CYBER-CRIME: WASTED COMPETENCIES IN THE WORLD OF TECHNOLOGY

Chafika KHANIFER
Lecturer, PhD, Mohamed-Cherif Messaadia University - Souk Ahras (Algeria),
E-mail: c.khanifer@univ-soukahras.dz

Abstract: *Through this scientific intervention, we seek to shed light on one of the practices that has distinguished and continues to distinguish our contemporary world through the emergence in the realm of crime, which has transitioned from its real world setting to a virtual one, namely cyber- crime. This involves understanding its origins, history, and concept, as well as addressing the controversies surrounding it. Additionally, we will delve into its characteristics, objectives, and its parties involved, including the perpetrator and the victim, while also discussing its forms and methods of combating it.*

Keywords: cyber-crime, competencies, technology.

1. Introduction

The society we live in today is a society of information, knowledge, and human intelligence. The advancements of the human mind have given rise to various forms and shapes of technology, contributing to the efficiency and speed of tasks. The emergence of the internet has further amplified the importance of technology, transforming the world into a small village. This convergence and the widespread adoption of this virtual world have displayed numerous behaviors and practices, both acceptable and unacceptable. While technology has facilitated life and expanded human interactions, it has also been misused, with the internet being used against others with malicious intent, shifting it from its supportive nature to a criminal one.

This forms the subject of this scientific paper, titled "Cyber-crime: wasted Competencies in the World of Technology!" Through it, I aim to answer the following question within the conceptual framework:

What is cyber-crime, and what are its objectives and characteristics? Who perpetrates this type of crime and against whom? What is the way to curb it or at least reduce its expanding scope?.

2. The world before the emergence of cyber-crime

Before the emergence of the internet and its crimes, there existed criminal activities such as murder, theft, fraud, forgery, and other crimes due to the persistence of evil. However, the internet facilitated the ease of committing these crimes. The realm of information knows no general ethical principles, as the boundaries of acceptable behavior or even ethical behavior in the information space are not clear. The presence of the internet has led to the evolution of traditional crimes and the emergence of new ones. (Ghada Nassar, 2017: 09)

3. The emergence of cyber-crime

Cyber-crime has followed a historical evolution in line with the development of technology and its usages. We can summarize the stages of these crimes into three phases:

1.The first phase: This phase saw the widespread use of computers in the 1960s and 1970s. With the increasing use of personal computers in the 1970s, several survey and legal studies emerged that focused on computer crimes. Actual criminal cases were addressed, and discussions began to view them as a criminal phenomenon rather than just unacceptable behaviors.

2. The second phase: In the 1980s, a new concept of cyber-crimes emerged, linked to remote system intrusion and activities involving the dissemination and planting of computer viruses that destructively targeted files and programs.

3.The third phase: this phasein the 1990s, witnessed a tremendous growth in the field of cyber-crimes, along with changes in their scope and concept. This was primarily due to the facilitation provided by the internet in accessing systems and infiltrating information networks. (Hisham Bashir, 2012: 06-07)

Cyber-crimes first appeared prominently in Western societies such as America and its neighboring countries. This was attributed tothe technologies that initially found their roots in facilities like those of the U.S. Department of Defense. It was normalthere to be significant breaches and violations by internet users within these government departments, including technicians, engineers, and computer personnel.

The absence of laws criminalizing attacks on information and data, and even if such laws were imposed, the difficulty of detecting these crimes and prosecuting the perpetrators, encouraged many to venture into this realm of criminal activity. (Hamoud bin Mohsen Al-Dajani: 557).

4. On the concept of cyber-crime

The concept of informational crime is challenging to define, as research and studies have provided various definitions. These definitions reflect the diversity of terms used to refer to and define this type of crime. Some terms include computer crimes, misuse of computers, crimes related to or associated with computers, crimes involving automated data processing, modern technology crimes, or information crimes. (Khaled Hassan Ahmed Lotfy, 2019: 25)

Those who use the term "informational crime" intend to express a crime in which the subject of the violated right is information. On the other hand, those who use the term "internet crimes" are using a narrower scope because they restrict these crimes to unauthorized activities conducted through internet access, excluding crimes that could be committed using a computer without internet access. As for those who use the term "cyber-crime," they refer to crimes committed through computers and other modern communication means. (Khaled Hassan Ahmed Lotfy, 2019: 27)

Definitions of informational crime have varied due to disagreements over defining the crime itself and, preceding that, defining information. Informational crimes represent a new category of crimes. With the information and communication revolution, a new type of crimes emerged, transitioning crime from its traditional form to an electronic one, which may be difficult to address. Informational crime is a modern phenomenon linked to modern technology, specifically information and communication technology.

Defining informational crime has been shrouded in ambiguity due to efforts to establish a comprehensive definition. Some argue against defining it, claiming it's merely traditional crime committed through electronic means. (Abdel-Al Derbi, Muhammad Sadiq Ismail, 2012: 41)

5. The concept of cyber-crime

the concept of cyber-crime:, or cyber- crimes, consists of two parts: "crime" and "cyber." The term "cyber" is used to describe the idea of a part of the computer or the information age. Cyber-crime is defined as violations committed against individuals or groups of individuals with criminal intent, aiming to harm the reputation of the victim or cause material or mental harm, whether directly or indirectly, using communication networks such as the internet (such as chat rooms, email, and mobile phones). (Dhiab Musa Al-Badaina: 03).

Internet crimes can be defined as "the sum of crimes committed using information technology or information networks, and these crimes have a diverse nature and can take the form of traditional crimes using technical means of networks." (May Al-Abdullah, 2014: 139). Other definitions include: "Any harmful act against others through electronic media such as computers, mobile devices, telephone communication networks, information transmission networks, the internet, or the illegal use of computer or electronic data in general." It is also defined as: "A collection of actions and activities punishable by law, linking criminal acts with the technological revolution" (Mahmoud Madian)

It isalso defined as: "An unlawful act that relies on technical knowledge and expertise in information technology, carried out using any tool of smart and programmatic communication, with the electronic space serving as its platform and stage" (Ibrahim Mohammed bin Mahmoud Al-Zandani, 2018).

5/ criminal Activity in the space of internet

Physical activity or behavior in internet crimes requires the presence of a digital environment and internet connectivity. It also requires knowledge of the initiation, execution, and consequences of this activity. For example, the perpetrator of the crime may prepare a computer to facilitate the committingof the crime by downloading hacking programs or by developing such programs themselves. Additionally, they may need to create pages containing content that violates public decency and upload them. They could also commit crimes by developing virus programs for dissemination. Not every crime requires preparatory actions, and it is difficult to distinguish between preparatory work and the commencement of criminal activity in computer and internet crimes (Abdul Haleem Musa Yaqoub, 2014: 215-216).

6/ aims of cyber-crimes

1.Illegally accessing information, such as theft, viewing, deletion, or modification of information to achieve criminal goals.

2. Accessing and disrupting or sabotaging information-providing server devices, commonly targeting websites on the internet.

3. Obtaining information, altering internet site addresses to sabotage public institutions and extort them.

4. Accessing individuals or entities using technology for the purpose of threatening or blackmailing, such as banks, government departments, official agencies, and all forms of companies.

5. Exploiting information technology for illegitimate financial, moral, or political gains through credit card fraud and hacking electronic websites on the internet, etc.

6.Utilizing technology to support terrorism and extremist ideas, or disseminating ideas that could establish extremist ideologies . (Abdul Haleem Musa Yaqoub, 2014, 214-213).

7/characteristics of Cyber Crime

Cybercrime is similar to traditional crime in terms of the elements of the crime, such as a criminal with a motive to commit the crime, a victim, who may be a natural person or a legal person, and the instrument of the crime. In cybercrime, the instrument of the crime is a product of technology, as well as the location of the crime that does not burden the offender in Access to it, which facilitates the process of electronic crime, and in many of these crimes, the crime is carried out remotely, using communication lines and networks between the perpetrator and the crime site.Abdul Haleem Musa Yaqoub, 2014: 201).

Some characteristics of cyber-crime are the following:

1**. Overseas Crimes**

Information technology's ability to shorten distances and enhance connectivity across the globe has influenced the nature of criminal activities. Criminals utilize these technologies to violate the law, making the stage of cyber-crime no longer local but global.

2**. Soft and Tempting Crimes for Criminals**

Unlike traditional crimes that often require physical effort such as murder and rape, cyber-crime does not necessitate any physical exertion. Instead, it relies on mental acumen and deliberate thinking, based on knowledge of computer technologies. Cybercrime does not require any degree of physical proximity or contact between the perpetrator and the victim;hence, it is characterized by being less violent and aggressive than traditional crimes (Adham Bassem Nimr Baghdadi, 2018: 11-12)

8/ parties Involved in Cyber- Crime:

Every crime has a perpetrator, a victim, and consequences resulting from the implementation of the crime. (Khaled Hassan Ahmed Lotfy, 2019: 35)

1. **The Perpetrator in Cyber- Crime**:

In the digital world, criminals come in all shapes and sizes, ranging from sophisticated individuals to pranksters. Ensuring information security and avoiding liabilities necessitates treating everyone as a potential threat, not as a waste of goodwill or trust in others. It's the only guarantee for protection against highly dangerous sources that could lead to incalculable losses and responsibilities (Ayman Abdullah Fikri, 2014: 120)

Most studies and legislations consider the perpetrator in cyber-crimes to be a natural person acting on their own behalf, aiming to achieve their own interest behind the committed crime. Most individuals committing computer crimes are classified as belonging to the younger generation, professionals working in the field of computer science, or amateurs. However, practical experience has shown otherwise, as alongside natural persons, there may be accomplices who provide tools, programs, and equipment necessary for the crime, or at least sell such products and programs without which there would be no crime. Additionally, perpetrators can be groups of individuals, organizations, or legal entities, and cyber-crimes can even involve political systems and states (Ibrahim Muhammad bin Mahmoud Al-Zindani, 2018: 36)

The seriousness of these crimes lies mainly in the criminal who carries out the crime, as he is distinguished by intelligence and knowledge in dealing with the field of automated data processing and familiarity with technical skills and knowledge. (Khaled Hassan Ahmed Lotfy, 2019: 35)

A. Personal Characteristics of the Cyber Criminal:

Studies identifying the personal traits of the cybercriminal have found that there is no specific model for them, but rather common traits among these criminals, summarized as follows:

- Highly intelligent criminals capable of modifying and developing security systems to evade detection and tracking of their criminal activities on networks or within computers.

- Specialized criminals with exceptional technical skills who exploit their knowledge and abilities to penetrate networks and crack passwords or codes.
- Recidivist criminals who consistently engage in criminal activities, employing their skills in computer operation, data storage, and unauthorized access repeatedly.
- Criminals affiliated with computer-related professions functionally. (Khaled Hassan Ahmed Lotfy, 2019: 36)

B. Psychological Characteristics of the Cyber Criminal:

Psychological studies of cyber criminals have shown that they have no sense of the illegitimacy of their actions or the deservingness of punishment for these actions. For this category, the boundaries between good and evil are blurred, and feelings of guilt are absent due to the lack of direct interaction between the perpetrator and the victim. (Khaled Hassan Ahmed Lotfy, 2019: 37)

C. Types of Cyber Criminals:

First type; hackers:

They can be classified in two types:

Hackers: This category includes individuals who challenge system and network security measures. However, they often lack malicious or destructive motives but are driven by the desire to prove their abilities. The term "hackers" is usually synonymous with challenge attacks. (Ayman Abdullah Fikri, 2014: 123)

Hackers are known for infiltrating your device, allowing them to view, steal, destroy files, eavesdrop, or monitor your online activities. (Abdel Halim Musa Yacoub, 2014: 201)

By gaining unauthorized access to computer systems and bypassing security barriers for this purpose, the goal of this category is usually skilled young people, driven by curiosity or self-assertion (Khaled Hassan Ahmed Lotfy, 2019: 38)

2. Crackers: The term "crackers" is synonymous with malicious and harmful attacks. (Ayman Abdullah Fikri, 2014: 123) These individuals infiltrate computer processing systems to access stored information, cause damage, tamper with it, or steal it(Khaled Hassan Ahmed Lotfy, 2019: 38)

This distinction does not affect the responsibility of the perpetrators of activities from both categories, and they are held accountable for the damages they cause to the targeted sites through their attacks (Ayman Abdullah Fikri, 2014: 123)

Second type; malicious Actors:

This category is motivated by the desire for revenge and retaliation due to the actions of an employer or the treatment received from the concerned institution.

When they are not employees in it, they tend to use techniques such as planting viruses, malicious software, or system sabotage. (Ayman Abdullah Fikri, 2014, p. 123)

Employees in the technology sector or users of it in other sectors are often subjected to significant psychological pressures resulting from work pressure, financial problems, and the nature of alienating work relationships. These factors may serve as a driving force for some workers to commit cybercrimes as a means of revenge against the institution or employer. For example, a disgruntled accountant might manipulate information technology programs to hide the company's accounting data six months after leaving. (Khaled Hassan Ahmed Lotfy, 2019, p. 39)

Third type; amateurs:

This category commits these crimes for entertainment purposes without intending to cause any harm to the victims. They are characterized by their young age and proficiency in computer science. However, their danger lies in the fact that they may form a good nucleus for turning into professional hackers. (Khaled Hassan Ahmed Lotfy, 2019: 38)

2. Victims in Cyber- Crime

It is difficult to accurately determine the victims of cyber-crimes because they often become aware of these crimes only after they have occurred. Like the perpetrators, the victims can be natural persons, legal entities, communities, or even countries (Ibrahim Muhammad bin Mahmoud Al-Zindani, 2018: 37)

9. Forms of cyber-crimes

1. Sexual, Pornographic, and Unethical Crimes

There are websites on the internet that promote sexual activities, whether for adults or children. These websites publish more specialized sexual images, including videos and images, and many of them specialize in chat programs. A study found that there are 71 Arabic pornographic websites on the internet.

2. Software Piracy via the Internet

Although software piracy has been associated with the advent of computers in general, the emergence of information networks has significantly increased the volume of this crime. The open nature of these networks and the ease of copying software in seconds, coupled with the fertile ground these networks provide for marketing pirated software, have encouraged software pirates to operate within the network.

3. Information Destruction

This involves damaging data storage units using heavy tools, explosive charges, corrosive gas bombs, or flammable materials with ignition keys. Information can also be destroyed magnetically by subjecting it to destructive magnetic forces.

4. Misuse of Bank Cards:

This crime is particularly prevalent in societies with highly advanced and modern banking systems that issue bank cards with minimal security procedures. Forms of this crime include using stolen or expired cards, forging cards, withdrawing larger amounts of cash than allowed using someone else's card at ATMs, exploiting vulnerabilities in the machines. Also, some individuals falsely report their bank cards as lost, then immediately withdraw cash before the bank can freeze their funds, giving the impression that the thief who found or stole the card made the withdrawals. (Ghada Nassar, 2017: 15-19)

5. Theft of Personal Data:

This involves obtaining information provided to the device (software or processing data), whether stored on disks, magnetic tapes, or paper.

6. Manipulation of Personal Programs:

Software is of great importance in the field of computer use because it gives life to the computer and enables it to perform its tasks. Examples include changing the operating system program or creating a new (fake) program to commit a crime.

7. Defamation Crimes:

These involve invading individuals' privacy and spying on their online profiles, then publishing personal photos and news that may affect their honor. (Ghada Nassar, 2017: 19-22) Sometimes these crimes take on extortionist logic, where photos of individuals in socially unacceptable situations are taken and then broadcasted on the internet through platforms like YouTube. (Abdel Halim Musa Yacoub, 2014: 222)

8. Gambling Crimes:

This includes owning and managing an online gambling project, facilitating and encouraging it, and using the internet to promote alcohol and addictive substances to minors.

9. Electronic Fraud:

This refers to any behavior or action by an individual or group that burdens or imposes additional burdens on other parties as a result of using unethical practices to gain an unfair or illegal advantage. (Ghada Nassar, 2017: 23)

10. Combatting cyber-crimes

Combatting cybercrimes can be summarized in the following methods:

➢ Establishing International policies, and implementing strict penalties for internet crime perpetrators requires governmental and international intervention due to the severity of the matter.

➢ Utilizing Advanced Techniques to detect the identity of offenders and gather evidence as quickly as possible.

➢ Raising Awareness to educate individuals about the nature and risks of cyber-crimes.

➢ Maintaining Confidentiality of personal information such as bank accounts and credit cards.

➢ Securing Passwords to avoid disclosing passwords entirely, regularly changing them, and selecting strong ones.

➢

➢ Avoiding Social Media Image Storage by refraining from storing personal photos on social media platforms and computers.

➢ Avoiding Unknown Software Downloads by staying clear of downloading software from unknown sources.

- Regularly Updating Security Software by ensuring that computer protection programs are regularly updated.
- Establishing Special Organizations dedicated to combating cybercrimes and minimizing their occurrence.
- Prompt Reporting: by informing law enforcement agencies immediately upon experiencing a cybercrime.
- Keeping Up with Technological Advances by staying updated on developments related to cybercrimes and improving methods to combat them.
- Using Secure Software and Patch-Free Operating Systems by utilizing safe software and operating systems without vulnerabilities.
- Disconnecting Computers from the Internet When Not in Useby disconnecting devices from the internet when not actively being used.
- Exercising Caution by being cautious and skeptical of all advertisements and verifying their credibility through reputable search engines (Lamiya Talla, Kahinah Salam, Volume 06, Issue 02 2020, pages 86-88)

Conclusion

Cybercrime, given the overlaps among its various forms, has made it challenging to establish a universally agreed definition for this concept. Each perspective sheds light on some aspects of cybercrime. Through what has been mentioned, we can define cybercrime as various unethical and illegal practices conducted through different technological means in the virtual world. These practices result in causing harm to the victims, regardless of their backgrounds. The offenders' intelligence and technological are exploited to inflict harm, leading to disruptions in accounts, destruction of information systems, leakage of personal data and documents, among other consequences. Considering the various outcomes of such practices, concerted efforts are required to control and mitigate this type of criminal activity, given its significant detrimental effects on society, whether economic, financial, or moral Hence, it is essential to allocate educational programs and awareness sessions about this danger. Furthermore, there is a need to guide consumption in the right direction and raise awareness about the proper usage of various modern technologies. Extreme caution and vigilance are necessary to avoid becoming additional victims of technological misuse.

References:

1. Ibrahim Mohammed bin Mahmoud Al-Zandani. (2018). *Cybercrimes from the Perspective of Islamic Sharia and their Provisions in Qatari and Yemeni Law*. Master's thesis, Department of Islamic Studies. Thailand: Fattani University.
2. Adham Basim Nimr Baghdadi. (2018). *Methods of Research and Investigation into Cybercrimes.* Master's thesis, Faculty of Graduate Studies, An-Najah University. Nablus, Palestine.
3. Ayman Abdullah Fikri. (2014). *Cybercrimes: A Comparative Study of Arab and Foreign Legislation*. Riyadh: Law and Economics Library.
4. Hamoud bin Mohsen Aldujani. (n.d.). *Supplement* to Issue 173, Vol. 16, *Journal of the Islamic University*.
5. Khaled Hassan Ahmed Latif. (2019). *The Digital Evidence and its Role in Proving Cybercrime*. Alexandria: Dar Al-Fikr Al-Jami'i.
6. Ziyab Musa Al-Badayneh. Cybercrimes: *Concept and Causes*. Amman, Hashemite Kingdom of Jordan: Scientific Forum on Emerging Crimes Amid Regional and International Changes.
7. Abdel Halim Moussa Yaqoub. (2014). *New Media and Cybercrime*. Global Publishing and Distribution House.
8. Abdel Aal Alderby, Mohammed Sadeq Ismail. (2012*). Cybercrimes: A Legal and Judicial Study in Comparison with the Latest Arab Legislation in the Field of Combating Cyber and Internet Crimes.* Cairo: National Center for Legal Publications.
9. Ghada Nassar. (2017). *Terrorism and Cybercrime*. Cairo: Arabi for Publishing and Distribution.
10. Lama Talta, Kahina Salam. (Vol. 06, No. 02, 2020). Cybercrime: A New Dimension to the Concept of Crime through Social Media Platforms. *Al-Rawaf Journal of Social and Humanitarian Studies*, pp. 86-88.
11. Mahmoud Madin. *Cybercrime and National Security Challenges:* A Doctoral Thesis in Public International Law. Egyptian Publishing and Distribution House.
12. May Abdullah. (2014). *Lexicon of Modern Concepts of Media and Communication*, Arab Terminology Unification Project. Beirut, Lebanon: Dar Al-Nahda Al-Arabiya.
13. Hisham Bashir. (2012). *International Mechanisms for Combating Cybercrime.* International Center for Future and Strategic Studies