**Migration Letters**

Volume: 21, No: S4 (2024), pp. 816-828

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

# Legislative Evolution Of Cyber Security In Jordanian Law

Dr. Alaa Majed Ahmad Bani Younes[1], Dr. Ammar Mahmoud Ayoub Al-Rawashed[2], Aseel Mahmoud AL RASHDAN[3], Dr. Ahmad Fahed Mohammad AlBtoosh[4]

## Abstract

*In this study, we aim to study the development of cyber security legislation in Jordan and find out how effective these laws are in reducing this type of crime and the efforts made by the Jordanian government to raise awareness and development in cyber security via known challenges facing the government during the development of this legislation and contributions, the analytical approach was used in this study, by presenting the cyber security laws and legislations in Jordan and comparing them with the number of cybercrimes and cyber-attacks that occurred in recent years.*

*We conclude from this study that we see that there are still areas in which the legal framework for cybersecurity in Jordan can be improved and that in some cases the government was unable to identify the perpetrator of the attack, so it is good to develop the techniques used to detect the perpetrators of the hack to enable the application of the penalties provided for in the law.*

***Keywords**: Cybersecurity, cybercrime, laws and legislations, Jordan.*

## 1. Introduction

The increasing reliance on technology and the internet have made the cybersecurity a critical concern for governments worldwide. Jordan is no exception, as it has witnessed a significant increase in the number of cyber-attacks in recent years. To address this issue, the Jordanian government has taken several steps to develop its legal framework related to cybersecurity. This has included the enactment of various laws and regulations aimed at protecting individuals, organizations, and the country's critical infrastructure from cyber threats. (1 AL-SOUD & AL- ASFOUR, (2020). Jordan's cybersecurity strategy in the light of the constitutional and legislative framework. Journal of Applied Security Research, 15 (4), P P 469-483. )

The tremendous development of digital technology and the rapid access of individuals to the internet has led to tremendous and rapid development in such issues as completing transactions, receiving and providing s[1]ervices, communicating with individuals, and creating new areas for expressing ideas. However, this development has increased the possibility of violating the right to privacy by causing risks such as monitoring, tracking, and disclosure of the private life of individuals. Therefore, given all these developments and risks, the classical understanding of

[1]Assistant Professor Faculty of Law Department of Private Law University: Jerash University Jerash, Jordan.
[2]Associate Professor Faculty: Faculty of Law Department: Department of Private Law University: Jerash University Jerash, Jordan.
[3]Assistant Professor Faculty of Law Department: Department of Private Law University: Jerash University Jerash, Jordan.
[4]Associate Professor Faculty of Law Department of Private Law Ajloun National University Ajloun, Jordan.

privacy has been restored, which is limited to some ethical dimensions related to values such as the right to protect the reputation, honor, and dignity of individuals, and usually, physical dimensions such as residential immunity need addressing. For this reason, it was necessary for a new understanding of privacy to emerge that covers all aspects of attacks on the rights, freedoms, and personal data of individuals. The new understanding in question differs from the right to privacy in its classical version in terms of its elements and characteristics, digital privacy is an understanding related to the development of technologies and the spread of the internet, cyberspace, telecommunications, computer systems, intranets, technical technologies of cellular technologies and cable and satellite communication services. Cyberspace is also about the components that make it up, as the common memory of all mankind it is described that the logistical elements that enable the operation of cyber activities are also accepted as common property. (2 AL-SOUD & AL- ASFOUR, (2020). Jordan's cybersecurity strategy in the light of the constitutional and legislative framework. Journal of Applied Security Research, 15 (4), P P 469-483.)

As a result of the cyberattack, the countries secret some infrastructures created within their structure, in addition to the lack of a clear constitutional text regulating the right to digital privacy with its understanding and its new nature in the Jordanian constitutions, also there has been no development comparable to the rapid digital developments in the legal legislation regulating the world. For this reason, there are some scattered articles in the legal regulations in the Jordanian constitution, old and different laws that deal with this right. The most prominent of these laws is the Cybercrime Law and the cybersecurity law in Jordan, which includes clear violations of the right to digital privacy in some of its articles. Despite the lack of a comprehensive constitutional, legal, and regulatory framework, digital developments affecting privacy continue to increase, The importance of the study lies in shedding light on the legislation in the Jordanian laws related to cyber security, because of its effects on the loss of rights and destruction of property and its impact on economic, social and intellectual security.

Due to the high possibility of hacking into networks and controlling them completely or partially and the high number of cybercrimes, the Jordanian government should have imposed laws and legislation to limit the commission of such crimes. Therefore, in this study, we will present the legislative development of cybersecurity in Jordanian law. (3 Saleh, M., Al Saud, M., Sparrow, A. (2019). Cybersecurity and cybercrime legislation in Jordan: an overview. International Journal of intelligence cybersecurity and cybercrime, 8 (1), 1-16)

### 1.1. The Study Problem:

Due to the increasing dependence on technology and the internet and the increasing use in light of the advancement of networks and technologies, it was natural to increase the number of cybercrimes and cyber-attacks, but in light of this progress, the government has taken many legislations and laws and developed them and efforts have been made to reduce this type of crime, The research problem lies in knowing the identification of the development of these legislations and knowing the extent of their effectiveness and whether they were highly efficient in addressing any attacks or electronic wars that could affect citizens and the Jordanian society and the cyber attacks that occurred in recent years and were these laws effective in reducing this type of crime.

### 1.2. The Study Importance:

The importance of the research appears in knowing the sequence of Jordanian legislation governing the protection of cybersecurity services, and identifying effective laws to prevent

any electronic attacks that threaten individuals, companies, or the country as a whole, and the measures taken to protect systems and networks in following appropriate security measures to address any electronic incident and knowing their effectiveness and efficiency.

**1.2. The Study Objectives:**

The study aims to:

- Identify the concept and techniques of cybersecurity in Jordan.

- Knowledge of cybersecurity laws and legislations and their developments.

- Identify the efforts made by the government to develop cybersecurity in Jordan.

- Knowledge of the reality of electronic crimes and cyber-attacks in Jordan.

- Finding out how effective the laws are in reducing cybercrime and cyber-attacks.

**2. Methodology:**

The researcher uses the analytical approach by presenting the cyber security laws and legislations in Jordan and comparing them with the number of cybercrimes and cyber-attacks that occurred in recent years, which were effective in reducing this type of crime.

**3. The concept of cyber security and cyber attacks.**

**3.1. The concept of cyber security**

Cybersecurity is an application for protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as IT security or electronic information security. This term is applicable in a variety of contexts, from companies to mobile phone information processing. (4 John Erickson. (2008). Hacking is the art of exploitation. p. 253-254.)

Cyber security can be divided into several subsections:

**1. Network security:** is the practice of protecting a computer network from hackers, regardless of whether they are targeted attackers or opportunistic malware

**2. Security of Access Applications:** Focuses on data and ensuring that software and hardware are not affected by threats. A compromised app could provide access to the data it was designed to protect. Successful security even begins at the design stage before software or hardware is deployed.

**3. Information Security:** Information security ensures the integrity and confidentiality of data during storage and transmission.

**4. Operational Security Operations:** includes operational processes and decisions related to the handling and protection of data assets. The permissions that users have when accessing a network and the actions that determine how and where data is stored or shared fall within this scope.

**3.2 The concept of Cyber attacks**

Cyber attacks is the attacks carried out by professional hackers or hacker groups on computers and the internet on websites, networks, and computers of companies or individuals to make a profit and cause damage. In a 2009 study conducted at the National Research Council of the United States, it was defined the Cyber-attacks as: Actions taken to disrupt, deceive, humiliate,

or destroy networks, computer systems, or the information and software embedded in or carrying them". (5 National Research Council (USA) Commission on the Trustworthiness of Information Systems. (2009). towards a safer and more secure cyberspace. National Academies Press (USA).

These attacks are performed through a computer to eliminate the availability of the designated target computer. During the attack, it aims to slow down the computer and the networks used by the computer as much as possible and render them unusable. Since it is implemented with the support of more than one computer and connection at the same time, its scope can cause more damage. Internal firewalls or content filters should be used for blocking. )6 Vandals, A.; (2013). Electronic attacks and their impact on the banking sector. International Journal of Cybersecurity and Digital Forensics, 2(4), 196-206.)

In recent years, the damage caused by cyber-attacks has seriously threatened enterprises. It was imperative to protect information from cyber-attacks, confidentiality of processed information, and integrity by taking measures against cyber-attacks and disclosing them.

Therefore, it was necessary to know the legal regulation of the Jordanian legislator, which was defined in Cyber Security Law No. 16 of 2019, and to put in place measures to protect information systems, networks, and infrastructure, which constitute a group of electronic systems and networks to ensure the security of the state, its economy, and the safety of society, and this is what will be dealt with in the second topic.

## 4. Efforts and development of cyber security law legislation in the Kingdom of Jordan

There are many concerted efforts to put in place measures to protect systems and networks from threats to information systems and infrastructure. When the Jordanian government submitted the draft law, it was studied from all technical, organizational and procedural aspects to prevent and limit attacks against various state agencies. There are two cyber security institutions that are subject to oversight. The House of Representatives so that there is a National Council for Cyber security that undertakes approving strategies, policies, plans and standards related to cyber security and enjoys a legal personality with financial and administrative independence to build an effective system for cyber security at the national level and confront threats efficiently and effectively to maintain national security and the safety of people and property, and the law obliges the persons and agencies that provide Cyber security services in the Kingdom to rectify their situation in accordance with the law, regulations and instructions issued pursuant thereto, with the prohibition of providing any cyber security services without a license. The National Center for Cyber security Regulation No. 1 of 2020 was issued, consisting of seven articles.

Thus, cyber threats can be classified into two types: cybercrimes against individuals, companies, etc., and threats against the state, and this is what will be dealt with in the first requirement.

### 4.1. Electronic crimes and cyber-attacks in Jordan

Statistics and studies indicate a high rate of cybercrime in Jordan, which shows that the most important motives are financial motives, the desire for entertainment, the love of fame, religious, sexual and political purposes, and the high rate of commission due to the ease of commission and the ease of disposal of digital evidence. In 2018, the number of cybercrimes was equal to 2038, while in 2019 The number of crimes was 12,872, and in 2020 the number of crimes was 9,514, while in 2021 the number of crimes was 13,000. In 2021, the number of

cases of hacking and cyberattacks was 897, of which 34% were related to users, 27% were international breaches "or from state entities", 26% were related to cybercrimes, and 13% were related to terrorist organizations. (7 Criminal Investigation Department. Jordanian public security.

) Among the most prominent targets for penetration are the military and security institutions, the financial sector, and the energy sector, “electricity companies.” These attacks and penetrations aimed at espionage and information collection by 4%, data and information theft by 21%, and data and information theft for political and economic goals. 4% and 33% for other goals. According to the statements of the National Center for Cyber Security, there are no prosecutions or lawsuits related to these attacks! And that it is difficult to determine the location of the attack. According to studies, there has been a 6-fold increase in the rates of cybercrime and cyber attacks since 2015. (8 National Center for Cyber Security. And public safety statement.)

- Among the most prominent of these attacks:

1- In 2018, the Jordanian government experienced a major cyberattack that targeted its email system. The attack, believed to have been carried out by state-sponsored hackers, compromised the email accounts of several government officials and departments. Hackers managed to steal sensitive information and disrupt government operations for days. (9 BBC News (2018). Jordan under massive cyberattack".)

2- In 2016, a group of hackers claiming affiliation with ISIS launched a cyberattack on several Jordanian government websites, including the Ministry of Interior and Ministry of Justice. The attackers defaced websites with pro-ISIS messages and images, causing embarrassment to the government.

3- In 2013, a group of hackers calling themselves the Jordan Electronic Army targeted several news websites, including those of Al Jazeera and the BBC. The attackers managed to hack and deface websites with pro-Assad messages, as the group is believed to be allied with the Syrian government. (10) BBC News. (2013). Jordanian pirates strike Al-Jazeera and the BBC" - BBC News, March 31, Article, p. 7)

4- In May 2018, several Jordanian banks were subjected to a cyber attack targeting their ATMs. The attackers used a variant of the Fastcash malware to make concessions to banks' networks and steal cash from their ATMs. (11 BBC News. (2018). Jordanian banks under 'quick cash' cyberattack, May 30, Article, p. 4)

5- In May 2017, Jordan's official Petra News Agency was hacked and its website was defaced with fake news articles. The attackers also claimed to have stolen sensitive information, including emails and government documents. (12 Reuters. (2017). The Jordan News Agency website was hacked and fake news was published", May 9, Article, p. 8)

6- In January 2013, the Arab Bank, one of the largest banks in Jordan, was subjected to a cyber attack that caused a major disruption to its online banking services. The attack was attributed to the "Izz al-Din al-Qassam Cyber Fighters," a hacktivist group that launched similar attacks against several American banks. (13 Reuters. (2013). The Arab Jordan Bank is subject to a cyberattack", January 23, article, pp. 9-11)

7- Jordan Nuclear Energy Commission (2018) Cyber Attack In September 2018, the Jordan Nuclear Energy Commission was subjected to a cyberattack that targeted its computer systems. The attack was attributed to a state-sponsored hacking group known as Charming Kitten, which

has been linked to Iran. (14 NBC News. (2018). Iran hackers tried to hack US energy grid, caught by industry cybersecurity", September 27, Article, p.9)

8- The cyber-attack of the National Electric Power Company (2015) In December 2015, the Jordanian National Electric Power Company was subjected to a cyber attack that caused widespread power outages in the capital, Amman. The attack was attributed to a group of hackers from Syria. (15 The Guardian, 24 December 2015, article p. 9.)

9- Jordan Customs Department Cyberattack (2018) - In August 2018, the Jordan Customs Department was subjected to a cyberattack that disrupted its services. The attack was attributed to a group of hackers known as "Anonymous Jordan." (16 Reuters. (2018). The Jordanian Customs Department was disrupted due to the electronic attack", August 15, article, p. 13)

10- Jordan Civil Service Office Cyber Attack (2016) - In May 2016, the Jordan Civil Service Office was subjected to a cyber attack targeting its website and causing it to shut down for several hours. The attack was attributed to a group of infiltrators from Algeria. (17 Morocco World News. (2016). The website of the Civil Service Office was hacked by Algerian hackers", May 24, article, pp. 1-2)

11- Jordanian Ministry of Foreign Affairs cyberattack (2015) - In February 2015, the Jordanian Ministry of Foreign Affairs was subjected to a cyberattack targeting its email system. The attack was attributed to a group of hackers from Russia. (18 Jordanian Ministry of Foreign Affairs. Jordan News. Article p. 3.)

12- In October 2013, several Jordanian government websites were hacked and defaced with political messages. The attack was attributed to a group of infiltrators from Algeria. (19 Jordanian General Intelligence. Article p. 11.)

13- In June 2016, the Jordanian Ministry of Interior was subjected to a cyber attack targeting its website, causing it to shut down for several hours. The attack was attributed to a group of hackers from Morocco. (20 Al-Jazeera. (2016). The website of the Jordanian Ministry of Interior was hacked", June 5, article, p. 8)

14- In January 2012, several Jordanian government websites were hacked and defaced with political messages. The attack was attributed to a group of infiltrators from Tunisia (21 The Verge. (2012). Hacking of Jordanian government websites by the "Tunisian Cyber Revolution Group", January 5, article, p. 4)

The Cybercrime Unit of the Public Security Directorate renews its warning against dealing with fake accounts and strangers who use the names of spiritual healing and witchcraft to attract their victims, because cyberspace is a fertile environment for rumors, through social networking sites and other digital means.

### 4.2. Developing cyber security law legislation in the Kingdom of Jordan

Jordan has made significant strides in developing cyber security laws and regulations in recent years. The state has realized the importance of cyber security in protecting its vital infrastructure, business and citizens from cyber threats. We will present the developments of the laws that occurred in Jordan:

#### 4.2.1. Electronic Transactions Law No. 15 of 2015

The law addresses issues related to electronic fraud and piracy in Jordan The law provides a framework for electronic transactions, including digital signatures, electronic records, and

electronic contracts. It also contains provisions relating to electronic fraud and hacking. Under the Electronic Transactions Act, it is a criminal offense to gain unauthorized access to computer systems, networks, or data. Any person who obtains unauthorized access to a computer system or network intending to commit a crime or obtain confidential information shall be liable to imprisonment for a term not exceeding three years and/or a fine not exceeding 3000 Jordanian dinars, as the law criminalizes the act of hacking, which is defined as accessing a system or a computer network with the intent to cause damage or disruption to the system or network. Any person who commits an act of piracy shall be subject to imprisonment for a term not exceeding three years and/or a fine not exceeding 5,000 dinars. The Electronic Transactions Law deals with issues related to electronic fraud, such as the use of false electronic records or electronic signatures to commit fraud. The Jordanian National Team has also been established to respond to cases of Computer Emergencies in 2004 to provide a central point of contact for reporting and responding to cyber incidents. (22 Cybercrime Law in Jordan: Definition, Effects and Implications, 2015.)

The center also works with government agencies, critical infrastructure operators, and private sector organizations to enhance the country's cybersecurity capabilities and respond to cyber threats. The government passed the Encryption and Electronic Signature Law in 2009 to provide a legal framework for electronic signatures and encryption. The law guarantees the legal validity of electronic transactions and protects the confidentiality and integrity of electronic data.

### 4.2.2. Cybercrime Law in 2010:

Jordan passed the Cybercrime Law (No. 30) which criminalizes a range of electronic activities, including unauthorized access to computer systems, data interception, and electronic fraud. The law also stipulates penalties for those who commit cybercrimes, including fines and imprisonment. (23 Cybercrime Law, the official newspaper. Prime Minister 2010.)

Jordan enacted the Cybercrime Law, which criminalizes a wide range of cybercrime, including unauthorized access, hacking, identity theft, cyberterrorism, and cyberstalking. The law also includes provisions that specifically address attacks on critical infrastructure. The Cybercrime Law imposes prison penalties and fines for cybercrime, and stipulates the confiscation of equipment and data.

### 4.2.3. Electronic Signature Law No. 15 of 2017:

This law provides for the legal recognition of electronic signatures in Jordan and establishes rules for their use in electronic transactions. It also establishes a certification process for electronic signature providers to ensure the integrity and security of electronic signatures. (24 Jordanian Electronic Signature Law No. 15 of 2017", Global Risk Advisor Law, 2018.)

### 4.2.4. Information Technology Crime Law No. 11 of 2019:

This law criminalizes various types of information technology crimes, including unauthorized access to computer systems, hacking, and spreading false information online. It provides for penalties ranging from fines to up to ten years in prison. (25 Jordan Information Technology Law No. 11 of 2019", Global Risk Consultant Law, 2020.)

### 4.2.5. Electronic Transactions Law No. 85 of 2019:

This law regulates electronic transactions in Jordan and provides for the legal recognition of electronic signatures, contracts, and documents. It also sets rules for data protection and privacy

in electronic transactions. (26 Jordan: A New Law on Information Technology Crimes, Global Legal Observatory, Library of Congress. 11 of 2019, pp. 23-24.)

#### 4.2.6. Personal Data Protection Law No. 30 of 2020:

This law defines the rules for collecting, processing, and using personal data in Jordan. Requires data controllers to obtain consent from data subjects before collecting and processing their data, and imposes penalties for non-compliance. (27 Personal Data Protection Law No. 30 of 2020," Jordanian Ministry of Justice.)

#### 4.2.7. Jordan's Cyber security Strategy 2020-2024:

This strategy aims to enhance Jordan's cyber security capabilities and resilience by strengthening the country's legal and regulatory frameworks, developing cyber security-related infrastructure and services, and promoting awareness and education in the field of cyber security. (28 The National Cybersecurity Strategy for Jordan 2020-2024 Implementation and Evaluation." Jordan Information Technology Association.)

### 4.3. Contributions made by Jordan to the development of cyber security

Jordan has made a number of contributions to the development of cyber security and protection from cross-border cyber attacks, the most important of which is:

#### 4.3.1. The National Center for Security and Crisis Management:

Jordan established a National Center for Security and Crisis Management in 2015, which is responsible for coordinating cybersecurity efforts across the country. The center works to improve cyber security resilience, detect and respond to cyber threats, and strengthen national cyber security policies. (29 The official website of the National Council for Cyber Security: http://www.ncscm.gov.jo/.)

#### 4.3.2. Jordan Cyber Emergency Response Team:

The Jordan Cyber Emergency Response Team was established in 2010 to provide rapid responses to cyber incidents and support national cyber security efforts. The team works closely with the National Counter Terrorism Council and other government agencies to coordinate responses to cyber threats. (30 Cybersecurity and Electronic Warfare: What Everyone Needs to Know by B.W. Singer and Alan Friedman. M-13.)

#### 4.3.3. Jordan Cyber Security Forum:

The Jordan Cybersecurity Forum is an annual event that brings together cybersecurity experts and stakeholders from around the world to discuss the latest trends, challenges, and opportunities in the field. The forum provides a platform for sharing knowledge and best practices, for networking and collaboration. (31 National Center for Cyber Security. Published report. 2018 p. 17.)

#### 4.3.4. Jordan Cyber Security Council: in 2019

Jordan established a cybersecurity council to oversee the implementation of the national cybersecurity strategy and coordinate cybersecurity efforts across government agencies, the private sector, and civil society. The Board is responsible for identifying cybersecurity risks and developing policies and procedures to mitigate them. (32 The Jordanian National Center for Information Technology. Published report. 2019. p.23.)

**4.3.5. Cyber Defense Center of the Jordanian Armed Forces:**

The Jordan Armed Forces Cyber Defense Center was established in 2016 to protect military networks and systems from cyber-attacks. The center works closely with Jordan Certification and other government agencies to ensure national cyber security resilience. (33 Jordanian Armed Forces. Cyber security. An article. p. 8.)

**4.3.6. The Jordanian Advanced Research and Education Network:**

The Jordan Advanced Research and Education Network (JANNET) is a high-speed network infrastructure that connects universities and research institutions across Jordan. The network provides advanced cybersecurity features to protect sensitive research data and intellectual property. (34 Jordan Advanced Research and Education Network (Janet). "The Center for Information Exchange and Analysis of Research and Education Networks. Article. p. 42.)

**4.3.7. Cyber security incident reporting system in 2019**

Jordan has launched a cyber security incident reporting system that aims to facilitate the reporting of cyber incidents by individuals, companies, and government agencies. The system allows users to report incidents anonymously and provides a platform for sharing information and best practices. (35 Cyber Security Incident Response System - Jordan Times, 17 June 2019. s. 16.)

**4.3.8. National encryption policy in 2020:**

Jordan has launched a national encryption policy aimed at protecting the privacy and security of communications and data within the country. The policy sets guidelines for the use of encryption by individuals, businesses, and government agencies, and establishes a national cryptographic authority to oversee implementation and compliance. (36 National Encryption Data Privacy Protection." Jordan Times, August 31, 2020.)

**4.3.9. The Jordanian National Program for Information Security and Privacy:**

This program is designed to promote cyber security and privacy awareness among government employees and the public. It includes training and awareness programs, as well as guidelines for securing government information systems. (37 Jordanian electronic government. Information security service and network accidents. p. 34. 2021.)

**4.3.10. Jordan Information and Communication Technology Association:**

This association represents the Jordanian information and communication technology sector and works to promote the development of the sector, including its capabilities in the field of cybersecurity. (38 Mobile World Congress 2021, Jordanian technological developments in the fields of 5G, the Internet of Things, and artificial intelligence. article. p.13)

**4.3.11. The Jordanian Coalition for Cyber Security:**

This alliance brings together government agencies, private sector organizations, and academic institutions to enhance cyber security in Jordan. Its activities include cybersecurity awareness campaigns, research and development initiatives, and policy advocacy.

**4.3.12. Cyber Security Infrastructure:**

Jordan has invested in developing robust cybersecurity infrastructure, such as secure data centers and advanced network security systems. For example, the Jordanian government has

established a national data center that provides secure hosting services to government agencies and companies.

**4.3.13. Cooperation with regional and international partners:**

Jordan has been engaged in active cooperation with regional and international partners on cybersecurity issues, including through participation in initiatives such as the Arab Regional Center for Cyber Security and the Global Forum for Cyber Expertise. Jordan has also signed cybersecurity agreements with countries such as the United States, France, and Germany, intending to enhance cooperation and information exchange.

**4.3.14. Cybersecurity awareness campaigns:**

Jordan has launched several cyber security awareness campaigns aimed at increasing public awareness of cyber threats and promoting best practices for online safety. These campaigns target various sectors of society, including students, businesses, and government employees. (39) Information Security and Network Incidents Service - E-Government. 2020. p. 22)

**4.3.15. Cyber security for e-government services:**

Jordan has implemented e-government services that require robust cybersecurity measures to protect citizens' data and government systems. The Jordanian government has established a security center dedicated to e-government to provide secure hosting services, monitor e-government systems and respond to electronic incidents. (40 Slate, Azzam. (2022). Cyber security for smart city Jordan. p. 54)

**4.3.16. Cyber security for smart cities:**

Jordan has embraced the concept of smart cities and recognized the importance of cyber security for these urban environments. The Greater Amman Municipality has established a smart city program that includes cybersecurity measures to protect citizen data and critical infrastructure.

**4.3.17. The Jordanian National Strategy for Information Technology 2019-2022:**

This strategy aims to promote the development of the information technology sector in Jordan and enhance its competitiveness on the global stage. It includes a focus on cybersecurity, with measures to raise awareness and education about cybersecurity risks, develop national policies and standards for cybersecurity, and enhance the ability of the government and the private sector to respond to cybersecurity incidents.

**4.4. The effectiveness of current laws and regulations in addressing cyber threats in Jordan**

Because of the number of crimes and cyber attacks committed in recent years and the number of existing cases, we find that these laws have not proven their effectiveness and efficiency and that they need further development, especially in many cases that the party that carried out the attack has not been identified, but given the rapid technical development and methods, The advanced level with which the attack is carried out makes it difficult to identify the party that attacked unless it leaves evidence or even a loophole. Therefore, hackers, hackers, and malware writers are one step ahead of the Jordanian government. We must look at developing the technologies used in Jordanian cybersecurity to reduce the percentage of this. Crimes Just as cybersecurity is still a recent development in Jordan; the matter is not limited only to legislation

and laws, but rather to developing the techniques used to arrest the perpetrators of this infiltration!

## 5. Conclusion

In Article 2 of the Cybersecurity Law No. 16 of 2019, the Jordanian law states that cybersecurity is a set of measures taken to protect information systems, networks, critical infrastructure, and all technical and administrative activities in the field of cybersecurity, as it has become an integral part of society's security, which confirms that There must be a legal organization and legislative development in line with these developments and the protection of individuals, companies and the state.

Jordan has also made efforts to develop legislation to confront cybersecurity threats in recent years, including laws and legislation that aim to reduce cybercrime and cybersecurity attacks. That there are still areas in which the legal framework for cybersecurity in Jordan can be improved, and in some cases the government was unable to identify the party that carried out the attack, so it is good to develop the techniques used to detect the parties that carried out the breach to be able to apply the penalties stipulated in the law.

## 6. Recommendations

- We recommend developing the infrastructure and technologies used in cybersecurity, awareness of cybersecurity as it is still new in Jordan,
- Enacting new legislation that will reduce crimes to address the gaps in the legal framework and he must continue to invest in his national strategy for cybersecurity.
- Enhance awareness of cybersecurity among the general public, increase the capacity of cybersecurity verification teams in the Hashemite Kingdom of Jordan, and improve cooperation with international partners on cybersecurity issues.
- We recommend the Jordanian legislator introduce amendments or add articles, as we find that there are legislative shortcomings because the Cyber Security Law has not established a specific mechanism to regulate cyber security services and did not specify penalties if there is a breach of the obligations to provide these services.
- Updating strategic plans in line with the technological developments taking place in the Kingdom to prevent any electronic accidents or electronic wars that threaten our security and the safety of Jordanian society.
- Educating workers and employees in the public and private sectors and individuals in all state institutions to develop professional standards, warn against unsafe use of information technology, and spread the culture of use more effectively to maintain a good level of cybersecurity and safety.
- Develop frameworks and implementation plans and address gaps related to information security by the National Center for Cybersecurity to protect electronic government networks and vital sectors related to national security, as protecting government networks from attacks contributes to supporting the economy.
- Strengthening Response to Cybersecurity Incidents: While the Jordanian Computer Emergency Response Team is responsible for monitoring and responding to cybersecurity incidents, there is a need to strengthen incident response capabilities. This could include developing standard operating procedures for incident response and investing in additional resources and technology to support these efforts.
- Adopt stronger regulations and legal frameworks to support data protection. This includes regulations about data retention and privacy and data breach notification.
- Increase the severity of penalties for cybercrime to discourage individuals from engaging in such activities.

## 7. References

(1-2) AL-SOUD & AL- ASFOUR, (2020). Jordan's cybersecurity strategy in the light of the constitutional and legislative framework. Journal of Applied Security Research, 15 (4), P P 469-483.
(3) Saleh, M., Al Saud, M., Sparrow, A. (2019). Cybersecurity and cybercrime legislation in Jordan: an overview. International Journal of intelligence cybersecurity and cybercrime, 8 (1), 1-16
(4) John Erickson. (2008). Hacking is the art of exploitation. p. 253-254.
(5) National Research Council (USA) Commission on the Trustworthiness of Information Systems. (2009). towards a safer and more secure cyberspace. National Academies Press (USA).
(6) Vandals, A.; (2013). Electronic attacks and their impact on the banking sector. International Journal of Cybersecurity and Digital Forensics, 2(4), 196-206.
(7) Criminal Investigation Department. Jordanian public security.
(8) National Center for Cyber Security. And public safety statement.
(9) BBC News (2018). Jordan under massive cyberattack".
(10) BBC News. (2013). Jordanian pirates strike Al-Jazeera and the BBC" - BBC News, March 31, Article, p. 7
(11) BBC News. (2018). Jordanian banks under 'quick cash' cyberattack, May 30, Article, p. 4
(12) Reuters. (2017). The Jordan News Agency website was hacked and fake news was published", May 9, Article, p. 8
(13) Reuters. (2013). The Arab Jordan Bank is subject to a cyberattack", January 23, article, pp. 9-11
(14) NBC News. (2018). Iran hackers tried to hack US energy grid, caught by industry cybersecurity", September 27, Article, p.9
(15) The Guardian, 24 December 2015, article p. 9.
(16) Reuters. (2018). The Jordanian Customs Department was disrupted due to the electronic attack", August 15, article, p. 13
(17) Morocco World News. (2016). The website of the Civil Service Office was hacked by Algerian hackers", May 24, article, pp. 1-2
(18) Jordanian Ministry of Foreign Affairs. Jordan News. Article p. 3.
(19) Jordanian General Intelligence. Article p. 11.
(20) Al-Jazeera. (2016). The website of the Jordanian Ministry of Interior was hacked", June 5, article, p. 8
(21) The Verge. (2012). Hacking of Jordanian government websites by the "Tunisian Cyber Revolution Group", January 5, article, p. 4
(22) Cybercrime Law in Jordan: Definition, Effects and Implications, 2015.
(23) Cybercrime Law, the official newspaper. Prime Minister 2010.
(24) Jordanian Electronic Signature Law No. 15 of 2017", Global Risk Advisor Law, 2018.
(25) Jordan Information Technology Law No. 11 of 2019", Global Risk Consultant Law, 2020.
(26) Jordan: A New Law on Information Technology Crimes, Global Legal Observatory, Library of Congress. 11 of 2019, pp. 23-24.
(27) Personal Data Protection Law No. 30 of 2020," Jordanian Ministry of Justice.
(28) The National Cybersecurity Strategy for Jordan 2020-2024 Implementation and Evaluation." Jordan Information Technology Association.
(29) The official website of the National Council for Cyber Security: http://www.ncscm.gov.jo/.
(30) Cybersecurity and Electronic Warfare: What Everyone Needs to Know by B.W. Singer and Alan Friedman. M-13.
(31) National Center for Cyber Security. Published report. 2018 p. 17.
(32) The Jordanian National Center for Information Technology. Published report. 2019. p.23.
(33) Jordanian Armed Forces. Cyber security. An article. p. 8.
(34) Jordan Advanced Research and Education Network (Janet). "The Center for Information Exchange and Analysis of Research and Education Networks. Article. p. 42.
(35) Cyber Security Incident Response System - Jordan Times, 17 June 2019. s. 16.
(36) National Encryption Data Privacy Protection." Jordan Times, August 31, 2020.
(37) Jordanian electronic government. Information security service and network accidents. p. 34. 2021.

(38) Mobile World Congress 2021, Jordanian technological developments in the fields of 5G, the Internet of Things, and artificial intelligence. article. p.13
(39) Information Security and Network Incidents Service - E-Government. 2020. p. 22
(40) Slate, Azzam. (2022). Cyber security for smart city Jordan. p. 54