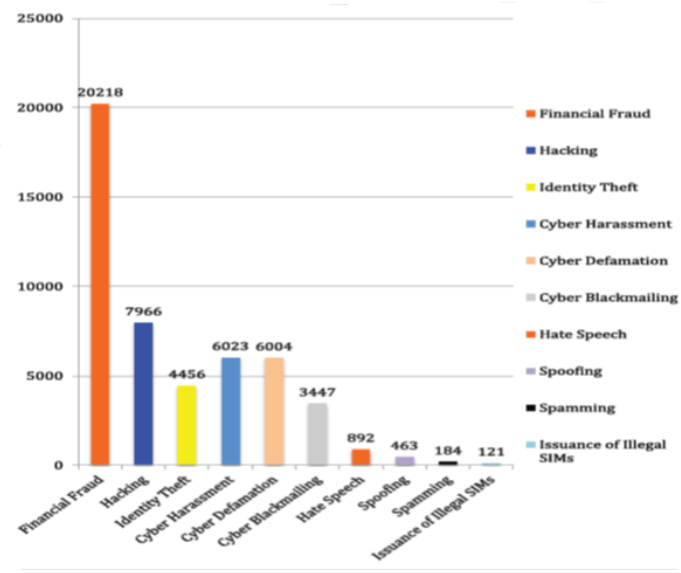

Figure 4: Cybercrime Complaints from Cybercrime Wing of Pakistan[37]

2.6. Cyber Security and Need to Develop a Cybersecurity Culture

The prevention and control of cybercrime and measures to enhance cyber security are mutually reinforcing. Cybersecurity is the act of protecting the confidentiality, integrity, and availability of computer data and systems to enhance security, resilience, reliability, and trust in ICT. This includes technical, procedural, and institutional measures for the protection against, mitigation of, and recovery from intentional attacks and non-intentional incidents affecting critical information infrastructure. An effective criminal justice response to offenses against ICT can also reinforce cybersecurity [38]. For cyber security to be efficient, the crime ought to be detected and a defense method is set up to mitigate the cybercrime. Legal policies are also tools for fighting cybercrimes. Cybersecurity includes among others the use of firewalls and antispyware, making sure operating system and anti-virus are up to date as well as the use of pop-up advertising blocker, use of strong passwords, secure wireless network, reputable websites and mobile applications, avoid clicking on unexpected or unfamiliar links[32].

Cyber security is primarily about people, processes, and technologies working together to encompass the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, etc.It plays an important role in the ongoing development of information technology, as well as Internet services. Enhancing cybersecurity and protecting critical information infrastructures are essential to each nation's security and economic well-being. Making the Internet safer (and protecting Internet users) has become integral to the development of new services as well as government policy. Deterring cybercrime is an integral component of a national cybersecurity and critical information infrastructure protection strategy. This includes the adoption of appropriate legislation against the misuse of ICTs for criminal or other purposes and activities intended to affect the integrity of national critical infrastructures. At the national level, this is a shared

responsibility requiring coordinated action related to prevention, preparation, response, and recovery from incidents on the part of government authorities, the private sector, and citizens. At the regional and international level, this entails cooperation and coordination with relevant partners. The formulation and implementation of a national framework and strategy for cybersecurity thus requires a comprehensive approach.

Protecting information is a crucial issue to take into consideration in developing the information society. At the crossroads of technological, legal, sociological, economic, and political fields, cybersecurity is an interdisciplinary domain by nature. Depending on the country, a national cybersecurity approach must reflect the vision, the culture and the civilization of a nation as well as meeting the specific security needs of the local context in which it is introduced. Because cybersecurity has a global dimension and deals with a large range of issues as:

1. ICT uses or misuses.
2. Technical measures.
3. Economic, legal, and political issues.

It is important to develop a general cybersecurity culture to raise the level of understanding of each member of the cybersecurity chain. A cybersecurity culture deals with key economic, legal, and social issues related to information security to contribute to helping countries get prepared to face issues and challenges linked to information and communication technologies (ICT) deployment, uses and misuses[39].

2.6.1. Cyber security Goals and Prevention Strategies

Cybersecurity strategies that are, the development of technical protection systems or the education of users to prevent them from becoming victims of cybercrime – can help to reduce the risk of cybercrime. The development and support of cybersecurity strategies are a vital element in the fight against cybercrime [40]. The following are the objectives of Cyber-security[41]:

1. To help people reduce the vulnerability of their Information and Communication Technology (ICT) systems and networks.
2. To help individuals and institutions develop and nurture a culture of cyber security.
3. To work collaboratively with public, private, and international entities to secure cyberspace.
4. To help understand the current trends in IT/cybercrime and develop effective solutions.
5. Availability.
6. Integrity, which may include authenticity and non-repudiation.
7. Confidentiality.

Precautious preventive attitude towards cybercrimes or cyber threats or cyber-attack cannot be overemphasized. If people are aware of these cybercrimes without the corresponding precaution, then something is wrong. In fact, it is necessary to raise awareness of cybercrime and to minimize its effects by ensuring that everyone has a wide and current knowledge. Some measures towards cybercrime include public key infrastructure, intrusion detectors, and prevention through firewalls, anti-virus, anti-spam, and anti-spyware. Measures against e-fraud are a horrendous task. The public can contribute to reducing cybercrime by reporting any person seen engaging in cybercrime to the law enforcement agent and the law enforcement agent should also help by allowing the law to take control in respect of the person's position in the society. Empowering the youths is another strategy that will help in reducing cybercrime in society.

Furthermore, the government should regularize engagement with industrial Training companies to develop strategies that can prevent and reduce cybercrime by making laws to terminate criminals that are caught engaging in any form of cybercrime. The implementation of this law will put fears to all students in Nigeria and make parents give reasonable advice to their children not to engage in any form of cybercrime [42]. Legal policies have been formulated internationally by many countries of the world these include among others: The Budapest convention on the control of cybercrime; the Nigerian Cybercrime Act, 2015; cybercrime laws of the United States of America; cybercrime Laws of Canada; cybercrime laws of the United Kingdom etc. Furthermore, to tactically establish cyber security, there should be a cybercrimes detection steps, crime detection tools as well as cybercrime defense methods.

2.6.2. Crime Detection Steps

The detectability of the crime is a very important step toward tackling cybercrimes and hence establishing cyber security tactics. The following crime detection steps can be followed:

1. Security of Evidence*:* Physical and electronic perishable evidence must be protected. Devices such as modems, call boxes, etc. must be connected to the telephone. In addition, if there is a LAN / Ethernet, wireless, infrared, and firmware connection, they must be identified and labeled in the same way. Fingerprints or other physical evidence should be retained on the keyboard, mouse, floppy disks, CDs and DVDs and other computer cognitions. Owners and / or users of passwords, passwords, usernames, and internet service providers should be identified.
2. Detection of Evidence: Computer systems, mobile phones, digital cameras, removable storage tools, portable USB sticks, memory cards, modems, network devices, printers, GPS receivers should be investigated.
3. Collection of Evidence: Image is receiving one-to-one copy of media, and it should be taken from devices. But, hardware, software, never work on the original evidence should not be made
4. Protection of Evidence: Electronic evidence must be packaged and transported with special collection, packaging, and transport system. Data must be strongly protected against possible damage to the magnetic field created by static electricity, magnetic, radio transmitters and the like.
5. Extracting Information from Evidence: In existing, deleted, unallocated space, file and word searching should be done. Web process, link file, print spool file should be examined. Signature analysis and hash analysis should be checked. Recycle bins, recovery bin, swap file, unused disk area, hidden partitions are carefully researched.

6. Reporting of Evidence: Information about the research organization, information about the incident should be written in the report. Also, the start date and end date of the study should be added to the report. Additionally, information on seized and reviewed electronic evidence should be included. Information about the hardware and software used in the study should be included in the report. The road followed and the tactics used in the research have an important place in the report. If the research has reached a conclusion, it should be noted how it reached it.
7. Detection of Criminals: The evidence must be secured. The evidence should be correctly identified. Appropriate image-taking programs should be used. Stored, hidden and deleted data should be available. The extracted data should be examined well. Reports should be prepared in an understandable and complete manner.

2.6.3. Crime Detection Tools

There are many methods to detect cybercrime. Apart from physical methods, there are also electronic details. The most important of these are hardware and software tools. A digital forensic investigation is conducted. Whether it is for an internal human resources case, an investigation into unauthorized access to a server, or if it just wants to learn a new skill, these suites and utilities help conduct memory forensic analysis, hard drive forensic analysis, forensic image exploration, forensic imaging, and mobile forensics. As such, they all provide the ability to bring back in-depth information about what's "under the hood" of a system. Some software and hardware tools used in forensic crimes are given below[25]:

1. **EnCase©:** Itis the global standard in digital investigation technology for forensic practitioners who need to conduct efficient, forensically-sound data collection and investigations using a repeatable and defensible process.
2. **Guidance Software:** This software delivers software for endpoint detection and response (EDR), risk and compliance management, e-Discovery, and corporate & law enforcement investigations.
3. **Enterprise:** Enterprise application software (EAS) is software used to satisfy the needs of an organization rather than individual users. Such organizations include businesses, schools, interest-based user groups, clubs, charities, and governments.
4. **Forensics:** The science of analyzing software source code or binary code to determine whether intellectual property infringement or theft occurred. It is the focus of lawsuits, trials, and settlements when companies are in dispute over issues involving software patents, copyrights, and trade secrets.
5. **Fastbloc©:** The FastBloc® SE (Software Edition) module is a pool of tools designed to control reads and writes to a drive attached to a computer through USB, FireWire, and SCSI connections. It enables the safe acquisition of subject media in Windows to an EnCase evidence file.

2.6.4. Cybercrime Defense Methods

There are many ways to detect crime when cybercrime is stumbled upon. But there are a lot of ways to protect those crimes before they are processed. The use of these methods' benefits individuals and institutions. Still, it is not enough. Attackers, Hackers are always ready to infiltrate networks. Changing settings will prevent easy access to hackers. IDS, Firewall and Honeypot are important technologies that prevent an attacker from entering the network etc.

1. Network Access Control (NAC): Network access control, also called network admission control, is a method to bolster the security, visibility, and access management of a propriety network. It restricts the availability of network resources to endpoint devices and users that comply with a defined security policy.In a nutshell, it is a system that implements security protocols for accessing a network or a device on a network.
2. Air gap: A system used for securing data flow between two networks.
3. Honeypot: This system is used to target the attackers, to see the types of attacks and to develop the essential defense mechanisms in the system, especially the devices that contain weakness.
4. Encryption systems: Encryption of both stored data and data flowing on the network.
5. Digital Signature: The digital signature allows proof of the identity and content of the sender.
6. Antivirus: This is useful for detecting malicious software by its signature and behavior
7. Data Loss Prevention (DLP): DLP ensures that critical data remains within certain limits. Prevents data leakage from hardware or network.

8. Shorthand: Information is not encrypted, but hidden in another information
9. Electromagnetic Safety: In the case of attacks for data playback, tapping devices are placed in the network paths and electromagnetic leakages are captured. In defenses, physical access to network paths is minimized, using tap detection methods reduces tapping attacks. Electromagnetic amplifiers or signal mixing can be used to prevent electromagnetic leakage.
10. Content Filtering Systems: Filtering by file type, web address, specific words, specific images, specific applications
11. Firewall: A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
12. Vulnerability Scanner: Nessus, Nmap, NetProbe programs should be used.
13. Intrusion Detection/Prevention Systems (IDS/IPS): Examining the packets passing over the network, Examining the packets coming to the device[25].

3. METHODOLOGY AND EXPECTED OUTCOME

This study was carried out purposely to explain clearly cyber-security tactics in mitigating cyber-crimes and provide adequate and sufficient ways of getting out of these problems in the present days of internet usage and applications. A mixed-methods approach involving questionnaires, interviews, observation, and media reports are also applied by targeting a diverse group of internet users, including bankers, students, directors, and university lecturers. Some researchers do analyze data to understand the causes and effects of cybercrime and propose recommendations for governments and corporations to improve cybersecurity measures. The expected outcomes include a deeper understanding of cyber threats, identification of key issues, actionable recommendations, potential policy impact, increased awareness, and a contribution to the knowledge base on cybercrime and cybersecurity.

4. LIMITATIONS AND RECOMMENDATIONS

While the field of cybersecurity has made significant strides, it is not without its limitations. Acknowledging these limitations is essential for driving future research and innovation in the right direction.

4.1. Limitations

1. Rapidly Evolving Threat Landscape: Cybercrimes are evolving at an unprecedented pace. Existing studies and methods may become quickly outdated as new attack vectors and techniques emerge. Researchers must continuously adapt and update their approaches to keep pace with cybercriminals.

2. Lack of Comprehensive Global Data: Cybercrimes often go unreported or underreported, leading to a lack of comprehensive global data. This hinders researchers' ability to fully understand the scope and impact of cybercrimes. Collaborative efforts among nations to share data on cyber incidents are needed.
3. Privacy Concerns: Many cybersecurity measures involve monitoring and data collection, raising legitimate privacy concerns. Striking the right balance between security and individual privacy is an ongoing challenge that requires careful consideration in future research.
4. Resource Constraints: Small and medium-sized organizations often lack the resources to implement advanced cybersecurity measures. Research should focus on cost-effective solutions that cater to the specific needs of these entities.
5. Attribution Challenges: Attributing cybercrimes to specific individuals or entities can be exceptionally challenging, particularly when nation-states are involved. Developing robust techniques for cybercrime attribution remains a complex task.

4.2. Recommendations

1. Advanced Threat Intelligence: While we have discussed various cybersecurity tools and methods, there is a growing need for advanced threat intelligence. Researchers should focus on developing more sophisticated threat detection systems that can proactively identify emerging cyber threats. Utilizing machine learning, artificial intelligence, and big data analytics to analyze vast datasets for anomaly detection and early threat identification is a promising avenue for future research.

2. Human-Centric Cybersecurity: Understanding human behavior in cyberspace is crucial. Future research should explore the psychology of cybercriminals and the decision-making processes of both victims and potential attackers. This knowledge can inform the development of effective awareness campaigns and user-friendly security interfaces. Additionally, research on the impact of cybersecurity education and training programs on reducing cybercrimes is essential.
3. Legal and Ethical Frameworks: Given the global nature of cybercrimes, there is a need for international collaboration on legal and ethical frameworks. Future research should focus on analyzing existing cybersecurity laws and regulations, identifying gaps, and proposing standardized international guidelines for addressing cybercrimes. This includes considerations for data privacy, extradition of cybercriminals, and jurisdictional issues.
4. Cyber-Physical Systems Security: As our world becomes increasingly interconnected through the Internet of Things (IoT) and cyber-physical systems, there is a pressing need for research into securing these systems. Investigating vulnerabilities in critical infrastructure such as smart cities, healthcare, and transportation systems is crucial to preventing potentially catastrophic cyber-attacks.
5. Cybersecurity Metrics: Developing standardized metrics for evaluating the effectiveness of cybersecurity measures is an ongoing challenge. Researchers should work on defining key performance indicators (KPIs) that organizations and governments can use to assess their cybersecurity posture. This includes metrics related to incident response times, threat detection rates, and the overall resilience of systems.
6. Cybersecurity Education and Workforce Development: The shortage of skilled cybersecurity professionals is a persistent issue. Future research should focus on innovative approaches to cybersecurity education and workforce development. This includes online training programs, gamified learning experiences, and strategies for attracting diverse talent to the field.

5. CONCLUSION

The global surge in cybercrime requires immediate attention and coordinated efforts. Cybersecurity is not solely the responsibility of governments but also of organizations and individuals. By fostering a culture of cybersecurity, embracing comprehensive strategies, and remaining vigilant in the face of evolving threats, we can collectively mitigate cybercrimes and promote a secure digital ecosystem. The path forward demands unity, adaptability, and unwavering commitment to safeguarding our interconnected world.The digital era has ushered in unparalleled connectivity and convenience, but it has also exposed societies worldwide to the insidious threat of cybercrimes. As this review underscores, cyber-attacks and cyber-threats are not bound by geographical borders; they are global problems that demand comprehensive solutions. The implications of cybercrimes, from financial losses to critical infrastructure vulnerabilities, necessitate a concerted effort from all stakeholders to combat this pervasive menace effectively. Through a meticulous examination of the characteristics, victims, causes, and categories of cybercrimes, this review has provided valuable insights into the multifaceted nature of the challenge. We have explored the methods and tools employed by cybercriminals, shedding light on the ever-evolving landscape of cyber threats.

In tandem with our exploration of cybercrimes, this study emphasized the pivotal role of cybersecurity in defending against digital threats. The development of a cybersecurity culture, encompassing individuals, organizations, and governments, is imperative in safeguarding our digital realm. Effective prevention strategies, bolstered by robust detection and defense mechanisms, must be woven into the fabric of our interconnected society.

Furthermore, this review has proposed a methodology for assessing the effectiveness of various cyber-security tactics in mitigating cybercrimes. This methodology, rooted in empirical research and real-world implementation, holds promise in shaping more targeted and impactful strategies to counter cyber threats.

The expected outcome of this comprehensive endeavor is not only the mitigation of cybercrimes but also the fortification of self-protection, organizational resilience, and government system security. By understanding the intricacies of cyber threats and the nuances of effective cybersecurity tactics, we are better equipped to confront the challenges of the digital age.

In closing, the battle against cybercrimes is ongoing, and it demands vigilance, collaboration, and innovation. With the concerted efforts of governments, businesses, and individuals, we can aspire to create a digital environment that is secure, resilient, and conducive to progress in the modern age. Our collective commitment to cybersecurity will ultimately determine the safety and prosperity of our interconnected world.

REFERENCES

[1] O. Adekunle *et al.*, “A Review of Cybersecurity as an Effective Tool for Fighting Identity Theft across United States,” *Int. J. Cybern. Inform.*, vol. 12, no. 5, pp. 31–42, Aug. 2023, doi: 10.5121/ijci.2023.120504.

[2] O. P. Efijemue, C. Obunadike, E. Taiwo, S. Kizor-Akaraiwe, C. Odooh, and S. Olisah, “Addressing Insider Threats: Cybersecurity Measures to Prevent Fraud in the US Banking Industry (Unpublished work).” 2023.

[3] U. V. Awhefeada and O. O. Bernice, “Appraising the Laws Governing the Control of Cybercrime in Nigeria,” *J. LAW Crim. JUSTICE*, vol. 8, no. 1, 2020, doi: 10.15640/jlcj.v8n1a3.

[4] A. N. Ayofe and O. Oluwaseyifunmitan, “Approach To Solving Cybercrime And Cybersecurity.” arXiv, Aug. 01, 2009. Accessed: Sep. 06, 2023. [Online]. Available: http://arxiv.org/abs/0908.0099

[5] R. K. Chaubey, *An Introduction to Cyber Crime and Cyber law*. Kamal Law House, 2012.
[6] A. Okutan and Y. Çebi, "A Framework for Cyber Crime Investigation," *Procedia Comput. Sci.*, vol. 158, pp. 287–294, 2019, doi: 10.1016/j.procs.2019.09.054.
[7] S. Tan, P. Xie, J. M. Guerrero, J. C. Vasquez, Y. Li, and X. Guo, "Attack detection design for dc microgrid using eigenvalue assignment approach," *Energy Rep.*, vol. 7, pp. 469–476, Apr. 2021, doi: 10.1016/j.egyr.2021.01.045.
[8] M. A. Judge, A. Manzoor, C. Maple, J. J. P. C. Rodrigues, and S. U. Islam, "Price-based demand response for household load management with interval uncertainty," *Energy Rep.*, vol. 7, pp. 8493–8504, Nov. 2021, doi: 10.1016/j.egyr.2021.02.064.
[9] G. Aghajani and N. Ghadimi, "Multi-objective energy management in a micro-grid," *Energy Rep.*, vol. 4, pp. 218–225, Nov. 2018, doi: 10.1016/j.egyr.2017.10.002.
[10] H. Akhavan-Hejazi and H. Mohsenian-Rad, "Power systems big data analytics: An assessment of paradigm shift barriers and prospects," *Energy Rep.*, vol. 4, pp. 91–100, Nov. 2018, doi: 10.1016/j.egyr.2017.11.002.
[11] I. Priyadarshini, R. Kumar, R. Sharma, P. K. Singh, and S. C. Satapathy, "Identifying cyber insecurities in trustworthy space and energy sector for smart grids," *Comput. Electr. Eng.*, vol. 93, p. 107204, Jul. 2021, doi: 10.1016/j.compeleceng.2021.107204.
[12] M. Amir and T. Givargis, "Pareto optimal design space exploration of cyber-physical systems," *Internet Things*, vol. 12, p. 100308, Dec. 2020, doi: 10.1016/j.iot.2020.100308.
[13] N. Li, C. Tsigkanos, Z. Jin, Z. Hu, and C. Ghezzi, "Early validation of cyber–physical space systems via multi-concerns integration," *J. Syst. Softw.*, vol. 170, p. 110742, Dec. 2020, doi: 10.1016/j.jss.2020.110742.
[14] K. S. Niraja and S. Srinivasa Rao, "WITHDRAWN: A hybrid algorithm design for near real time detection cyber attacks from compromised devices to enhance IoT security," *Mater. Today Proc.*, p. S2214785321008488, Mar. 2021, doi: 10.1016/j.matpr.2021.01.751.
[15] I. H. Sarker, "Machine Learning: Algorithms, Real-World Applications and Research Directions," *SN Comput. Sci.*, vol. 2, no. 3, p. 160, May 2021, doi: 10.1007/s42979-021-00592-x.
[16] J. Cao, Da Ding, J. Liu, E. Tian, S. Hu, and X. Xie, "Hybrid-triggered-based security controller design for networked control system under multiple cyber attacks," *Inf. Sci.*, vol. 548, pp. 69–84, Feb. 2021, doi: 10.1016/j.ins.2020.09.046.
[17] S. Gupta Bhol, J. Mohanty, and P. Kumar Pattnaik, "Taxonomy of cyber security metrics to measure strength of cyber security," *Mater. Today Proc.*, vol. 80, pp. 2274–2279, 2023, doi: 10.1016/j.matpr.2021.06.228.
[18] B. Alhayani, S. T. Abbas, D. Z. Khutar, and H. J. Mohammed, "WITHDRAWN: Best ways computation intelligent of face cyber attacks," *Mater. Today Proc.*, p. S2214785321016989, Mar. 2021, doi: 10.1016/j.matpr.2021.02.557.
[19] A. N. Ayofe and O. Oluwaseyifunmitan, "Towards Ameliorating Cybercrime and Cybersecurity.," *Int. J. Comput. Sci. Inf. Secur. IJCSIS*, vol. Vol. 3(1)., 2009.
[20] J. Aghatise, "Cybercrime definition," *Cyber Crime*, Jun. 2006.
[21] F. Begum, "Beware of Cyber Crime with Awareness - A Review.," *Int. J. Sci. Healthc. Res.*, no. Vol.4(3), pp. 135–138, 2019.
[22] H. M. Khadas, "The Causes of Cyber Crime," *Int. J. Innov. Sci. Res. Technol.*, vol. 5, no. 8, pp. 476–478, Aug. 2020, doi: 10.38124/IJISRT20AUG432.
[23] A. Sarmah, R. Sarmah, and A. J. Baurah, "A Brief Study on Cyber Crime and Cyber Law's of India.," *Int. Res. J. Eng. Technol. IRJET*, vol. Vol. 04, pp. 1633–1641, 2017.
[24] L. Gorman and D. Maclean, *Media and Society in Twentieth Century*. Blackwell publishing., 2003.
[25] A. Okutan and Y. Çebi, "A Framework for Cyber Crime Investigation," *Procedia Comput. Sci.*, vol. 158, pp. 287–294, Jan. 2019, doi: 10.1016/j.procs.2019.09.054.
[26] H. Jahankhani, A. Al-Nemrat, and A. Hosseinian-Far, "Cyber crime Classification and Characteristics," 2014, pp. 149–164. doi: 10.1016/B978-0-12-800743-3.00012-8.
[27] S. Cobb, "Advancing Accurate and Objective Cybercrime Metrics," Feb. 2020.
[28] E. Ajayi, "Challenges to enforcement of cyber-crimes laws and policy," *J. Internet Inf. Syst.*, vol. 6, pp. 1–12, Aug. 2016, doi: 10.5897/JIIS2015.0089.
[29] A. Yeboah-Ofori, J.-D. Abdulai, and F. Katsriku, "Cybercrime and Risks for Cyber Physical Systems 2019," Dec. 2019.
[30] K. Sundarraj and K. P. g.v, *Cyber Crime – Attacks, Types and Protection*. 2015. doi: 10.13140/RG.2.2.32794.44481.

[31] K. Arun, K. Deepan, K. S. Thinesh, and S. Vignesh, "Crimes: Kinds and Types.," *Int. J. Res. Dev. IJRD*, vol. Vol 4, no. 2, pp. 68–71, 2019.
[32] M. M. L. Prasanthi, "Cyber Crime: Prevention & Detection," *IJARCCE*, pp. 45–48, Mar. 2015, doi: 10.17148/IJARCCE.2015.4311.
[33] S. Ogunlere, "Cyber Crimes and Cyber Laws in Nigeria," Jan. 2013.
[34] V. Sood, "Cyber Crimes, Electronic Evidence & Investigation – Legal Issues," NABHI Publications, New Delhi, 2010, pp. 137–139.
[35] P. Magutu, G. Ondimu, and C. Ipu, "Effects of Cybercrime on State Security:Types, Impact and Mitigations with the Fiber Optic Deployment In Kenya," *J. Inf. Assur. Cybersecurity*, pp. 1–20, Jan. 2011, doi: 10.5171/2011.618585.
[36] S. Sharma and V. Sharma, "Cyber Crime analysis on Social Media," *BSSS J. Comput.*, May 2020, doi: 10.51767/jc1104.
[37] E. Sadiq, "Cybercrimes risks, Prevention and Legal Remedies Guidelines for Cyber Users. Cyber Crime Wing Federal Investigation Agency, Ministry of Interior, Government of Pakistan.," 2020.
[38] "Global Project on Cybercrime. Capacity building on cybercrime Discussion paper.," *Data Protection and Cybercrime Division, Council of Europe, Strasbourg.*, Nov. 2013. www.coe.int/cybercrime
[39] S. Ghernaouti-Helie, "Information Security for Economic and Social Development. UNESCAP," 2008. www.unescap.org/icstd/policy/
[40] M. Gercke, "Understanding cybercrime: Phenomena, challenges and legal response.," TU Telecommunication Development Bureau, 2012.
[41] F. Ibikunle, "Approach to cyber security issues in nigeria: Challenges and solution," *Int. J. Cogn. Res. Sci. Eng. Educ.*, vol. 1, Jun. 2013.
[42] I. D. Igba, E. C. Igba, A. S. Nwambam, S. C. Nnamani, E. U. Egbe, and J. V. Ogodo, "Cybercrime among University Undergraduates: Implications on their Academic Achievement.," *Nternational J. Appl. Eng. Res.*, vol. Volume 13, no. 2, pp. 1144–1154, 2018.

AUTHORS

Adeniyi Phillips is a highly skilled professional with a passion for leveraging data to drive innovation and improve business outcomes. Holding a master's degree in computer science, he has established himself as a proficient data engineer with a keen understanding of cutting-edge technologies and their applications.

Ibraheem Ojelade holds an M.Sc. in Computer Science with a concentration in Data Management and Analysis. With a strong background in this field, he has excelled in his career as a Cloud Solution Architect, leveraging his expertise to design and implement cutting-edge cloud solutions. Ibraheem's dedication to data-driven decision-making is a driving force behind his professional achievements.

Esther Taiwo, a dedicated professional in the IT and data field holds a Bachelor of Science (BSc.) degree in Mathematics and Statistics. Currently, she is pursuing a Master of Science (MSc.) degree in Computer Science and Quantitative Methods. Esther's passion lies in utilizing data to foster innovation and enhance solutions that positively impact our world.

Callistus Obunadike holds three Master of Science degrees in geology, mining engineering, and computer science. Callistus combines his extensive knowledge of geosciences with data science. Callistus has a passion for applying machine learning algorithms to improve geological processes and predicting of future events.

Kunle Oloyede has a B.Sc. in Geography and M.Sc. in Geographic Information System and is currently pursuing his second M.Sc. degree in Computer Science & Quantitative Methods. With 7 years of experience in the IT space. Kunle is passionate about using data to forecast and improve organizational metrics.