Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

# A Descriptive Study on the Impact of Cybercrime and Possible Measures to Curtail its Spread Worldwide

Mohammed I. Alghamdi
Department of Computer Science,
Al-Baha University, Al-Baha City, Kingdom of Saudi Arabia

***Abstract*— The 21st century has been characterized by massive technological innovations that have shaped the way people interact. The social, political, and economic dimensions of human life are facilitated by a digital age that has encompassed the whole world. Universally, there has been a rapid rise in the use of computers and electronic gadgets. These developments have led to significant growth in criminality, especially in cyberspace. Cybercrimes have grown progressively with perpetrators developing newer and sophisticated techniques every day. Despite the measures taken by the international community to combat the vice and mitigate its effects, cybercrimes have continued to rise alarmingly across the world. According to Cyber Security Breaches Survey of 2018, 40% of businesses worldwide have been a victim of cybercrime. The research projects that up to six trillion dollars per year could be lost in the hands of cybercriminals. This study examines the various forms of cybercrimes worldwide and why there is a rapid increase in such activities. The study also recommends various measures and recommendations to curtail cybercrime incidents. They include the introduction of a concrete legal framework, establishment, and strengthening of cybercrime law enforcement organizations complete with high technology monitoring devices and modern infrastructure.**

***Keywords*— *Cybercrime, Cyberspace, computer crime, hacktivists, hacking, DoS, Phishing, Cyberattacks.***

## 1. INTRODUCTION

***Background of the Study:***

Alsmadi, (2019) acknowledges that there is no clear definition of cybercrime in the academic milieu. Some quotas have referred to it as “electronic crime,” “computer crime," and "computer-related crime." There have been different classifications of cybercrime. Krausz & Walker, (2013) argue that cybercrime is an offense committed when the computer is the main instrument of crime or when the computer is targeted for the crime. Even though such a classification is unsaleable for this study, its essential to the understanding of the term.

Cybercrimes can be categorized into Type I and Type II depending on the intensity of the crimes (Moore, 2016). Type I refers to cybercrime activities that are technical, for example, hacking. On the other hand, Type II relies on human interaction rather than technology. Criminal activities such as identity theft, credit card fraud, harassment, stalking, and threatening behaviors have been known to be traditional crimes that are now easier to pursue on computers. Such crimes can exist independently without computer technology.

However, there exists another range of offenses that are utterly cyber dependent. This means that they cannot exist without computer technology. Criminals have found it easier to destroy businesses through inflicting harm to their databases. Notably, in 2015, there was a massive cyberattack that targeted individuals and businesses through ransomware named Cryptowall version 3.0(Alazab & Broadhurst, 2015). Using the kit, criminals searched, encrypted documents on victims' computers before asking them to pay thousands of dollars if they ever needed their originals back. It was estimated that this attack caused approximately 325 million dollars in damage. Over the last two decades, unscrupulous cyber-tech users have continued to commit cyber dependent and independent crimes in sophisticated and unprecedented manners. Cyber technology has been used to commit the highest atrocities in world systems such as electoral fraud and treasonable offenses. So high is the level of sophistication that murders have been executed through the cyberspace. For example, in January 2002, the United States recorded its first cybercrime murder whereby the offender hired a computer guru to alter prescriptions of his rival patient through hacking of the hospital’s computer system (Krausz & Walker, 2013). Consequently, this resulted in a wrongful prescription that led to the fatality of a patient in the hands of an innocent nurse.

The evolution of Information Technology (IT) has brought about successful communication through the internet, thriving businesses, and global interaction through social media platforms. However, these developments are threatened by criminal activities in the world's cyberspace. Computer crime has become a major global challenge and continues to be a major concern for international security. With the arrival of fast internet and the advent of new technology, cybercriminals have the chance to infiltrate individuals and businesses via their computer systems. For example, Interpol reports show that there are millions of cases and attempt to illegally access and interfere with other people's files. Every day, there are new developments in malicious software and viruses that are developed across the world. Approximately 400 million people are affected by compromised computer systems every day (DCIMS, 2019).

Cybercrime has led to significant damage not only for individuals but also for businesses whereby it causes employment disruptions and reduced trust for a company’s online activities. It is estimated that the damages worldwide accrue to over 2.8 billion dollars every year. Data breaches have become a norm for big social media companies such as

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

*Facebook* and *TikTok.* Data breach refers to unlawful gaining of information by unauthorized persons that often compromises security or integrity personal information. In 2020, a US senate committee released reports showing that a Chinese firm was in breach of privacy regulations as it's a database consisting of customer records that was shared with third parties. The responsibilities of addressing cybercrime activities lie in individual countries which should ensure that they protect and empower institutions to create an organized mitigation campaign that monitors what happens in cyberspace. Cybercriminals all over the world can only be brought to justice if there are available and adequate laws to combat the vice. Further, there is a need to engage in proactive strategies in observing and averting cybercrime attacks (Howard & Gulyas, 2014).

***Statement of the Problem:***

The implications of cybercrime on international security have risen from the manner of technology use by individuals and a set of people known as cybercriminals. These people have mastered the art of computer networks to their advantage. Hidden behind computer monitors they commit atrocities such as data theft, hacking, espionage, and virus scattering. Most countries of the world have highly developed internet networks. Recently, there have been breakthroughs in the field as major telecommunication companies sprint to introduce 5G networks to the globe. However, there are fears that this network will also be used by criminals to gain access to victims' organization network systems causing destruction and losses across all continents. Numerous techniques are being used by criminals of the 21st century to target sensitive data, recording the highest levels of fraud in history. At the hands of cybercriminals, victims lose private information, money, and even their characters. This study seeks to explore the forms of cybercrimes that have rocked the world in the new age. Additionally, the study seeks to examine the impact of such activities on international security and correspondingly, the measures to curb the situation internationally.

***1) Research Questions***

This study aims to answer the following questions

1) What are the various forms of cybercrimes adopted by criminals in recent days?
2) How has cybercriminal activity impacted the world and international security?
3) What are the factors facilitating the rapid increase of cybercrime?
4) Which measures can the international community take up to curb the situation?

***2)*** *Objectives of the Study*

i) This study aims at identifying the various forms of cybercrimes adopted by criminals in recent days
ii) Its seeks to examine how cybercriminal activity has impacted the world and the international security
iii) This research aims at discussing the major factors facilitating the rapid increase of cybercrime
iv) It seeks to establish appropriate measures by the international community to curb the situation

## 2. LITERATURE REVIEW

***a) The Cybercrime concept***

There has been numerous scholarly work in the past that has aimed at defining cybercrime through different phases of history and under various circumstances. The international journal of Science and Information security defines cybercrime as harmful acts that are committed from or against a computer or a network. Another definition by Bernik, (2014) highlights cybercrime as illegal behavior that is carried out by electronic operations and seeks to target computer systems and data processed by the devices. From these definitions, it is clear that cybercrime occurs within a virtual space under which information concerning people objects, events, or facts fashioned in mathematical symbols and transferred through local and worldwide networks. Among the first people to write about computer crime was Donn Parker who was was considered the first national expert on computer security in the United States. Parker defined it as computer abuse saying it involves intentional acts in which victim (s) suffer a loss while others make a profit. However, past occurrences have proven that perpetrators may not always be after profit. Notably, there exists a faction of cybercriminals known as "hacktivists". These are people who protest organizations' policies and practices. For example in 2010 the Anonymous hacktivist group attacked Mastercard, Visa, and Paypal in retribution for stopping donations to WikiLeaks (Grispos, 2019).

The Foreign affairs and International Trade of Canada notes that cybercrime is a criminal activity committed using computers and computer networks. This implies that the facilitation of traditional crimes using computers also falls under cybercrime. Examples of such traditional crime include child pornography and online fraud. Some crimes that may cover indirect use of computers to carry out crime include communication and data storage and may be considered as a computer-assisted crime. Australian laws acknowledge electronic crime as one that is conducted via computer, targets cyber tech, or uses it to store illegal material. This definition concurs with that of Wall, (2007) who divides cybercrime into offenses that target computers and crime that's enabled by computers. The Cybercrime Act 2001 of Australia terms cybercrime as a crime that inflicts harm to computer data and systems. However, in the United Arab Emirates, their legislation is adjusted to include offenses against computer data systems and computer- associated crimes such as forgery, fraud, threats, and money laundering.

The United States laws define computer crime as a crime that utilizes or targets computer networks generally referring to viruses, worms, and DoS attacks. The UK also has a similar perception of criminal activity. However, the United Kingdom Computer Misuse Act stipulates that the use of networked computers, telephones, or internet technology to conduct or facilitate crime is tantamount to cybercrime. The development of technology has subsequently led to the development of the term computer crime. The organization for Economic and Development (OECD) in coherence with the United Nations member states declared crimes related to computer use as both unlawful and unethical. Likewise, they also declared the habitual processing and spread of data without the owner's permission as illegal behavior. The

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

council of Europe's recommendations on Criminal Procedural Law indicates that IT offenses constitute an unlawful crime and declared that investigating powers should have a right to information that's processed or conveyed via computer systems.

There exist disparities in the description of cybercrime at the international level. Organizations such as the Council of Europe Cybercrime Convention, The League of Arab States Convention, and the Draft African Union conventions have attempted to define cybercrime even though their definitions are not accepted worldwide (Alazab & Broadhurst, 2015). The Commonwealth of Independent States Agreement uses the term "computer information" to describe computer crime-related offenses. On the other hand, the Shanghai Cooperation Organization Agreement suggests the term information offenses as the exploitation of information property impacting it for illegal purposes. The term cybercrime or computer crime is interpreted differently by various factions and jurisdictions across the world. Consequently, not all cybercrime is treated or criminalized similarly in different states. This means that a particular cybercrime could be a crime in one country but fail to meet the criminal threshold in another. This research paper will use the term computer crime and cybercrime interchangeably to denote crime that utilizes or targets computer data and systems for committing an illegal activity.

***b) Efforts to counter Computer crime by International organizations***

There have been efforts to combat cybercrime by various organizations such as the United Nations, the European Union, the Council of Europe, and Interpol. Among the goals of the United Nations is to support economic development and the upholding of international law and security. The UN adopted *The United Nations Convention against Transnational Organized Crime* in order to fight against organized crime. The UN has in the past produced reports on measures to curb high technology and computer-related crime. During the 11$^{th}$ UN congress on crime prevention, a discussion workshop was held to discuss potential collaboration between nations and the private sector to battle cybercrime. the committee recommended that the United Nations should aid member countries in cybercrime management; that it should provide training to other member states and also enhance international law enforcement.

The UN also contributed to the fight against cybercrime by founding the International Telecommunication Union which coordinates the international use of telecommunication whilst improving its infrastructure (Boes & Leukfeldt, 2016). Part of the goals of the ITU is to solve global issues like strengthening cybersecurity. In 2002, the ITU developed sample legislation guidelines to enable member countries to develop harmonized cybercrime laws. The European Union member countries are cohesively working together to combat cybercrime. Cooperation is enhanced between member countries through the European Union Commission and its council. The EU adopted a policy that allows the adoption of substantive legislative grounds to deal with cybercrime activities and the hiring of well-trained law enforcement personnel (Boes & Leukfeldt, 2016). Its researchers have continued to work together with scholars and IT specialists to advance standards for cybercrime investigations. Similarly, the CoE is engaged in activities that endeavor to curb computer crime. Since 2001, the CoE requires that its members have cybercrime laws and appropriate law enforcement authorities. The G8 has also focused on combatting transnational organized crime. Through its subgroup on High Tech crime, it advises and assists member countries on computer crime. additionally, the subgroup offers recommendations for its member countries to enact legislation that fortifies them against high technology criminal activities. On the other hand, Interpol, an organization that facilitates police officers across the world contributes significantly to the battle against cybercrime. Police officers from Interpol member countries can access each other's databases. Such collaboration facilitates the organization to fight major criminal activities including cybercrime (Alsmadi, 2019). Collaboration between Interpol and private entities such as Microsoft enables it to tackle and neutralize impending threats.

## 3. METHODOLOGY

This study uses the qualitative method that intends to collect comparable records on cybercrime and computer crime activities across the world. The study was conducted purposively to elaborate and provide more knowledge on the concept of cybercrime and cybersecurity. The research utilized instruments such as questionnaires, virtual interviews, and reports from radio and electronic media. The author conducted a survey covering a variety of internet users among them students, business persons, and bankers. The impact of cybercrime on societies across the world is immense and consequential. There also exists an upward trend in the cases of cybercrime activities across the world. Currently, there is a disconnect in the manner the world has handled this form of criminal activity. Cybercriminals have taken advantage of this gap to undermine global efforts. Undoubtedly, this vice has been deleterious to economies costing countries millions of dollars every year. Research efforts must be boosted towards understanding criminal activity globally through international initiatives, legislation, and procedures.

## 4. DATA ANALYSIS

### *B. Forms of cyber crimes*

#### *1) Hacking*

Gupta (2019) has defined hacking as gaining unauthorized access or compromising systems to get access. While hacking may be characterized as criminal in some countries, there is a need for information security experts with the knowledge of hacking to counter cyber threats in the fields of business, politics, social media, and national security. There are three main types of hackers, according to Gupta, (2019). The first type of hackers is the white hat hacker who defends systems from other attackers. They are authorized, and they are mainly known for the provision of security. The second type is the black hat hacker who works without authorization. This caliber of hackers are also known as malicious hackers, and they act without the permission of any kind. The third type is the Grey hat hacker, whose sword is double-edged. They can be both offensive and defensive, depending on the benefits.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

The term grey hackers can also mean hackers whose intention is to warn others of their vulnerability even if they sometimes do it illegally.

Hacking has four main stages, namely reconnaissance, scanning, gaining of access, and maintenance of access (Grispos, 2019). In the first stage, the hacker attempts to find information about his target either actively or passively. The attacker then proceeds to seek much more information about the target by scanning or conducting various assessments to get sensitive information about the target. The third phase is gaining access, whereby the attacker performs the hack. The attacker takes advantage and performs an exploits vulnerability to gain access. In the next phase, the attacker installs backdoors or Trojans to keep up access. Lastly, they delete logs and other details to avoid getting caught. The *Lizard Squad* is a black-hat-type of a hacker group that has been identified as an example for this study. The group's history and activity can be traced back to 2014 when it attacked the gaming platform of Xbox and PlayStation, sharing hosting with them. The group also conducted various detrimental hacks including taking down the internet in North Korea, attacking of PlayStation network, and an attack on Destiny in which they changed the company's logo on their webpage (Grimes, 2017).

***2) Computer Fraud***

This form of cybercrime is also known as "phishing." It involves situations in which perpetrators pose as representatives of an organization, aiming directly at bank customers (Doyle, 2011). Older communication tools like telephones and postal mail were previously the instruments used to scam and defraud people. Today, modern tools like email, text messages, and social media chats have replaced traditional methods and are now used to commit cybercrime. Fraudsters impersonate legitimate senders such as bankers and they can get away with essential credentials such as usernames, passwords, and account numbers. In this form of cybercrime, the fraudsters manually target recipients through texts that are sent out in bulk with the sender hoping to ploy unsuspecting victims into sharing their personal data. Cybercriminals may also act to be promoting deals that appear too good to be true. They may pretend to offer victims "investment" opportunities upon which after some time they dazzle away with victims' funds.

According to the 2019 Verizon Data Breach Investigations Report, nearly a third of all breaches involved this form of computer fraud. Casey (2011) attributes the skyrocketing of phishing cases to well- modeled ideal tools that fraudsters and perpetrators use even with little computer- software knowledge. In 2016, phishing attacks succeeded to get critical passwords from Hillary Clinton's campaign team in the run-up to the general election. In the same year, some employees from the University of Kansas reportedly lost their pay after they gave away paycheck deposit information to phishers. Grispos,( 2019) notes that the availability of phishing kits has made it possible for cybercriminals to launch phishing attacks even though some of them have very little knowledge of the subject. These kits are made available on the dark web, a shady and dangerous platform that is often used for conducting illegal undertakings.

***3) Denial of Service attacks***

These attacks involve large amounts of traffic being sent to a host network rendering it inaccessible to normal users. These attacks act to prevent people from connecting to a network or a computer. Subsequently, these attacks harness numerous computers across the web to send data to a victim's computer leaving it unable to send and receive ordinary internet traffic. Such attacks have proven to be detrimental to businesses that require the internet to operate. During Dos attacks, the attacker floods a network server with requests by making several requests to the server(Doyle, 2011). These requests are illegitimate and contain fabricated return addresses that mislead the victims' computer servers as they authenticate the requestors. During this process, the system becomes overwhelmed and fails to perform normal tasks. The most common Dos attacks are *Smurf Attacks* and *SYN Flood.*

***4) Viruses, Trojans, and Worms***

The name Trojan is derived from ancient Greek mythology. The Greeks wanted to conquer the city of Troy but its walls were impenetrable. They put their best soldiers in a big curvature of a Trojan horse tricking their rivals into bringing the soldiers within their walls. Similarly, in computer lingo, a Trojan is a program that is employed in a victim's device unknowingly. It provides the perpetrator with remote access for the victim's computer (Shea, 2012). A virus attaches itself to programs or files and can spread from computer to computer leaving infections. Computer viruses, like human viruses, vary in their severity and can cause damages to software, hardware, and documents. Victims' computers are susceptible to the virus once they run or open infected programs. Equally or more dangerous is the warm which refers to a subgroup of the virus that can travel from one computer to another without help from a person. Worms are critically dangerous as they can replicate and create devastating effects.

***C. Causes of Cyber Crime***

This study notes that there are several reasons why cybercriminals engage in crime. The main reason is to make quick money. Such groups are motivated by greed and often engage in electronic commerce, electronic banking, and fraud. Secondly, cybercrimes can be committed for prestige and recognition. Most of the perpetrators here are youngsters who want to attract attention and feel tough. They may are idealists who want to be in the spotlight but not hurt anyone. Thirdly, cybercrime can be committed to fighting for a cause that is key to the perpetrators' beliefs. In this situation, the perpetrators do not mind causing harm and destruction as long as their goals are accomplished.

***1) Impact of cybercriminal activity on the world***

In comparing cybercrime with the conventional crime, there is no much difference because both cause breaching of legal rules. According to Shea (2012) cybercriminals have been used various channels to distribute illegal emails, websites, and also simple crimes such as downloading illegal music files. Wall (2007) posits that international criminals steal intellectual property for their own or at the request from their governments. Losses are estimated at 10 billion dollars annually. Germany, for example, estimated its own IP losses

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

from industrial espionage at $25- 50 Billion dollars, much of which is caused by weak internet security. Notably, most enterprises do not report harm from cybercrimes indicating that the figure could be higher. Other companies that have been hacked choose to conceal the information to avert scaring customers and investors. The financial system has been increasingly targeted by cybercriminals. They tend to go after Automated Teller Machines, credit cards, and online bank accounts. In a single example, A Russian gang took $ 9.8 million from ATMs over a Labor Day weekend.

The cybercrime threat has become widespread touching on all corners of the globe and affecting developmental efforts socially and economically. As opportunities unfold, they have brought along new opportunities to commit crimes. Wall (2007) argues that cybercrime has not created new crimes but it has instead provided an additional method through which offenses such as theft, extortion, illegal protests and terrorism thrives. According to Moore (2016) terrorism in cyberspace takes many forms such as physical destruction of machinery, remote interference of computer networks, disruption of government networks, and mass media. A good example of such destruction is in 2015 when an alleged Russian cyber attacker seized control of the Prykarpatnergo Control Center (PCC) in Western Ukraine. This incident left approximately 230000 people without power for up to 6 hours.

Table 1.2 showing distribution of internet users across the world

| World Regions | Population (2020 Est) | Population % of the world | Internet Users 31st May 2020 | Growth 2000-2020 |
|---|---|---|---|---|
| Africa | 1,340,598,447 | 17.2% | 526,710,313 | 11,567% |
| Asia | 4,294,516,659 | 55.1% | 2,366,213,308 | 1,970% |
| Latin America | 834,995,1997 | 10.7% | 727,848,547 | 592% |
| Middle East | 260,991,960 | 3.3% | 453,702,292 | 2,411% |
| North America | 368,869,647 | 4.7% | 183,212,099 | 5,477% |
| Australia | 42,690,838 | 0.5% | 38,917,600 | 279% |

## 5. CONCLUSION AND RECOMMENDATIONS

This research has pointed out that cybercrime is fast gaining ground in both developed and developing countries. The lead perpetrators of cybercrime are the youth who may have technical competence and experience to commit computer-related crimes. Findings also indicate that a lot of cybercrime cases go unreported due to the fear of humiliation. The study also found a mismatch between countries' legislations, institutions, and agencies that have been given the power to combat cybercrime. This study discovered that conventional laws and policies are currently incapable of mitigating cybercrime cases. It is therefore crucial that they are reviewed in order to include new technological changes. It is also clear that computer crime is not considered a priority in some countries. It is therefore not even budgeted for as the United Nation securitization framework postulates. Further, this study has shed light on the rapidness of cybercrime across the world. This paper recommends that similarly, the response to cybercrime need also be proportional. To effectively combat cybercrime, there needs to be harmonization of cybercrime regulation and legislation across the world. As discussed, cybercrime is regarded differently in various countries. It is critical that a common classification of computer crimes be adopted by all nations globally.

## REFERENCES

[1] Alazab, M., & Broadhurst, R. (2015). The role of spam in cybercrime: Data from the Australian cybercrime pilot observatory. *Cybercrime Risks and Responses*, 103-120. https://doi.org/10.1057/9781137474162_7

[2] Alsmadi, I. (2019). Cyber intelligence. *The NICE Cyber Security Framework*, 75-90. https://doi.org/10.1007/978-3-030-02360-7_5

[3] Bernik, I. (2014). Cybercrime. *Cybercrime and Cyberwarfare*, 1-56. https://doi.org/10.1002/9781118898604.ch1

[4] Boes, S., & Leukfeldt, E. R. (2016). Fighting cybercrime: A joint effort. *Cyber-Physical Security*, 185-203. https://doi.org/10.1007/978-3-319-32824-9_9

[5] Casey, E. (2011). Digital evidence and computer crime: Forensic science, computers, and the internet. Academic Press.

[6] DCMS: Cybersecurity breaches survey 2019. (2019). *Network Security*, *2019*(4), 4. https://doi.org/10.1016/s1353-4858(19)30044-3

[7] Doyle, C. (2011). Cybercrime: An overview of the federal computer fraud and abuse statute and related federal criminal laws. DIANE Publishing.

[8] Grimes, R. A. (2017). Hacking the hacker: Learn from the experts who take down hackers. John Wiley & Sons.

[9] Grispos, G. (2019). Criminals: Cybercriminals. *Encyclopedia of Security and Emergency Management*, 1-7. https://doi.org/10.1007/978-3-319-69891-5_80-1

[10] Gupta, S. (2019). Ethical hacking terminologies. *Ethical Hacking – Learning the Basics*. https://doi.org/10.1007/978-1-4842-4348-0_1

[11] Howard, P. N., & Gulyas, O. (2014). Data breaches in Europe: Reported breaches of compromised personal records in Europe, 2005-2014. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2554352

[12] Krausz, M., & Walker, J. (2013). The true cost of information security breaches and cybercrime. IT Governance Publishing.

[13] Moore, M. (2016). Cybersecurity breaches and issues surrounding online threat protection. IGI Global.

[14] Rajan, A. V., Ravikumar, R., & Shaer, M. A. (2017). UAE cybercrime law and cybercrimes — An analysis. *2017 International Conference on Cyber Security And Protection Of Digital Services (Cyber Security)*. https://doi.org/10.1109/cybersecpods.2017.8074858

[15] Shea, J. M. (2012). *Combating computer viruses*. Gareth Stevens Publishing LLLP.

[16] T., S. (2016). Combating cybersecurity breaches in the digital world using misuse detection methods. *Advances in Digital Crime, Forensics, and Cyber Terrorism*, 85-92. https://doi.org/10.4018/978-1-5225-0193-0.ch006

[17] Wall, D. (2007). Cybercrime: The transformation of crime in the Information Age. Polity.