THE ROLE OF CYBERSECURITY IN ENHANCING THE EFFECTIVENESS OF LAW AGAINST CYBERCRIMES

Monther Abed-Alrazzaq Musleh Al-Amaireh ¹

ABSTRACT

Objective: This study aims to understand the nature of cybercrimes and the challenges faced by legal authorities in combating them.

Theoretical Framework: The progress in information and communication technology is not limited to the positive aspects related to technology and infrastructure development. It has also revealed a negative side with serious implications for the state and its sovereignty. This negative aspect has eroded privacy and greatly encouraged the proliferation of cybercrimes, posing a threat to international security and peace. The negative aspect is manifested in the phenomenon of cyberattacks that now threaten a nation's security and its citizens, necessitating measures to mitigate these threats.

Method: in this study, the descriptive analytical approach was followed by analyzing the texts in Jordanian law and describing each case dealt with in relation to the role of cyber security in enhancing the effectiveness of criminal law against cybercrimes.

Results and Discussion: The role of cybersecurity in addressing cybercrimes is of significant importance in ensuring the safety of information and preserving digital security for individuals and institutions. Jordanian legislation has imposed deterrent laws to combat cybercrimes, including the Electronic Crimes Law and the Cybersecurity Law.

Research Implications: The study also reached a number of recommendations, including the need to develop a clear legal framework to combat cybercrime, strengthen cybersecurity in all fields, train its employees and raise their efficiency.

Originality/Value: The significance of this study arises from the increasing severity of cyber threats and electronic crimes worldwide, which have become a serious threat to individuals, organizations, and nations. As a result, enhancing the effectiveness of criminal law in combating these electronic crimes has become an urgent necessity.

Keywords: Cybersecurity, Cybercrime, Law, Enhancing the Effectiveness.

O PAPEL DA CIBERSEGURANÇA NO REFORÇO DA EFICÁCIA DA LEI CONTRA O CIBERCRIME

RESUMO

Objetivo: Este estudo visa compreender a natureza dos crimes cibernéticos e os desafios enfrentados pelas autoridades jurídicas no seu combate.

Referencial Teórico: The progress in information and communication technology is not limited to the positive aspects related to technology and infrastructure development. It has also revealed a negative side with serious implications for the state and its sovereignty. This negative aspect has eroded privacy and greatly encouraged the proliferation of cybercrimes, posing a threat to international security and peace. The negative aspect is manifested in the phenomenon of cyberattacks that now threaten a nation's security and its citizens, necessitating measures to mitigate these threats.

¹ Middle East University, Faculty of Law, Jordan. E-mail: montheram@hotmail.com
Método: neste estudo, a abordagem analítica descritiva foi seguida pela análise dos textos do direito Jordaniano e pela descrição de cada caso tratado em relação ao papel da cibersegurança no reforço da eficácia do direito penal contra os cibercrimes.

Resultados e Discussão: O papel da cibersegurança no combate aos crimes cibernéticos é de importância significativa para garantir a segurança da informação e preservar a segurança digital para indivíduos e instituições, a legislação jordaniana impôs leis de dissuasão para combater os crimes cibernéticos, incluindo a Lei de Crimes eletrônicos e a Lei de cibersegurança.

Implicações da Pesquisa: O estudo também chegou a uma série de recomendações, incluindo a necessidade de desenvolver um quadro jurídico claro para combater a cibercriminalidade, reforçar a cibersegurança em todos os domínios, formar os seus funcionários e aumentar a sua eficiência.

Originalidade/Valor: O significado deste estudo decorre da crescente gravidade das ameaças cibernéticas e crimes eletrônicos em todo o mundo, que se tornaram uma série ameaça para indivíduos, organizações e nações. Consequentemente, o reforço da eficácia do Direito Penal na luta contra estes crimes electrónicos tornou-se uma necessidade urgente.

Palavras-chave: Cibersegurança, Cibercrime, Direito, Reforço da Eficácia.
1 INTRODUCTION

The modern era has witnessed a noticeable increase in the use of digital technology and electronic communications in various aspects of life. As these technologies have advanced, new forms of crimes targeting individuals and organizations online have emerged, known as cybercrimes. These crimes encompass electronic fraud, identity theft, cyber breaches, electronic espionage, and other threats related to the digital realm. Therefore, it has become necessary to enhance the effectiveness of criminal law in combating these crimes.

The progress in information and communication technology is not limited to the positive aspects related to technology and infrastructure development. It has also revealed a negative side with serious implications for the state and its sovereignty. This negative aspect has eroded privacy and greatly encouraged the proliferation of cybercrimes, posing a threat to international security and peace. The negative aspect is manifested in the phenomenon of cyberattacks that now threaten a nation's security and its citizens, necessitating measures to mitigate these threats.

Information and communication technology has rapidly evolved in the modern era, and with this evolution, the exposure to cyber threats and incidents has increased. The need to secure electronic systems and data for both organizations and individuals has become paramount. Cybersecurity is considered one of the effective tools to combat these threats and deal with cyber incidents in a manner that protects both personal and public interests.

1.1 STATEMENT OF THE PROBLEM

The study's problem arises from the rapid evolution of technology and communications, with electronic crimes now posing a significant threat. Effectively countering these crimes and developing comprehensive strategies that integrate criminal laws and cyber security measures have become imperative. Cybersecurity plays a crucial role in enhancing the effectiveness of criminal law in combatting electronic crimes. However, these efforts face multiple challenges that affect the criminal law's ability to keep pace with the evolution of electronic crimes. This deficiency could potentially facilitate the exploitation of electronic crimes and hinder countermeasures.

1.2 RESEARCH QUESTIONS

1. What is the concept of cybersecurity?
2. What is the concept of electronic crimes?

1.3 RESEARCH OBJECTIVES

In order to improve the efficiency of criminal law in thwarting electronic crimes, this study intends to shed light on the function of cybersecurity. In order to accomplish its main goals, the study aims to:

1. Understanding the nature of electronic crimes and the challenges faced by legal authorities in combating them;
2. Analyzing the importance of cybersecurity as a means to protect individuals and organizations from electronic crimes and bolster criminal law.

1.4 SIGNIFICANCE OF THE STUDY

The significance of this study arises from the increasing severity of cyber threats and electronic crimes worldwide, which have become a serious threat to individuals, organizations, and nations. As a result, enhancing the effectiveness of criminal law in combating these electronic crimes has become an urgent necessity. Criminal law faces significant challenges in addressing electronic crimes, as countering such crimes requires specialized knowledge and advanced techniques for detection, tracking, and prosecution. Therefore, the development of legal and electronic tools and the promotion of cooperation among relevant authorities are essential to address these challenges. Cybersecurity is a fundamental element in safeguarding individuals and organizations against electronic crimes. Information and communication technology relies on a robust cyber security system to ensure the safety of data and sensitive information. Hence, it is crucial to enhance and integrate cybersecurity with criminal law to ensure comprehensive protection.

2 METHODOLOGY

Descriptive-Analytical Method: This is achieved through the analysis of legal texts in Jordanian law and the description of each case concerning the role of cybersecurity in enhancing the effectiveness of criminal law against electronic crimes.
2.1 PREVIOUS STUDIES


This study aimed to explore cybersecurity threats and their countermeasures within international public law. It sought to provide legal answers by reviewing the rules of international public law related to the use of force in general and the legitimacy of self-defense in particular, and the linkage between them. The study followed a comparative methodology and arrived at several important findings, including that international law jurisprudence and experts uphold the consideration of cyber weapons as conventional weapons with specific constraints. It also highlighted that the comparison between physical armed attacks and cyber-attacks is impractical due to fundamental differences between these categories of attacks, making it difficult to apply some of the obligatory conditions for activating Article 51 regarding cyber-attacks.


The goal of this study was to understand cybercrimes, which have become a threat to individuals, societies, and national security. Cybercrimes are evolving rapidly as criminals employ cutting-edge technologies in them cyberattacks. The study aimed to shed light on technological developments and cybercrimes to identify and assess the problems they present and to maximize the benefits of these developments while mitigating their risks. The study also examined regional and international cooperation in combating cybercrimes. Cyberattacks with high momentum are often challenging to identify, eliminate, and prosecute. The study is structured into three sections, covering an introduction to cybercrimes, an exploration of Arab and international agreements, and concluding with research results and recommendations.

2.2 STUDY STRUCTURE

Chapter 1: The Nature of Cybersecurity and Electronic Crimes
- Introduction;
- Section 1: Defining Cybersecurity;
• General concept of cybersecurity;
• Significance of cybersecurity in the modern era;
• Section 2: Defining Electronic Crimes;
• Definition of electronic crimes;
• Common types of electronic crimes;
• Potential impacts and damages of electronic crimes.

3 THE ROLE OF CYBERSECURITY IN COMBATING ELECTRONIC CRIMES

3.1 SECTION 1: THE IMPORTANCE OF CYBERSECURITY IN COMBATING ELECTRONIC CRIMES

3.1.1 The Nature of Cybersecurity and Electronic Crimes

The term "cybersecurity" refers to a set of measures and precautions aimed at safeguarding electronic systems, computer networks, and digital data from cyber threats and attacks. Cybersecurity is a vital aspect of the world of communication and information technology, playing a pivotal role in ensuring the continuity of vital operations for organizations and safeguarding the privacy and integrity of sensitive information.

With the increasing use of the internet and the expansion of wired and wireless networks, cybersecurity threats have notably escalated. Cybersecurity threats encompass various forms, ranging from electronic piracy to cyber intrusions, making them some of the most significant threats to cybersecurity. These threats encompass a wide spectrum, from attacks directed at individuals, such as electronic fraud and identity theft, to large-scale attacks targeting governments, corporations, and their infrastructures.

However, it's not only cybersecurity that concerns the international community and the private sector; the fight against electronic crimes is equally significant. Electronic crimes encompass all unlawful activities involving digital technology, including fraud, electronic manipulation, espionage, piracy, and electronic extortion. These crimes have a negative impact on individuals, organizations, and communities, resulting in material losses and unimaginable damages.
3.2 THE FIRST REQUIREMENT

3.2.1 Defining Cybersecurity

The term "cybersecurity" is derived from the terms "security" and "cyber," with "cyber" having Latin origins, meaning information security. Therefore, cybersecurity is a broader and more general expression than information security. It encompasses a set of tasks, tools, methods, strategies, principles, and security procedures.²

It also includes risk management practices related to technology. Its main goal is to safeguard the cyber environment, assets of organizations, and users. Cybersecurity aims to reduce activities and practices that target protecting systems, networks, and software against any electronic attacks or violations, regardless of their form or type. These activities and practices have two main objectives: prevention through proactive measures and remediation after the occurrence of any disruption.³

Cybersecurity is the practice of protecting computer devices, networks, software applications, essential systems, and data from potential digital threats. Organizations bear the responsibility of securing data to maintain customer trust and comply with regulatory requirements. They rely on cybersecurity measures to protect sensitive data from unauthorized access and prevent any disruptions to business operations due to unwanted network activity. Institutions implement cybersecurity by simplifying digital defense among individuals, operations, and technologies.⁴

Cybersecurity includes a set of tools, policies, secure concepts, safety assurances, and principles, guiding those involved in managing risks and ensuring the proper use of technology for protecting the cyber environment and instructing its users.⁵

Cybersecurity is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security or electronic information security. This term applies in various contexts, ranging from business operations to mobile computing, and can be categorized into several common classes.⁶

² Khater, Nouri Hamad, Protection of Computer-Related Works and Information with the Copyright Protection Law, Al al-Bayt University, research published in Al-Manara Magazine, Mafraq, Issue 4, January 2012, p. 35.
³ Adel Jaber Allah, Means of Cybersecurity Protection, An Original Jurisprudential Study Compared to Contemporary Systems, Journal of the Faculty of Sharia and Law, No. (34), Part Three, Al-Azhar University, Egypt, January, 2022-2023
⁴ Adel Jaber Allah, the previous reference
⁵ Khater, Nouri Hamad, Protection of Computer-Related Works and Information with the Copyright Protection Law, Al al-Bayt University, research published in Al-Manara Magazine, Mafraq, Issue 4, January 2012, p. 36
⁶ Khater, Nouri Hamad, op. cit
In Jordan, cybersecurity is defined in Article 2 of Cybersecurity Law No. 16 of 2019 as follows: "The measures taken to protect cyber information systems, critical infrastructures, and networks from cybersecurity incidents, and the ability to recover and maintain their operation, whether access to them is unauthorized, misused, resulting from a failure to follow security procedures, or as a result of deception."\(^7\)

Additionally, the International Telecommunication Union defines cybersecurity as a "set of missions, means, policies, security procedures, guiding principles, approaches to risk management, training, best practices, and technologies that can be used to protect the cyber environment, assets of organizations, and users." This definition highlights the multifaceted nature of cybersecurity and emphasizes its importance in safeguarding the digital environment and the assets of institutions and individuals. It encompasses a wide range of measures, strategies, and practices aimed at ensuring the security of digital spaces and information.\(^8\)

It may be impossible to arrive at a specific, single definition of cybercrimes due to the diverse perspectives in this field, whether concerning the context, methods, or the degree of the threat, among other factors. Consequently, there have been various concepts attempting to define the notion of cybercrimes and encompass their different aspects and variations, either by broadening or narrowing the scope of understanding.

For instance, legal scholar Nareman defines cybercrimes as "all forms of illegal or harmful behavior committed using a computer." Meanwhile, scholar Doul defines cybercrimes as "any criminal act committed using a computer." Similarly, Lameeto defines cybercrimes as "any unlawful act using a computer as the main tool." On the other hand, legal scholar Elie D. Ball defines cybercrimes as "any criminal act committed using a computer as the main tool." Notably, this trend in jurisprudence associates the crime with the primary role of the tool used in committing it, making it a cybercrime or an internet crime when the computer itself is the main instrument.

However, this approach overlooks a significant aspect of cybercrimes in which computer elements themselves and their associated ethical aspects play a crucial role. As a result, these definitions and others that follow a similar approach are incapable of comprehensively understanding this phenomenon and providing a comprehensive definition of cybercrimes.

---

\(^7\) Article 2 of the Jordanian Cybersecurity Law No. 16 of 2019

\(^8\) The report issued by the International Telecommunication Union on reform trends in communications for the year 2020-2021

The scholar Mass provides a definition of cybercrimes, stating that they are "unlawful actions committed through computer information with the intention of committing a crime." This definition takes into account both the use of computer information and the criminal intent behind the actions, offering a more comprehensive understanding of cybercrimes.\footnote{M. Mass la Droit Penal Special Ne de Linformatique, in infromatieque ET droit penal travvx de linstitute criminelles de pietiers 1981, 4ed, cujas, and p2.}

All forms of illegal acts and behaviors are committed through the use of computers.\footnote{Mounir Al-Julaihi and Mamdouh Al-Julaihi, Internet and computer crimes and means of combating them, first edition, Dar Al-Fikr Al-Jami’i, Egypt, 2006, p. 14.}

Cybercrime is an act or omission that results in an assault on wealth, whether it's material or immaterial, and this act is a result of utilizing electronic technologies. Furthermore, it is defined as unlawful actions committed by individuals with expertise and knowledge, requiring a similar level of expertise and knowledge for pursuing the perpetrator and investigating the crime.\footnote{Muhammad Ababneh, Computer Crimes and their International Dimensions, first edition, Dar Al-Thaqafa Publishing House, Jordan, 2005, p. 17.}

Indeed, there is a wide range of perspectives in legal jurisprudence regarding the definition of cybercrimes. This divergence of opinions often hinges on the level of technical expertise and knowledge required by the perpetrator to commit such crimes. As you've pointed out:\footnote{Salama, Muhammad Abu Bakr, Encyclopedia of Information Crimes, Ma’arif facility, Alexandria, 2006, p. 11.}

1. **Broad Definition**: Some legal perspectives adopt a broad definition of cybercrimes, where the emphasis is less on the technical expertise of the perpetrator. In this view, any unlawful act committed using a computer or electronic means qualifies as a cybercrime.

2. **Narrow Definition**: On the other hand, there is a more restrictive perspective that strongly links cybercrimes to the technical knowledge of the perpetrator. In this view, cybercrimes are considered to be crimes that require advanced technical knowledge for both committing and investigating them.

The variations in these perspectives can lead to differences in how cybercrimes are defined and prosecuted in different jurisdictions and legal systems. These differing viewpoints reflect the evolving nature of technology and the need for legal systems to adapt to these changes. In practice, the definition and handling of cybercrimes often depend on the specific laws and regulations of a given country or region.
There is still a wide debate in this regard, and opinions may differ according to different legislation and legal systems in different countries.

3.3 THE ROLE OF CYBERSECURITY IN COMBATING CYBERCRIMES

Modern societies are living in a digital age characterized by rapid and accelerating technological advancements. With the increasing use of the internet and electronic communication, new challenges have emerged in the realm of information security and the protection of personal data. Among these challenges, cybercrimes have come to the forefront. Cybersecurity aims to safeguard electronic systems, networks, and data from unauthorized breaches and illegitimate manipulations. The entities responsible for cybersecurity play a crucial role in countering cybercrimes and safeguarding the digital infrastructure of the state and the private sector.

Network security, therefore, is the practice of securing a computer network from intruders, whether they are targeted attackers or opportunistic malicious software. Application security focuses on keeping software and hardware free from threats and ensuring that an infiltrated application cannot access data meant to be protected. Successful security begins during the design phase, long before a program or device is deployed. Information security protects the integrity and privacy of data, whether during storage or transmission. This encompasses operational security - the processes and decisions related to managing data assets and protecting them, user permissions when accessing the network, and procedures that specify how and where data is stored or shared.14

3.4 TYPES OF CYBER THREATS15

Cybersecurity faces threats from three main aspects:

1. Cybercrimes: These encompass individual actors or groups that target systems with the aim of financial gain or disruption;
2. Cyber Espionage: Often, cyberattacks involve the gathering of information for political motivations;

3. Cyberterrorism: This form of cyber threat seeks to undermine electronic systems to incite fear and panic.

Cybersecurity is the practice of protecting systems, networks, and software from digital attacks. These electronic attacks typically aim to gain access to sensitive information, modify it, or destroy it, as well as extort money from users. Therefore, implementing effective cybersecurity measures is a particular challenge today due to the presence of more devices than people and the increasing innovation of attackers. A successful cybersecurity approach involves multiple layers of protection across devices, networks, software, and data that an organization intends to keep secure. People, processes, and technology must complement each other to establish an effective defense against cyberattacks. Threat management systems, by unifying the mechanism of integrated operations through Cisco Security software, accelerate the core security operation functions, including detection, investigation, and mitigation.16

In today's interconnected world, everyone benefits from advanced cybersecurity programs at an individual level. A cyber security breach can lead to a range of issues, from identity theft and extortion attempts to the loss of important data, such as family photos. Furthermore, critical infrastructure, including power stations, hospitals, and financial service companies, heavily relies on robust cybersecurity measures. Securing these organizations and others is essential for maintaining our society's functionality.17

Many local law enforcement departments depend on financial resources to combat cybercrimes. In this regard, leadership may consider seeking external expertise as strategic partners to help expand funding and resources. Some programs and technologies assist in enhancing the capabilities, potential, and flexibility of agencies dealing with cybercrimes. For example, the Federal Bureau of Investigation (FBI) maintains electronic task forces that are utilized by various government and local agencies to address the challenges related to cybercrimes.18

Therefore, national legislation requires periodic updates, particularly in the realm of addressing legal issues related to cybercrime. Among these issues, the lack of a clear and unified definition of cybercrimes in a specific country is a pressing matter. It is essential to establish specific definitions in domestic legislation for each cybercrime to outline its elements and

---

requirements, following the principle that "there is no crime and no punishment except by law."

As for investigating cybercrimes, it is well-known that traditional legal rules related to criminal investigations in Arab countries are not effectively equipped to deal with issues of cybercrimes due to their unique nature. Cybercrimes are characterized by their non-material, specialized technical nature, their ability to move rapidly and transcend borders, provide a different electronic identity from the real one, and the potential to cause significant remote harm. Therefore, updating these rules to be in line with this reality is crucial.

In the researcher's opinion, enhancing cybersecurity in the realm of the internet can help reduce cybercrimes through preventive measures taken by service providers. This includes enabling criminal investigations online by training investigators on how to handle digital evidence, collect electronic data, and enhancing international cooperation in combating cybercrimes. The effectiveness of the law can also be improved by establishing legislation and laws to combat cybercrimes, such as the Cybersecurity Law and the Electronic Crimes Law.

To address information security breaches in Jordanian law, the Jordanian legislator has taken measures to combat cybercrimes and ensure information security. This includes the issuance of the Electronic Crimes Law No. 17 of 2023, which contains provisions for electronic crimes and the penalties imposed on offenders. Additionally, the Cybersecurity Law No. 16 of 2019 and the old Telecommunications Law are important steps taken in this direction.

4 LAW ON ELECTRONIC CRIMES NO. 17 OF 2023

The Electronic Crimes Law of 2023 addresses various cybercrimes, including unauthorized access to information networks or information systems, or access beyond authorization. It also covers the entry, distribution, deletion, alteration, disclosure, or destruction of data, as well as interference, disruption, or disabling of an information system. Furthermore, the law criminalizes unauthorized acquisition of information related to credit cards or information used in financial transactions. The law also addresses unethical computer use.

4.1 UNAUTHORIZED ACCESS TO INFORMATION NETWORKS OR INFORMATION SYSTEMS

Article 3 of the Electronic Crimes Law stipulates penalties for those who enter information networks without permission or beyond authorization. The penalty includes imprisonment for a duration of not more than three months, with a minimum of one week. Alternatively, a fine is imposed, which is not less than 100 Jordanian Dinars and not exceeding 200 Jordanian Dinars, or both penalties simultaneously.

Moreover, if unauthorized access results in the erasure, deletion, destruction, or disclosure of data, the penalty is intensified. In such cases, the offender may be sentenced to imprisonment for no less than three months and not exceeding one year, coupled with a mandatory fine of no less than 200 Jordanian Dinars and not exceeding 1000 Jordanian Dinars. Instances of unauthorized access can involve circumventing restrictions imposed by the system's owner and accessing information without the owner's consent, such as in games and applications that typically require a financial transaction for access, but an individual gains entry through manipulation or hacking.

4.2 CRIME OF DISSEMINATING MALICIOUS PROGRAMS WITH THE INTENT TO DESTROY, DELETE, MODIFY, OR CONCEAL INFORMATION

Article 4 of the Electronic Crimes Law of 2015 outlines this crime. The article states that anyone who intentionally introduces, disseminates, or uses a program through an information network or an information system with the purpose of deleting, destroying, adding, modifying, disclosing, damaging, blocking, altering, changing, transferring, copying, capturing, enabling others to access data or information, obstructing, interfering, suspending, disabling the operation of an information system, accessing it, changing its location, deleting it, damaging it, altering its contents, occupying it, or impersonating its owner, or impersonating someone's identity without authorization or beyond authorization shall be subject to imprisonment for a period of no less than three months and no more than one year, along with a fine of no less than 200 Jordanian Dinars and no more than 1,000 Jordanian Dinars.

4.3 CYBERSECURITY LAW NO. 16 OF 2019

The Cybersecurity Law defines the cyber environment as an environment consisting of
the interaction of people, data, information, information systems, and software on information networks, as well as communication systems and the associated infrastructure. The legislator in this law focuses on regulating and managing efforts to achieve cybersecurity, establishing a center called the National Cybersecurity Center with legal personality, and defining the objectives of this center in Article 6 of the Cybersecurity Law.

4.4 TELECOMMUNICATIONS LAW NO. 13 OF 1995

The Jordanian legislator provided additional protection for human dignity, which is deemed applicable to the internet, in Article 75/A of Telecommunications Law No. 13 of 1995. The legislator inserted specific and explicit provisions that criminalize physical damage to telecommunications facilities, which necessarily include internet networks and their physical facilities. Article 72 of this law stipulates the following:

- Anyone who intentionally damages telecommunications facilities or causes damage to them is punishable by imprisonment for a period of no less than three months and no more than two years or a fine of no less than 200 Jordanian Dinars and no more than 5,000 Jordanian Dinars, or both penalties. The penalty is doubled if the act results in disrupting communication traffic.
- Anyone who negligently damages telecommunications facilities or causes damage to them is punishable by imprisonment for a period not exceeding three months or a fine not exceeding 100 Jordanian Dinars or both penalties.

4.5 PENAL CODE NO. 10 OF 2022

The Jordanian legislator introduced legal texts in the first section of the Crimes Against Property chapter that encompass a range of offenses closely related to theft, even if they do not meet all the elements of the crime of theft. Legal scholars have agreed to refer to this class of crimes as "crimes associated with theft." One of the offenses falling within this category is the crime of using another's property without right, as described in Article 416 of the Jordanian Penal Code:

- Anyone who uses, without right, something that belongs to another in a manner that causes harm without intending to embezzle that thing shall be punishable by imprisonment for up to six months or a fine of up to twenty Jordanian Dinars, or both penalties.
The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes

In the Penal Code, the Jordanian legislator addressed the crime of destruction and sabotage in the sixth section of the eleventh chapter under the title "Damage to Public and Private Property." The articles that addressed this crime clarified that destruction and sabotage apply only to real and movable properties. Article 445 of the Penal Code states that anyone who causes damage to another person's movable property of their choosing shall be punishable, upon the aggrieved party's complaint, with imprisonment for a period not exceeding one year or a fine not exceeding fifty Jordanian Dinars, or both penalties.

4.6 JORDANIAN COURTS MODEL

Judgment of the Court of Appeals in Irbid, Jordan, with reference number 5686 for the year 2021, issued on December 6, 2021. It pertains to the crime of unlawfully entering an electronic website with the intent to impersonate the owner, in accordance with the provisions of Article 3/j of the Electronic Crimes Law. We find that the following elements are required for the commission of this crime:

1. The Crime Scene: An electronic website, as defined in Article 2 of the Electronic Crimes Law, is a space for providing information on the information network through a specific address;

2. The Material Element: This is manifested through the criminal act of entering an electronic website without permission, altering it, canceling it, destroying it, or withdrawing it from its owner. This should create the appearance that the fake website is the original or that the perpetrator is the owner of the electronic site or a user. This act should lead to the commission of the criminal result for one of the purposes defined by the legal text;

3. The Moral Element: This element involves knowledge and intent, meaning that the perpetrator knows that they are entering without permission to achieve one of the purposes defined in Article 3/j of the Electronic Crimes Law, and their will is directed towards this.

5 CONCLUSION

In light of the rapid technological advancements and the increasing cyber threats, the role of cybersecurity has become crucial in enhancing the effectiveness of the law in combating cybercrimes. Based on the study conducted on the role of cybersecurity in strengthening the
effectiveness of the law in the field of combating cybercrimes, the study has concluded the following:

5.1 RESULTS

1. The role of cybersecurity in addressing cybercrimes is of significant importance in ensuring the safety of information and preserving digital security for individuals and institutions.

2. Jordanian legislation has imposed deterrent laws to combat cybercrimes, including the Electronic Crimes Law and the Cybersecurity Law.

5.2 RECOMMENDATIONS

1. It is recommended to enhance international cooperation and coordination in the field of cybersecurity to effectively combat cybercrimes.

2. The legislator is advised to establish a clear legal framework for combating cybercrimes and enhancing cybersecurity in all areas. This should include training for professionals and improving their competence.

3. It is recommended to develop the necessary technological capabilities for examining and analyzing digital evidence and tracking cybercriminals in the investigation of internet-related crimes.

REFERENCES


The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes


Electronic Crimes Law for the year 2015.


Jordanian Cybersecurity Law No. 16 of 2019.

Judgment of Irbid Criminal Court in its appellate capacity, No. 5686 of 2021, issued on December 6, 2021.


