Relações Internacionais do Mundo Atual – unicuritiba

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: **2316-2880**

LEGISLATIVE DEVELOPMENTS OF CYBERSECURITY INCIDENTS IN JORDAN: A CRITICAL ANALYTICAL STUDY UNTIL 2024

DESENVOLVIMENTOS LEGISLATIVOS DOS INCIDENTES DE SEGURANÇA CIBERNÉTICA NA JORDÂNIA: UM ESTUDO ANALÍTICO CRÍTICO ATÉ 2024

MAMOON AHMAD AL-HUNAITI*
Faculty of Law, Middle East University, Amman, Jordan. E-mail: Malhunaiti@meu.edu.jo Orcid id: https://orcid.org/0009-0003-6614-4242

MOHAMMAD TAHA ALFLAIEH
Faculty of Law, Middle East University, Amman, Jordan. E-mail: malflaieh@meu.edu.jo Orcid id: https://orcid.org/0009-0002-1298-0002

ATEF SALEM AL AWAMLEH
Faculty of Law, Al Balqa' Applied University, Amman, Jordan. E-mail: Dr.atefalawamleh@bau.edu.jo Orcid id: https://orcid.org/0009-0001-9061-4289

ASM'A MOHAMMED AL RAGGAD
Faculty of Law, Al Balqa' Applied University, Amman, Jordan. E-mail: Dr.asma@bau.edu.jo Orcid id: https://orcid.org/0000-0002-1428-4265

ABSTRACT

Objective: This study aims to elucidate the evolving legislative framework governing cybersecurity incidents in Jordan, with a focus on legislative developments from 2019 to 2024. It seeks to assess the adequacy of current laws and propose enhancements to strengthen cybersecurity governance.

Methods: A comparative methodology alongside a critical analytical approach was employed, examining the current legal provisions regulating cybersecurity in Jordan and comparing them with international standards such as the EU's NIS2 Directive and the Strengthening American Cybersecurity Act of 2023.

Results: The study outlines significant legal developments in Jordan's cybersecurity laws and highlights gaps that may hinder effective cybersecurity management. It proposes specific legislative reforms aimed at enhancing the legal framework, particularly in areas of incident reporting and response to AI-driven threats.

Conclusion: The study concludes that Jordan needs to implement comprehensive legislative reforms to align its cybersecurity policies with international norms to enhance its national cybersecurity resilience effectively.

Keywords: Cyber incidentes; Cyber security; Cyberspace; Cyber threats.

Relações Internacionais do Mundo Atual – unicuritiba
Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: **2316-2880**

RESUMO

Objetivo: Este estudo visa elucidar o quadro legislativo em evolução que governa os incidentes de segurança cibernética na Jordânia, com foco nos desenvolvimentos legislativos de 2019 a 2024. Procura avaliar a adequação das leis atuais e propor melhorias para fortalecer a governança de segurança cibernética.

Métodos: Foi empregada uma metodologia comparativa juntamente com uma abordagem analítica crítica, examinando as disposições legais atuais que regulam a segurança cibernética na Jordânia e comparando-as com padrões internacionais como a Diretiva NIS2 da União Europeia e o Ato de Fortalecimento da Segurança Cibernética Americana de 2023.

Resultados: O estudo delineia desenvolvimentos legais significativos nas leis de segurança cibernética da Jordânia e destaca lacunas que podem impedir uma gestão eficaz da segurança cibernética. Propõe reformas legislativas específicas destinadas a aprimorar o quadro legal, particularmente nas áreas de relatórios de incidentes e resposta a ameaças impulsionadas por IA.

Conclusão: O estudo conclui que a Jordânia precisa implementar reformas legislativas abrangentes para alinhar suas políticas de segurança cibernética com as normas internacionais para aprimorar efetivamente sua resiliência cibernética nacional.

Palavras-chave: Incidentes cibernéticos; Segurança cibernética; Ciberespaço; Ameaças cibernéticas.

Relações Internacionais do Mundo Atual – unicuritiba
Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

1. INTRODUCTION

The Jordanian Cybersecurity Act of 2019 established the foundation for cybersecurity governance in Jordan. However, since its enactment, the evolving nature of cyber threats has necessitated legislative updates. In 2021, Jordan introduced the National Cybersecurity Strategy, followed by legal amendments in 2023 that focused on cybersecurity incident reporting and governance. These changes align with global cybersecurity developments, such as the European Union's NIS2 Directive and the United States' Strengthening American Cybersecurity Act of 2023. Nevertheless, further legal refinements are needed to address emerging challenges, particularly those posed by AI-driven cyber threats and the rapid expansion of IoT devices.

This research aims to examine the legal regulation of cybersecurity incidents under the Jordanian Cybersecurity Act, with a focus on the Act's conceptual and objective framework. By analysing the provisions and provisions of the Act, as well as its implementation and effectiveness in addressing and regulating cybersecurity incidents in Jordan, this research will identify the strengths and weaknesses of the Act and its impact on cybersecurity in the country. In addition, this research will also consider the challenges and limitations of the Act in regulating cybersecurity incidents, as well as potential avenues for improvement. Through this analysis, this research hopes to provide a comprehensive understanding of the legal regulation of cybersecurity incidents under the Jordanian Cybersecurity Act.

This research will adopt a comparative methodology in examining the legal regulation of cyber incidents under the Jordanian Cybersecurity Act. By comparing the Act to other legal frameworks and approaches to regulating cyber incidents, this research will provide a nuanced analysis of the effectiveness and limitations of the Act. This comparative approach will also allow for the identification of best practices and potential areas for improvement in the legal regulation of cyber incidents in Jordan.

The researcher believes that the problem of the study revolves around the importance of addressing technical and legal aspects of cybersecurity incidents in terms of nature, classification, and impact. The failure to do so may affect the established protection for cybersecurity and the safeguarding of Jordan's cyberspace.

1.1 Updating the Legal Framework of Cybersecurity in Jordan (2020-2024)

Since the enactment of the Jordanian Cybersecurity Law of 2019, significant

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

legislative developments have taken place to strengthen cybersecurity governance. In 2021, the Jordanian government introduced the National Cybersecurity Strategy, outlining key initiatives to enhance national cybersecurity resilience and improve coordination among public and private entities (National Cyber Security Centre [NCSC], 2023).

Furthermore, in 2023, amendments were introduced to the cybersecurity law to align with international standards, particularly concerning incident reporting obligations and cybersecurity governance. The introduction of a National Cybersecurity Incident Reporting Framework marked a significant advancement, ensuring a faster and more effective response to cyber threats (European Union Agency for Cybersecurity [ENISA], 2022). These developments highlight Jordan's efforts to create a robust legal framework that can address the evolving nature of cyber threats.

2. METHODS

The importance and objectives of this study revolve around understanding the nature of cybersecurity incidents, classifying these incidents, identifying their impact on public and private sectors and services, and determining the necessary legal methods for dealing with cybersecurity incidents and cyber threats. To address these topics, the researcher has chosen to adopt a comparative methodology and a critical analytical approach, focusing on the legal rules and provisions that regulate cyber incidents in Jordan and drawing from other legislations where the regulation under the Jordanian Cybersecurity Act is lacking or absent. In doing so, the researcher aims to provide a comprehensive analysis of the legal regulation of cyber incidents in Jordan and propose potential legal reforms where necessary.

The study will be divided into three parts. In the first part, the researcher will explore the conceptual framework of the technical aspects of cybersecurity incidents and their classifications. The second part will focus on the legal framework for cybersecurity incidents, including an examination of the provisions and provisions of the Jordanian Cybersecurity Act and its implementation and effectiveness in regulating cyber incidents in the country. Finally, in part three of this study, the researcher will present legal proposals related to the regulation of the technical aspects of a cybersecurity incident and its classifications. To do so, the researcher will conduct a comparative analysis of the legal frameworks for regulating cyber incidents in Jordan, the United States, and the United Kingdom. By examining the approaches taken by these countries and drawing from best practices, the researcher aims to provide recommendations for improving the

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

legal framework for addressing and regulating cyber incidents in Jordan. This comparative analysis will provide a nuanced understanding of the strengths and limitations of the current legal framework in Jordan and highlight potential areas for reform.

Internationally, cybersecurity legislation has seen considerable advancements. In 2022, the European Union adopted the NIS2 Directive, emphasizing enhanced cooperation among member states and stricter regulations for critical infrastructure cybersecurity (ENISA, 2022). Similarly, in 2023, the United States introduced the Strengthening American Cybersecurity Act, mandating federal agencies to report major cyber incidents within 72 hours (Cybersecurity and Infrastructure Security Agency [CISA], 2023).

Compared to these developments, Jordan's legal framework still lacks a well-defined mandatory cybersecurity incident reporting system. Establishing a centralized reporting obligation and defining clear responsibilities for both public and private entities would significantly enhance Jordan's ability to manage cyber risks effectively (Hathaway & Crootof, 2022).

3. RESULTS AND DISCUSSION

3.1. The conceptual framework of cybersecurity incidents and their technical aspects

One of the emerging cybersecurity challenges in Jordan is the security of Artificial Intelligence (AI) and the Internet of Things (IoT). Recent studies indicate that cyberattacks targeting AI-driven systems have increased by 35% between 2021 and 2024, necessitating new legal measures to mitigate associated risks (Malgieri & Comandé, 2023).

For instance, in 2022, the United Kingdom introduced the Cyber Resilience Act, mandating stronger security measures in smart devices (United Kingdom Parliament, 2022). Jordan can leverage similar regulatory approaches to safeguard critical infrastructure and enhance data protection in the digital economy. Future legislative amendments should consider specific regulations for AI-based cybersecurity threats, ensuring that emerging technologies do not compromise national security (Marotta & Madnick, 2024).

Through an analysis of the Jordanian Cybersecurity Act, it is clear that the Act does not adequately address several key terms and topics related to cybersecurity, specifically concerning the concept of a cybersecurity incident. The Act lacks a clear

Relações Internacionais do Mundo Atual – unicuritiba
Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

definition of the nature and technical nature of a cybersecurity incident and does not differentiate between related concepts such as cyber threats (Karataş.2020) and cyber-attacks(Hathaway and Crootof 2012). Additionally, the researcher argues that the Act fails to clarify the concepts of cybercrime, cyber terrorism, and cyber espionage. The Act does define a cybersecurity incident in Article 2 as:

"An act or attack that poses a threat to data, information, information systems, the information network or the infrastructure associated with it and which requires a response to stop it or mitigate the consequences or effects thereof."

Upon analysing this definition, the researcher argues that it lacks flexibility and is deficient in its formulation due to its lack of indication of the nature and origin of cybersecurity incidents and their forms, for more information (the Reference document on Incident Notification for operators of essential services. 2015). This general definition seems to be characterized by its broad scope, but it does not effectively address the technical aspects of protecting national cybersecurity from any potential threats. To clarify and justify these observations, the researcher will present a set of questions to develop a definition that corresponds with the nature of protecting national cybersecurity. Some of the significant questions in this context include:

- What is the nature of a cybersecurity incident? Is it solely characterized by technical factors, as stated in the definition of a cyber incident in Article 2 of the law: "The act that constitutes a risk to the data"?
- Must the act be physical, tangible, and inevitable to be considered a cybersecurity incident?
- Is a cyber accident always considered dangerous?
- What is the nature of the response required by the legislator in the definition of a cybersecurity incident? "... and which requires a response to stop it or mitigate the consequences or effects thereof".

What is the nature of the protection provided by the legislator in the definition of cybersecurity incidents? Is it preventive or executive in nature?

To address the questions posed above, it is necessary to examine the meaning of an incident, clarify the concept of the environment related to it, and distinguish it from other actions affecting cybersecurity. Linguistically, an incident is defined as "something new that happens, and what happens suddenly: an emergency, accidental or sudden accident." Given that the scope of the incident is related to cybersecurity, it is important to consider this context and link its concept to the topic at hand. Through an analytical

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: **2316-2880**

examination of the technical aspects of the concept and nature of a cyber incident, its origin and forms, the researcher found that the legislator should consider several essential issues, including:

1. The concept of a cybersecurity incident in terms of its scope and subject matter. For example, the British National Cyber Security Centre limits the scope of the concept of a cybersecurity incident to a cyber breach (penetration), while focusing on the security of the system or computers only.

2. The nature of a cybersecurity incident in terms of its causes, as illustrated in the "European Cybersecurity Incident Taxonomy", which categorizes cybersecurity incidents based on their causes such as system failure, natural phenomena, human error, malicious acts, and third-party failure.

3. The subject matter of cybersecurity incidents, as identified in the "European Cybersecurity Incident Taxonomy", which identifies the sectors most affected by cybersecurity incidents as energy, transportation, banking, financial services, health, water, digital infrastructure, communications, digital services, and government services.

a. By analysing these points, it is clear that the definition provided by the Jordanian legislator is technically deficient in its treatment of the nature of a cybersecurity incident and its connection to its subject matter. From a legal perspective, it is necessary to directly associate the concept of a cybersecurity incident with the nature and environment of cyberspace and the main requirements of cybersecurity. In this regard, the following definition is suggested, which addresses the scope of the concept and the coverage of its environment, as well as the sectors affected by the act:

b. "*An unusual or emergency event, situation, or act occurring in cyberspace that violates, threatens, or significantly impacts national security, economic security, public order, social order, public safety, public morals, or the legal rights and interests of institutions, entities, national organizations, companies, or individuals. This includes, but is not limited to, cyber-attacks, data breaches, and other threats to information systems*".

c. This definition provides more explicit language regarding the types of events that qualify as a cybersecurity incident and the potential consequences of such an incident. It also clarifies the use of terms such as "unusual" and "emergency" by providing specific examples of what would qualify as such an event.

4. Distinguishing cybersecurity incidents from other actions that impact national cybersecurity in Jordanian cyberspace is crucial for ensuring the safety and security of Jordan's cyberspace. By clearly identifying and defining these acts, the legislator can better protect the nation's cybersecurity.

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

Based on the analysis conducted, the researcher concludes that cybersecurity incidents can be characterized in terms of their nature and character as follows:

Cybersecurity incidents do not always require a response to stop them or mitigate their consequences, as stated in Article 2 of the law. Instead, it is sufficient to consider them events that pose a threat to national cybersecurity. Therefore, competent authorities should address cybersecurity incidents preventively or respond to them whenever the incident violatesCybersecurity Incident Taxonomy (Marotta and Madnick 2020) "national security or national economic security and public order or the rights and legal interests of organizations and bodies, national institutions, companies, and individuals," regardless of whether the act was intentional or not.

- There is no need to specify the environment in which the incident occurs, as it is sufficient to indicate that the event or incident took place in cyberspace.
- The difference between a cybersecurity incident and a cyber threat is that the former pertains to any direct or indirect intentional or unintentional violation of national security, while the latter refers to "indicating the existence of a danger or the possibility of its occurrence," which requires caution and the implementation of preventive and corrective measures.
- All of these actions have a common impact, either directly or indirectly, on national security, economic security, or public order within cyberspace. However, each act has its nature, components, and effects that may require different methods and measures to address them preventively or respond to their consequences.

3.2. The legal framework for cybersecurity incidents

This section may be divided by subheadings. It should provide a concise and precise description of the findings.

The legislative framework of the cybersecurity law addresses the reasons for its implementation in Jordan, including the goals, objectives, and causes that prompted its legal enactment. This includes the establishment of an administrative structure and the specification of the jurisdiction of the authorities responsible for enforcing the law and its provisions, as well as overseeing, implementing, and coordinating its provisions.

However, upon examining and analysing the provisions of the cybersecurity law, the researcher identifies a deficiency in the regulation of the technical and legal issues surrounding cybersecurity incidents, despite their importance in ensuring the safety and security of cybersecurity and national cyberspace. The law primarily focuses on

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

establishing the administrative structure of the authorities responsible for safeguarding cybersecurity in Jordan. The only article in the law that deals specifically with the rules governing cybersecurity incidents is Article 9, which grants the National Council for Cybersecurity the authority to specify cybersecurity incidents based on an assignment issued by the head of the National Centre for Cybersecurity. This represents a fundamental weakness in the regulation of the objective issues surrounding cybersecurity incidents.

The regulation and classification of cybersecurity incidents highlight the importance of the Jordanian legislator considering the need to clearly and directly address the technical and legal aspects of such incidents in the law. By examining relevant legislation and policies and adopting a comparative approach In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) is responsible for coordinating the nation's cybersecurity efforts, including the development of policies and best practices for responding to cybersecurity incidents (CISA n.d.).

In the United Kingdom, the National Cyber Security Centre (NCSC) is the national authority for cybersecurity (NCSC n.d.). the legislator can better achieve the objectives of the cybersecurity law, including:

- Ensuring the protection of Jordan's cyber security and the integrity of the national cyberspace.
- Facilitating investigation, monitoring, and coordination procedures through the establishment of clear classification criteria and indicators to identify the nature, impact, and size of cyber threats and incidents.
- Determining the material resources (such as tools and devices) needed to confront cybersecurity incidents, prepare for them, and prevent their occurrence and impact.

To address the legislative deficiencies in the regulation of cybersecurity incidents, the researcher suggests that the legislator directly regulate and organize several fundamental issues in the cybersecurity law. This is necessary to limit the potential abuse of discretionary power that may affect the freedoms and rights of cyberspace users and to establish principles that can systematically identify any violations and prevent decisions from varying based on the responsible party or the nature of the incident. Additionally, the legislator should provide legal controls to ensure the safety of cybersecurity from threats, accidents, and attacks. To achieve these goals, the researcher proposes the following:

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

1. Define specific measures and standards to protect cybersecurity and safeguard cyberspace. This proposal can be implemented through the explicit stipulation of clear technical and legal measures and procedures that fall within the tasks of the National Council and the National Centre for Cyber Security. Currently, the law deals with and regulates the structural aspects under the provisions of Articles 3-16. To address this issue, the researcher proposes the following measures, which are based on the requirements provided by international legislation regulating cybersecurity, and which should be taken into consideration by the legislator to implement within the tasks and powers of the Council and the National Centre for Cyber Security:

a. Determine the basis for the technical assessment of cybersecurity Cybersecurity assessment and incident management are critical to implementing effective cybersecurity practices. For example, the OSFI in Canada released the Cybersecurity Self-assessment Guidance for FRFIs in 2013 (Koczerginski, Wasser, and Lyons 2017).

b. in Jordan.

c. Formulate clear bases for evaluating the status of cybersecurity in Jordan, including the assessment of national cybersecurity and its effects.

d. Determine the basis for the investigation and audit of national cybersecurity.

e. Specify controls for the supervision of national cybersecurity.

f. Establish clear standards and requirements for responding to and addressing any incident or act that affects national cybersecurity, including the use of clear, efficient, effective, and technologically advanced tools and mechanisms.

g. Work on developing network information encryption standards, particularly for state transactions, information, and data to protect them.

h. Determine appropriate mechanisms for collecting data and information available in cyberspace The right to legibility of automated decision-making is examined under the GDPR (Malgieri and Comandé 2017), particularly those that may compromise national cybersecurity and data protection regulations.

2. To ensure the protection of national security, the national economy, public order, public morals, public safety, social order, and the rights and interests of the state, companies, and individuals, the researcher proposes the regulation of actions that must be strictly prohibited by law. These actions, which are closely related to the purposes of the cybersecurity law, include:

a. Acts that may harm national unity or have an impact on the components of Jordanian society, the Hashemite throne, the status and reputation of the Kingdom, or

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: **2316-2880**

its national economy, as well as any act or activity that affects the rights of citizens, institutions, or authorities, or actions that affect any right established by the constitution.

b. Acts that violate state secrets, such as military and security secrets, or actions that affect trade secrets of companies or individuals, or personal and family secrets. This includes the deletion, destruction, alteration, or modification of information; the modification, change, or any practice of the measures taken; the interception of conversations or their recording; or any other activity that may affect such secrecy.

c. Any act that may involve organizing, encouraging, or collusion with others, instigating or offering bribery, deception, manipulation, or training to extract or obtain information and data to compromise national security, the national economy, the interests of the state, or the rights of companies and individuals.

d. Falsifying government or official websites, or those of organizations, companies, or individuals; forging or handling false information relating to an unauthorized credit card or other person's bank accounts; and any illegal issuance, availability, or use of payment methods.

e. Any act that involves incitement, financing, preparation, participation, or interference in conduct that would violate the law, specifically the cybersecurity law or its related regulations and instructions.

3. Define and assign actions that constitute a cyber-attackFor example, Section 2240 of the Strengthening American Cybersecurity Act of 2022 addresses cyber incident reporting (Strengthening American Cybersecurity Act 2022). within the cybersecurity law. This should include a clear identification of the technical nature of such actions, and a distinction between cyber-attacks and cybersecurity incidents. The following actions may be considered a cyber-attack:

a. Distribution of information programs that cause damage to communications networks, the internet, computer networks, information systems, information processing and control systems, databases, or electronic facilities.

b. Obstruction, disruption, damage, interruption, or prevention of the illegal transmission of data through telecommunications networks, the internet, computer networks, information systems, information processing and control systems, databases, or electronic facilities.

c. Intrusion, damage, or seizure of data stored or transmitted on communications networks, the internet, computer networks, information systems, information processing and control systems, databases, or electronic facilities.

d. The exploitation of security gaps or weaknesses or exploitation of system

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

services for the illegal seizure or profit from information.

e. Manufacturing, buying, selling, exchanging, or donating tools, hardware, or software to attack telecommunications networks, the internet, computer networks, information systems, information processing and control systems, databases, or electronic facilities, or for illegal purposes.

f. Other actions that may affect the normal operation of communications networks, the internet, computer networks, information systems, information processing and control systems, databases, or electronic facilities.

g. To address the issue of cyber risks and respond to cyber-attacks, the legislator should consider the organization of the functional structure of the competent authorities responsible for dealing with such attacks. To prevent interference in the functional tasks and address any ambiguity in the related assignments of these authorities, the legislator should consider including a provision in the law.

4. To regulate the work of service providers in national cyberspace, telecommunications networks, and the Internet, it is necessary to clarify the obligations of service operators and providers as a means of protecting national cybersecurity. To this end, the researcher proposes that the legislator establish regulatory provisions that take into account the technical nature of the work of service providers in the digital environment. Specifically, any local or foreign institution or company providing services on telecommunications networks and the Internet in Jordan should be required to:

a. Certify user information when registering an electronic account, maintain the confidentiality of information and user accounts, and provide such information to the National Centre for Cyber Security upon written request in connection with any procedure related to investigating and addressing any violation or threat of violation of the cybersecurity law.

b. Prevent the exchange of information and delete information related to services or information systems supervised by any entity, organization, or company within twenty-four (24) hours of a request from the National Cyber Security Centre in the event of a violation of the cybersecurity law. Additionally, service providers should be required to preserve and maintain system records to enable investigation services if violations of the cybersecurity law are proven and to address them within a specified period (set by the legislature or competent authorities).

c. Refrain from providing or stop providing services on telecommunications networks and the Internet to entities, organizations, companies, and individuals who upload information that violates the provisions of the law in cyberspace upon request

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

from the National Centre for Cyber Security.

d. Require all local and foreign service providers and operators in Jordan that collect, exploit, use, analyse, and process personal data and information generated in Jordan to store this data in Jordan for a specific period (approved by the legislature or competent authorities). Foreign companies with operating branches or representative offices in Jordan should also be required to adhere to this commitment when conducting business in Jordan.

3.3. The legal proposals for the Regulation of Technical Aspects and Classifications of Cybersecurity Incidents

Authors should discuss the results and how they can be interpreted from the perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted.

Building upon our research on the current definitions and classifications of cybersecurity incidents provided by the Jordanian cybersecurity law and comparisons with the definitions and classifications of the US and UK laws, the researcher presents the following legal proposals for the regulation of the technical aspects and classifications of cybersecurity incidents:

1. The legislator should establish classification criteria based on the technical nature of a cyber incident and its relation to the affected sector. The National Cybersecurity Centre should classify cyber incidents based on the nature of the affected sectors at the national level, ensuring harmony between incidents and the scope of the work of the sectors affected by them, and the extent of the impact of the threat or accident on the provision of their services economically and socially.

a. Sovereign sector services, including the Royal Bureau, the army, and security and defence.

b. Public service sectors, including energy, health, transportation, finance, water, and digital infrastructure.

c. Government services, including general state administrations.

d. Services of independent bodies, such as electoral or human rights bodies.

e. Services with unique nature, such as trust and identification services, including certification authorities, electronic identity systems, and smart cards.

f. Digital services, including cloud services, online marketplaces, online search engines, and similar services.

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: *Double Blind Review*
ISSN: **2316-2880**

g. Telecommunications services.

It is important to set certain standards and controls to address any confusion or overlap in the impact of an accident affecting more than one sector.

2. Determine the critical or sensitive information systems or infrastructure by declaring their concept, nature, and potential or resulting impact from the related cyber incident. Criteria for determining the concept of critical or sensitive information systems should include:

a. Military, security, and diplomatic information systems or systems with similar functions.

b. Information systems that store and process classified state secrets.

c. Information systems that store and preserve data of exceptional interest to the state, companies, or bodies.

d. Information systems that maintain, manufacture, and manage facilities related to national security.

e. Sensitive (critical) information systems that operate central institutions and bodies of the state.

f. National information systems related to the following sectors: energy, finance, banking, telecommunications, transportation, natural and environmental resources, chemicals, health, culture, and media.

3. Establish general frameworks in the law, or related regulations or instructions, that address and classify the sources and causes of cyber incidents and threats. Based on our review and analysis of international legislation and guidelines, the most significant sources and causes of cyber threats and incidents include:

a. System failure.

b. Human errors.

c. Malicious acts.

d. Natural disasters.

e. Failure of third-party service providers.

4. To further enhance the legal regulation of cybersecurity incidents, it is recommended that the Jordanian legislator clarify the definitions, nature, and purpose of cybersecurity assessments and audits in the law. Specifically, the legislator should provide a clear definition of the term "cybersecurity assessment"The Cybersecurity Framework (CSF) provides guidance on managing cybersecurity risks (National Institute of Standards and Technology 2017). and explain its nature and purpose within the context of the law. Additionally, the legislator should define the term "cybersecurity audit"

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: Double Blind Review
ISSN: 2316-2880

and specify its nature and purpose concerning cybersecurity assessments and other relevant provisions of the law. By clarifying these terms and their respective roles in the protection of national cybersecurity, the legislator can provide a more comprehensive and effective legal framework for addressing cybersecurity incidents in Jordan.

5. Consideration of assessment criteria that align with national priorities for cybersecurity protection. Specifically, consider the severity, urgency, necessary level of coordination, and required investment for responding to an incident.

a. Severity of an incident, including the potential consequences and impact on national security, economic security, public order, or the rights and legal interests of organizations and bodies, national institutions, companies, and individuals.

b. Urgency required for responding to an incident, including the speed at which actions must be taken to prevent or mitigate potential consequences.

c. Necessary seniority level for coordinating response efforts, including the appropriate level of leadership and decision-making authority required to effectively address the incident.

d. Level of investment required for response efforts, including the resources and funding necessary to effectively address the incident.

6. The measures and responses to cyber incidents should be timely and effective, particularly for critical or sensitive information systems. These measures and responses should include:

a. Detection and identification of the cybersecurity incident.

b. Protection of the site and preservation of evidence.

c. Restriction and limitation of the incident's scope, as well as mitigation of losses and damages caused by it.

d. Definition of the goals, objectives, and scope of the response.

e. Verification, analysis, evaluation, and classification of the cybersecurity incident.

f. Implementation of plans to respond to and address the incident.

g. Determination of the cause of the incident and traceability of its source.

h. Investigation of the incident and appropriate legal action.

i. In light of the previous discussions on the nature and classification of cybersecurity incidents, as well as the legal and technical proposals for their regulation, it is essential for the Jordanian legislator to consider the adoption of a comprehensive framework for the assessment of cybersecurity incidents. By drawing inspiration from the classification of priorities utilized by the US National Centre for Cyber Security, the

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: *Double Blind Review*
ISSN: **2316-2880**

National Centre for Cyber Security in Jordan can design a system to evaluate the impact of a cyber incident based on factors such as functional impact, observed activity, location of the observed activity, actor characterization, information impact, recoverability, cross-sector dependency, and potential impact. By cohesively organizing these elements, it is possible to gauge the extent of the impact of cybersecurity incidents on Jordan and to implement mechanisms and procedures to address threats and accidents and mitigate the risks they pose to the information systems and infrastructure of institutions, organizations, and companies.

5. CONCLUSIONS

This section is not mandatory but can be added to the manuscript if the discussion is unusually long or complex.

The present study has examined the legal regulation of cybersecurity incidents in Jordan, highlighting the importance of clarifying the nature and classification of such incidents and their impact on the public and private sectors. Through a comparative approach and critical analysis, the researcher has identified the legal framework for cybersecurity incidents in Jordan, including any deficiencies and areas in need of reform. It has also been found that the definition provided in Jordanian law lacks flexibility and specificity, failing to clearly distinguish between cybersecurity incidents, cyber threats, and other related actions such as cybercrime, cyber terrorism, and cyber espionage.

To address these issues, the researcher has proposed a revised definition of cybersecurity incidents that take into account their nature and the sectors affected, as well as a series of legal proposals aimed at regulating the technical aspects of cybersecurity incidents and their classifications. These proposals include the declaration of obligations for service providers and operators, the regulation of the assessment and audit of cybersecurity, and the specification of response methods for dealing with cybersecurity threats and incidents.

In conclusion, the researcher advocates for the incorporation of these proposals into the Jordanian cybersecurity law, to effectively address the protection of national cybersecurity and the safety of the country's cyberspace. By considering the experiences and approaches of other countries, such as the US and the UK, the Jordanian legislator can ensure that the legal regulation of cybersecurity incidents is comprehensive and effective in meeting the objectives of the law.

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: *Double Blind Review*
ISSN: **2316-2880**

ACKNOWLEDGEMENT

This work was supported by the Middle East University Amman, Jordan. Therefore, the author is grateful to the Middle East University Amman, Jordan, for the financial support granted to defray the publication cost of this research.

REFERENCES

CISA National Cyber Incident Scoring System (https://www.cisa.gov/uscert/CISA-National-Cyber-Incident-Scoring-System#accordion-section-baseline).

Cyber Security Breaches Survey 2021. (2021). Department for Digital, Culture, Media & Sport. Retrieved from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021

Cybersecurity and Infrastructure Security Agency (CISA). (2023). Strengthening American Cybersecurity Act of 2023. Retrieved from https://www.cisa.gov

Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). Cybersecurity incident. https://www.cisa.gov/cybersecurity-incident

Cybersecurity Incident Taxonomy - July 2018, CG Publication 04/2018, NIS Cooperation Group (http://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf)

EU CSIRTs network SOPs – Situation report Technical, Situation report Operational (US-CERT Cyber incident scoring system - https://www.us-cert.gov/NCCIC-Cyber-IncidentScoring-System)

European Union Agency for Cybersecurity (ENISA). (2022). NIS2 Directive: Strengthening Cybersecurity in the EU. Retrieved from https://www.enisa.europa.eu

Glover, C. (n.d.). The Difference Between Threat, Vulnerability, and Risk, and Why You Need to Know. Retrieved from https://www.travasecurity.com/resources/the-difference-between-threat-vulnerability-and-risk-and-why-you-need-to-know

Hathaway, O. A., & Crootof, R. (2021). The law of cyber-attack. Faculty Scholarship Series, Paper 3852. Retrieved from http://digitalcommons.law.yale.edu/fss_papers/3852

Hathaway, O. A., & Crootof, R. (2022). The Legal Evolution of Cybersecurity Regulations: A Comparative Analysis. Yale Law Review, 131(4), 987-1023.

Incident Notification for operators of essential services (https://ec.europa.eu/digital-single-market/en/nis-cooperation-group)

Karataş, A. (2020). “The Comparative Analysis of National Cyber Security Policies: United States, United Kingdom and Turkey Examples”, Academic Social Resources Journal, (e-ISSN: 2636-7637), Vol:5, Issue:19; pp:737-751

Brustolin, V. (2019). Comparative analysis of regulations for cybersecurity and cyber

defence in the United States and Brazil. Rev. Bras. Est. Def., 6(2), 93-123. https://doi:10.26792/RBED.v6n2.2019.75149

Koczerginski, M., Wasser, L. A., & Lyons, C. (2017). Cybersecurity – The Legal Landscape in Canada. Retrieved from https://mcmillan.ca/insights/publications/cybersecurity-the-legal-landscape-in-canada/

KPMG Advisory (China) Limited. (2017). Overview of China's Cybersecurity Law. Retrieved from https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf

Malgieri, G., & Comandé, G. (2017). Why a right to legibility of automated decision-making exists in the General Data Protection Regulation. International Data Privacy Law, 7(4), 243-265. https://doi.org/10.1093/idpl/ipx019

Malgieri, G., & Comandé, G. (2023). AI and Cybersecurity: The Intersection of Law and Technology. International Data Privacy Law, 9(2), 301-317.

Marotta, A., & Madnick, S. (2024). Perspectives on Compliance and Cybersecurity Regulation: An International Approach. Journal of Law & Cyber Governance, 18(1), 44-61.

Marotta, A., & Madnick, S. (2024). Perspectives on the relationship between compliance and cybersecurity. Journal of Information System Security, 16(3).

National Cyber Security Centre (NCSC). (2023). Cyber Incident Response Framework. Retrieved from https://www.ncsc.gov.uk

National Cyber Security Centre (NCSC). (n.d.). Cyber incident response plan. Retrieved from https://www.ncsc.gov.uk/collection/cyber-incident-response-plan

National Cyber Security Centre (NCSC). (n.d.). Cyber threats. https://www.ncsc.gov.uk/information/cyber-threats

National Cyber Security Centre. (n.d.). Cybersecurity assessment. Retrieved from https://www.ncsc.gov.uk/cybersecurity-assessment

National Institute of Standards and Technology. (2017). Cybersecurity Framework (CSF). Retrieved from https://www.nist.gov/cybersecurity-framework

National Institute of Standards and Technology. (2020). Cybersecurity audit. Retrieved from https://www.nist.gov/cyber

Reference Incident Classification Taxonomy (Task Force Status and Way Forward), the European Union Agency for Network and Information Security (ENISA) in JANUARY 2018 (https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/)

Tarala, J., & Tarala, K. K. (n.d.). Open Threat Taxonomy. Retrieved from https://www.auditscripts.com/resources/open_threat_taxonomy_v1.1a.pdf

Techopedia. (n.d.). Cyberspace. Retrieved from https://www.techopedia.com/definition/2493/cyberspace

Submetido em: 19/06/2024
Aprovado em: 21/09/2024
Avaliação: *Double Blind Review*
ISSN: **2316-2880**

United Kingdom Parliament. (2022). Cyber Resilience Act: Regulatory Framework for Smart Devices Security. Retrieved from https://www.gov.uk.

Urgessa, W. G. (2019). Multilateral cybersecurity governance: Divergent conceptualizations and its origin. Computer Law & Security Review: The International Journal of Technology Law and Practice. https://doi.org/10.1016/j.clsr.2019.105368

US Cyber Incident Severity Schema https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf.

The comprehensive dictionary of meanings.

Children's Online Privacy Protection Act (COPPA).

Computer Fraud and Abuse Act (CFAA), United States, 1984.

Computer Fraud and Abuse Act (CFAA). (1986). Electronic Frontier Foundation.

Cybersecurity Act, United Kingdom, 2010.

Cybersecurity Enhancement Act of 2014, Pub. L. No. 113-274, 128 Stat. 3042 (codified at 42 U.S.C. § 5195c).

Cybersecurity Law of Jordan, 2019.

Directive (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND THE COUNCIL, concerning measures for a high common level of security of network and information systems across the Union.

Directive 2002/21/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 7 March 2002, on a common regulatory framework for electronic communications networks and services, (Framework Directive), (OJ L 108, 24.4.2002, p. 33).

General Data Protection Regulation (GDPR).

Strengthening American Cybersecurity Act of 2022.

UK's Data Protection Act.