Cybersecurity Challenges in the Hashemite Kingdom of Jordan

Heba Al Muhaisen[1], Dr. Ali Aldabbas[2], Dr. Abeer Alqaisi[3], Sayel Almomani[4], Dr. Rehan Abu alzeit[3]

[1]Lecturer- University of Petra
[2]Associate professor -University of Petra
[3]Assistant Professor- University of Petra
[4]Professor- University of Petra
Corresponding Author: Heba Al Muhaisen, Email: Heba.almuhaisen@uop.edu.jo

KEYWORDS
Cybersecurity, digital revolution.

ABSTRACT

In an era marked by rapid advancements in technology and the digital revolution, cyber-security has become one of the most significant technical issues across countries, including nation-states like the Hashemite Kingdom of Jordan. This paper examines the very complex cyber security issues that Jordan experiences and evaluates how the legal structure established in Cyber Security Act No. 16 of 2019 can be used to face these challenges? Comparatively analyzed with global standards, the research identifies substantial shortcomings in Jordan's cybersecurity enforcement, coordination and integration capabilities. The research also discusses how international cooperation and public awareness can help improve national cybersecurity. The study appears to indicate that while significant steps have been taken Jordan's legal infrastructure, there is a need for continued modernization in line with a rapidly evolving cyber threat landscape. Finally, the paper ends by suggesting policy interventions that can bolster cybersecurity in Jordan, and it also draws attention to a number of issues regarding risk-based approaches for managing cyber threats regulation across different regulatory authorities; as well the necessity of more inclusive digital public engagement efforts. This is necessary to safeguard our vital structures in Jordan and provide a stable, secure cyberspace.

1. Introduction

There is no questioning the fact that the world around us continues to undergo substantive shifts, largely characterized by information now being everywhere and predominantly enabled through technology. These shifts have created new types of connectivity and activities. In the age of digital technology, dealing with information has become even more challenging because of the enormous amount of big data. Modern technology, then again, is very important to close the gap of development in all sectors of society, but information security needs to be a critical priority to adhere to online[Demirkan et al., 2020]. TINSIGHTThe influence of information and communication technology (ICT) is widespread and has manifold implications for the social, economic, political, and cultural spheres.

This has made cyber security a global issue as the most destructive among forms of cybercrime. This is manifested in the scope of threats and attacks on nation-state security. They create an important problem, as a crime that affects cybersecurity really is not national – it does not respect borders and geography — therefore necessitating international cooperation in order to solve. The landscape in cybersecurity is persistently changing; new technologies are coming up, and they inadvertently make way for novel types of cyber threats [Dash et al., 2022].

Given all that, one might ask — how serious is the global and domestic commitment to tackle cybersecurity challenges extensively in order to defeat increased cyber attacks vs. the Ability of de- devices to get hacked with a speed similar or greater than technological advancements? This comes back to stressing the severe and diverse nature of cyberthreats that can also affect public sector bodies — as well as private entities, which are fundamental for national security. However, with the evolution in technology and increased advancements comes much more sophisticated cybercriminals and attackers who are part of an illicit organization or group and are all working together for a particular mission objective.

In order to answer the research question successfully, a number of paramount aims can be applied. These range from exploring the characterization of cybersecurity incidents to studying in detail one area that is known for its low economic impact: cyberattacks on a country. In addition, a number of conditions need further investigation, such as the possible dangers deriving from cyber threats targeting the state political-military infrastructure and what are international and national tools aiming at securing cyberspace.

This paper reviews the research in two sections, both of which are related to global and national efforts for cybersecurity protection. Part 1 discusses key international agreements on ensuring the security of cyberspace across borders and initiatives, and declarations by different countries for countering cyber-attacks. It underscores, as well, the vital role international cooperation plays in ensuring a robust cybersecurity.

The research conducts an analysis within the field of national cybersecurity measures in com- mon, by shedding light on some (like cybercrime legislation No 16/2019 and Cybersecurity Council establishment, which has been vested with competencies). This research is significant by the need to protect the cyber sphere and, respectively, political institutions of state authority and defense sector, along with bank structures and medical establishments. If the state did not have these tools—or if it could not deploy them quickly enough—many basic services that Californians rely on every day would be put in jeopardy. It truly puts the need for industry-wide cooperation and cyber- threat hunting, not just within gaming but across even disparate institutions or sectors of society, into sharp focus. The paper also underlines the vital importance of sharing information between peers — across institutions within a specific sector, especially around their respective cybersecurity threat landscape.

Even though cyber-attacks are as common, scholarly work or study in the field of cybersecurity especially on global protection methods, is scarce. It remains necessary to research sustainable national and international cybersecurity policies as technology changes; the Internet continues to evolve.

2. Related Work

Previous research has predominantly focused on the legal framework governing Cybersecurity Services, particularly in relation to the Cyber Security Act No. 16 of 2019, as well as the broader understanding of cyberspace and its global ramifications [Hussein and Al-Hunaiti, 2021a]. These studies have provided valuable insights into the legislative measures that Jordan has implemented to secure its cyberspace, emphasizing the importance of legal structures in mitigating cyber threats. However, much of this work has been descriptive, outlining the provisions of the Act without critically assessing its effectiveness or the practical challenges associated with its implementation.

In contrast, current research expands upon and diverges from these earlier studies by exploring both global and domestic efforts to achieve cybersecurity while also highlighting various facets of cybersecurity. For instance, a study conducted at the Faculty of Political Sciences at Baghdad University examined the influence of cybersecurity on the proliferation of terrorism in Iraq post-2003. This research delved into the political, military, and social dimensions of cybersecurity, presenting a different perspective from prior studies in my area of research, which are more focused on international and national initiatives. While this study offers a comprehensive view of the interplay between cybersecurity and terrorism, its context-specific nature limits its applicability to other regions, including Jordan.

Additionally, a previous study by [Hussein and Al-Hunaiti, 2021b] explored the cybersecurity requirements for management information systems, investigating the causes of cyberattacks and identifying key areas of cybersecurity along with the necessary measures for effective protection. This research is valuable for understanding the technical and organizational challenges in im- implementing cybersecurity measures. However, it primarily focuses on the internal dynamics of management information systems and does not adequately address the broader legal and regulatory context, particularly the role of national legislation, like Jordan’s Cyber Security Act No. 16 of 2019, in shaping cybersecurity practices.

Moreover, while these studies contribute significantly to the understanding of cybersecurity, they often lack a comparative analysis with international standards. For example, research that examines cybersecurity within the context of Jordan frequently does so in isolation, without benchmarking Jordan’s practices against global best practices, such as those outlined by ISO/IEC 27001 or the NIST Cybersecurity Framework. This gap is crucial because it limits the ability to evaluate how well Jordan’s cybersecurity framework aligns with international norms and where improvements can be made to meet global standards.

Furthermore, the existing literature has not sufficiently addressed the dynamic nature of cyber- security threats and the need for continuous adaptation in legal and regulatory frameworks. While there is recognition of the rapid evolution of cyber threats, few studies have thoroughly examined how Jordan’s legal framework adapts—or fails to adapt—to these changes over time. This is a critical gap because the effectiveness of any cybersecurity strategy depends not only on its current adequacy but also on its ability to evolve with emerging threats.

Another notable gap in the current body of research is the limited focus on the practical implementation of cybersecurity laws and the challenges associated with enforcement. While the Cyber Security Act No. 16 of 2019 lays a solid foundation, the literature does not sufficiently explore how these laws are enforced across different sectors in Jordan, nor does it critically assess the coordination between various regulatory bodies responsible for cybersecurity. This gap is significant because enforcement is a key determinant of the success of any legal framework, and without proper implementation, even the most well-designed laws can fall short of their intended impact.

The gap is additionally present in international cooperation to improve national cybersecurity regimes. Some studies acknowledge the need for international collaboration, but they rarely discuss how to achieve it. The international character of cyber threats and the necessity for joint defence tactics make this significant for Jordan. This study addresses this gap by examining how Jordan may improve its cybersecurity through greater international cooperation and compliance with global cybersecurity treaties and conventions.

In conclusion, Jordan's legal and technical cybersecurity issues have been studied, but comparative analysis, adaptation to new threats, practical enforcement, and international cooperation are still lacking. A comprehensive analysis of Jordan's cybersecurity framework in comparison to international standards, legal structure adaptability, enforcement mechanisms, and international collaboration potential is the proposed work's focus. This approach expands on previous studies and provides a more holistic and actionable view of how Jordan may boost its cyber-security defenses in a more interconnected and threat-laden digital landscape.

3. Research Question

The primary research question guiding this study is: What are the key cybersecurity challenges faced by the Hashemite Kingdom of Jordan, and how can they be effectively addressed through national and international efforts? The research will assess Jordan's cybersecurity threats over the past decade, current cybersecurity policies and legislation, particularly the Cyber Security Act No. 16 of 2019, and the challenges of implementing and enforcing these measures across public and private sectors. Jordan's cybersecurity framework will be compared to international best practices to identify weaknesses and determine how international cooperation may strengthen it. How cybersecurity knowledge and comprehension affect national measures will also be studied.

4. National Efforts to Protect Cyber Security

Jordan has secured its digital infrastructure as cybersecurity becomes more essential. In September 2019, the Royal Decree ratified the Cyber Security Act No. 16 of 2019 and the National Cyber Security Centre endorsed it in January 2020 [Sarker et al., 2020]. Jordan took a huge step towards online security and cyber defense with this law.

The Cyber Security Act No. 16 of 2019 is a comprehensive legal framework that defines cy- be space as an environment encompassing the interaction of individuals, data, information systems, software, communication networks, and associated infrastructure. It also defines cybersecurity as the measures undertaken to protect these critical systems and networks from unauthorized access, misuse, and security breaches, while ensuring their continued operation and recovery from any disruptions [Qasaimeh and Jaradeh, 2022]. The Act protects Jordan from cybersecurity threats and fosters a safe, business-friendly environment for economic growth. Since information systems are advancing rapidly, electronic government services are becoming more vital, and cybersecurity events must be monitored and documented; this is crucial.

By establishing clear guidelines and policies derived from the national cybersecurity strategy, the Act aims to coordinate national efforts to improve the security of institutions and individuals. It also focuses on effectively managing cybersecurity incidents to minimize their impact and ensure the continued stability and security of Jordan’s digital infrastructure [Qasaimeh and Jaradeh, 2022]. The rising demand for cybersecurity professionals underscores the urgency of these initiatives, as the nation seeks to bolster its defenses against the evolving landscape of cyber threats.

Adoption of Preventive and Defensive Policies for Cyber Security

Many developed nations have proactively implemented comprehensive preventive and defensive measures to guard against cyberattacks. Countries such as the United States, Australia, and the United Kingdom have allocated substantial resources to address cybersecurity challenges, underscoring the critical importance they place on maintaining trust and stability in the digital realm. The persistent threat of cyber intrusions and attacks on global information networks poses significant risks to international relations, making cybersecurity a top priority for these nations. In response, there has been a growing emphasis on the creation of specialized units dedicated to tackling cybersecurity issues. For example, in 2011, then-Prime Minister Gordon Brown of the United Kingdom announced the establishment of a specialized unit within the Department of Defense to combat cybercrime [Youssef, 2011].

The National Cybersecurity Centre

The Cybersecurity Act No. 16 of 2019 established the Jordanian National Centre for Cybersecurity in early 2021. The Centre develops and implements a strong national cybersecurity system to protect the Kingdom from cyberattacks under the Prime Minister's direct supervision [Abu-Taieh et al., 2018]. The Centre has many essential functions and powers to achieve its goals under Article 6(b) of the Act:

1. Development of Strategies and Standards: The Centre is responsible for creating and enforc- ing cybersecurity strategies, policies, and standards, ensuring their proper implementation across both public and private sectors in Jordan. This includes developing plans and pro- grams that are then submitted for approval by the National Cybersecurity Council.

2. Operational Support and Coordination: The Centre plays a pivotal role in executing cyberse- curity operations and providing necessary support and consultation to strengthen operational security teams. It also coordinates response and intervention efforts, particularly in the event of cyber incidents affecting the nation's critical infrastructure.

3. Establishment of Cybersecurity Controls: The Centre is tasked with setting cybersecurity standards and controls, including the classification of cyber incidents. It grants authorization to cybersecurity service providers based on specific requirements, conditions, and fees as outlined in regulations established for this purpose.

4. Facilitation of Information Exchange: The Centre fosters cooperation with various organi- zations, both domestically and internationally, by facilitating the exchange of information and establishing agreements and memorandums of understanding with other cybersecurity bodies at national, regional, and international levels.

5. Capacity Building and Awareness Programs: Developing national expertise in cybersecurity is a critical function of the Centre. It designs and implements programs aimed at enhancing national capacity while also raising public awareness about cybersecurity threats and best practices.

6. Collaboration with Academic Institutions: The Centre actively collaborates with universities to promote scientific research in cybersecurity, thereby fostering innovation and advancing the field.

Article 6(a) of the Cybersecurity Act further outlines the Centre's overarching goal of building, developing, and organizing an effective national cybersecurity system to protect Jordan from cyber threats. This system aims to ensure the sustainability of critical infrastructure and the continued safety of the nation's citizens, property, and information [Al-Shawabkeh, 2019].

Article 8(b) of the Cybersecurity Act requires ministries, government departments, and public and private entities to follow Centre policies, standards, and controls. These entities must also disclose cybersecurity threats and provide the Centre with appropriate information to support its purpose [Al-Shawabkeh, 2019].

Article 13(a) of the Act authorises the President and Centre officials to serve as judges. They can investigate any area suspected of cybersecurity threats, administer related devices, instruments, and information systems, and execute sanctions against violators.

The Jordanian National Centre for Cybersecurity is well-known worldwide. Jordan ranks 18th globally and 2nd in Arab countries in cybersecurity, according to ITU data. Jordan has improved its cybersecurity, rising from 10th to 8th in the Arab world and 92nd to 74th globally.

These achievements are excellent, but the Centre needs continued funding and more work to reach its lofty goals. National security depends on cybersecurity's link to political, social, and economic stability. The internet's integration of financial and economic institutions emphasizes the need for strong cybersecurity to secure sensitive data, especially in security and military matters. To properly counteract social cyber-attacks, the National Centre for Cybersecurity leadership and personnel must be granted judicial powers. Trust in society can take time to rebuild.

Global Programs and Declarations for the Protection of Cybersecurity

International cybersecurity collaboration is also recognized. In 2007, the Global Cybersecurity Programme established a framework to improve information society trust and security. This program follows five pillars: legal, procedural, and technical measures; effective organizational structures; capacity building; and international cooperation. They guide worldwide cybersecurity initiatives.

The 2009 Erice Declaration on the Principles of Cyber Stabilization and Peace emphasizes communal efforts to promote global cyber-peace. The declaration aims to assess how information and communication technology (ICT) supports international stability, assess cyber threats, analyses cybercrime and conflicts, evaluate legal frameworks, and define cyber-peace [Borghard and Lonergan, 2018].

The National Council for Cybersecurity

In early 2021, Jordan established the National Council for Cybersecurity to protect its digital infrastructure. Under Article 3(a) of the Cyber Security Act No. 16 of 2019, the Council's main goal is to create a strong national cybersecurity system to defend the Kingdom against cyberattacks.

A Supreme Royal Government-appointed President leads the Council and includes representatives from the Ministry of Digital Economy and Leadership, the Jordanian Central Bank, the Jordanian Armed Forces, the General Intelligence Service, the Directorate of Public Security, and the National Centre for Security and Crisis Management. The Council of Ministers also picks three members, two of whom have private sector experience [Ababneh, 2020].

The responsibilities of the Council include adopting cybersecurity strategies, policies, and standards; approving the necessary plans and programs for the Centre to fulfill its duties, including initiatives for international and regional cooperation; reviewing quarterly reports on the cybersecurity situation in Jordan; and overseeing the Centre's annual budget as stipulated in Article 4 of the Cyber Security Act. The Council also establishes coordination committees to ensure the effective implementation of its objectives, determining their functions, duties, and decision-making processes.

5. Legal Framework and Regulatory Overview

The Cyber Security Act No. 16 of 2019 governs cybersecurity in Jordan, a major legislative effort to counter cyber threats. This Act governs and secures cyberspace in the country by outlining the obligations of the government, corporate sector, and individual stakeholders. The Act protects Jordan's government networks, financial systems, and important services from cyberattacks. The Cyber Security Act establishes defined parameters to develop a safe and resilient digital environment that promotes national security and economic stability [Ross et al., 2019].

Jordan has several cybersecurity laws and regulations in addition to the Cyber Security Act. The Penal Code criminalizes cyber offences such as unauthorized computer access, data breaches, and cyber fraud. The Telecommunications Law regulates Internet service providers (ISPs) and requires them to follow security standards. The Electronic Transactions Law can prevent e-commerce and online banking cybercrimes by establishing a legal framework for secure electronic communications and transactions [Ibrahim et al., 2024].

Despite these rules, Jordanian cybersecurity enforcement is difficult. Due to rapid technological advancement, the legal structure often cannot adapt to new dangers. This technology-law mismatch can be exploited by cybercriminals. To avoid confusion, regulatory agencies need to coordinate and clarify their roles. Even though cybersecurity awareness is promoted, private sector entities and the public still struggle to comply with the cybersecurity legal framework [Marune and Hartanto, 2021; Hossain et al., 2024; Kayode-Ajala, 2023].

Jordan's cybersecurity policy requires international cooperation. Because cyber risks traverse borders, Jordan has improved its legal and regulatory framework alongside international organizations and global cybersecurity projects. This requires aligning its cybersecurity laws with international best practices and engaging with other states. To address changing cyber threats, the legal framework must be reviewed and modified [McIntosh et al., 2024; Mullet et al., 2021].

Although Jordan has made headway in developing a cybersecurity legal framework, more can be done. To stay up with the fast-changing cyber world, these policies must be updated and enforced. Jordan's cyberspace needs regulatory coordination, public awareness, and international cooperation. Politics influence Jordan's cybersecurity policy. Cybersecurity policy execution is solid in Jordan, a constitutional monarchy with a centralized administration. The government's cybersecurity strategy prioritizes national security and stability. In a volatile zone, Cyber Security Act No. 16 of 2019 protects the country's digital infrastructure and political institutions, which are essential to its stability. Jordan's strategic connections with international allies, especially in regional security, impact its proactive cybersecurity position. These agreements improve Jordan's cyber defenses, notably against cross-border threats. However, the centralized nature of governance in Jordan also means that the success of cybersecurity initiatives heavily depends on political will and coordination at the highest levels of government. Therefore, continuous political commitment is essential to ensure that cybersecurity remains a national priority, particularly in the face of evolving threats that could impact the nation's political and economic stability.

6. Comparative Analysis with International Standards

Jordan's cybersecurity legal framework, particularly the Cyber Security Act No. 16 of 2019 [Al-Kasassbeh et al., 2023, Al-ma'aitah, 2022, Al-Flaieh,], represents a significant step forward in addressing the increasing threat of cyberattacks. However, when compared with international standards, there are areas where Jordan's approach can be further strengthened. International standards, such as those set by the International Organization for Standardization (ISO), particu- larly ISO/IEC 27001, provide a comprehensive model for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). While Jordan's legislation aligns with many of the principles outlined in these standards, there remains a gap in the adoption of comprehensive risk management frameworks that are integral to international standards [Kawar et al., 2022].

Enforcement and compliance monitoring distinguish Jordan's cybersecurity approach from worldwide best practices. In the EU, the General Data Protection Regulation (GDPR) sets strict standards for organizations, with severe consequences for noncompliance. Jordanian laws provide a strong cybersecurity foundation, but enforcement and consequences for non-compliance are less. This lax enforcement could hurt Jordan's cybersecurity efforts, especially in the business sector, where compliance is vital [Saqf Al Hait, 2023].

Furthermore, international standards stress constant improvement and adaptation to new threats. The US National Institute of Standards and Technology (NIST) Cybersecurity Framework is adaptable and adaptive, helping organizations adapt to changing threats. While thorough, Jordan's cyber-security regulations may benefit from similar flexibility to allow rapid adjustments to evolving threats. Cyber dangers are developing and becoming more sophisticated worldwide, making flexibility crucial [Dunn Cavelty and Wenger, 2020].

Another important aspect of international standards is the emphasis on cross-border collaboration and information sharing. The Budapest Convention on Cybercrime, for example, encourages international cooperation in the investigation and prosecution of cybercrimes. Jordan has made strides in this area by participating in regional cybersecurity initiatives and collaborating with international organizations. However, there is still room for improvement in terms of formalizing these collaborations and ensuring that Jordan's legal framework is fully aligned with international treaties and conventions on cybersecurity [Johnson, 2024].

In conclusion, Jordan has a solid cybersecurity law, but complying with international norms could improve it. Jordan should better defend its digital infrastructure by adopting comprehensive risk management frameworks, increasing enforcement measures, and being more flexible in responding to emerging threats. Jordan must also improve cross-border collaboration and comply with international cybersecurity accords to fight transnational cyber threats. In addition, Jordan's cybersecurity system could benefit from worldwide standards in incident response and recovery. According to ISO/IEC 27035, an international framework for information security incident management, a well-structured, quick reaction plan is needed to mitigate cyber incidents. Jordan's Cyber Security Act No. 16 of 2019 specifies stakeholders' roles in securing vital infrastructure, however it doesn't establish cybersecurity breach response procedures. Jordan might recover faster from cyberattacks and reduce long-term harm to national security and the economy by adopting more detailed incident response guidelines [Settembre-Blundo et al., 2021].

Regular cybersecurity audits and monitoring might also help Jordan learn from international standards. In order to ensure information security management system compliance, ISO/IEC 27001 needs regular internal audits. Audits are critical to uncover vulnerabilities, evaluate security measures, and make improvements. Jordan's cybersecurity architecture lacks strict inspection, potentially exposing security weaknesses to attackers. Jordan's cybersecurity legislation can better protect its systems from new attacks by requiring regular audits and monitoring [Alhajeri, 2022].

To fulfil international cybersecurity requirements, Jordan must improve technical and procedural aspects and train its workforce. Cyber threats evolve rapidly, requiring a staff proficient in the newest technology and worldwide cybersecurity best practices. ISO/IEC 27032, which describes cybersecurity training and awareness, emphasizes the need to create a security culture in organizations. All personnel, from IT experts to management, receive monthly cyber threat training. More systematic capacity building would assist Jordan in bridging the skills gap and ensure its cybersecurity personnel can adopt and maintain international standards [Uchendu et al., 2021].

Finally, Jordan’s approach to data protection and privacy also merits closer alignment with international norms. While the Cyber Security Act No. 16 of 2019 provides a foundation for safeguarding personal and organizational data, it lacks the comprehensive data protection measures found in regulation.

7. Challenges and Policy Recommendations

The implementation and enforcement of cybersecurity regulations in Jordan face numerous major challenges that hamper the country's cybersecurity framework. One of the biggest concerns is that technology advances faster than the legal system can react to new dangers. Cybercriminals might abuse obsolete laws as cyber dangers grow. The lack of a comprehensive risk management framework to assist legal adaptation to emerging dangers exacerbates the gap between technology and law [Settembre-Blundo et al., 2021].

Jordan's cybersecurity regulatory bodies lack coordination. Multiple agencies' overlapping duties can cause inefficiencies, misunderstanding, and enforcement gaps. The Cybersecurity Council, law enforcement agencies, and regulatory authorities like the Telecommunications Regulatory Commission may not clearly define their tasks, which can divide cybersecurity efforts. Fragmentation and limited resources and experience make cybersecurity law enforcement harder [Alhajeri, 2022].

Additionally, Jordanian public awareness and cybersecurity compliance remain issues. Even though cybersecurity awareness is promoted, many private sector organizations are still not fully compliant with cybersecurity standards and best practices. This non-compliance raises the risk of cyber incidents since organizations may not have enough protection to protect sensitive data and key infrastructure. Many personnel lack the training to recognize and respond to cyber risks due to the lack of a cybersecurity culture [Uchendu et al., 2021].

Many policies address these issues. Adapt cybersecurity policies to technology first. This can be done via a cyber-threat committee that recommends law amendments. Jordan could detect and mitigate hazards with ISO/IEC 27001 risk management.

Second, Cybersecurity enforcement requires regulatory cooperation. A central cybersecurity organization can oversee all cybersecurity regulations, ensuring clear commands and effective resource allocation. The authority may also strengthen international collaboration and ensure Jordan's cybersecurity system satisfies global standards.

Third, increasing public awareness and promoting a culture of cybersecurity is crucial. This can be achieved through targeted awareness campaigns, training programs, and incentives for organizations that demonstrate compliance with cybersecurity standards. By fostering a culture of cybersecurity, Jordan can enhance the overall resilience of its digital infrastructure against cyber threats.

In conclusion, Jordan has made tremendous progress in developing a cybersecurity legal framework, but technology advancement, regulatory cooperation, and public awareness must be addressed to improve these laws. These policy proposals can help Jordan establish a stronger cybersecurity environment that can handle complex and growing cyber threats.

8. Conclusion

The Hashemite Kingdom of Jordan has made noteworthy progress in creating a legislative and regulatory framework to handle cybersecurity issues. Enacting the Cyber Security Act No. 16 of 2019 is important to protecting the nation's digital infrastructure. This report shows numerous major areas where adjustments are needed to combat evolving cyber threats. Jordan's legal framework meets many international norms. However, enforcement, coordination, and adaptation are issues.

The comparison to ISO/IEC 27001 and the NIST Cybersecurity Framework shows the need for a more comprehensive and flexible cybersecurity risk management strategy. Jordan's cybersecurity legislation must be updated as technology advances to stay effective. Enhancing regulatory coordination and international cooperation is also necessary to reduce transnational cyber threats.

Building a strong cybersecurity culture in Jordan requires public knowledge and compliance with cybersecurity rules. The report suggests focused awareness efforts, enhanced training, and incentives for organizations to follow cybersecurity standards to improve national cybersecurity.

In conclusion, while Jordan's legal framework has laid a solid foundation for cybersecurity, there is an urgent need for ongoing reforms and proactive measures to address the challenges identified in this study. By implementing these recommendations, Jordan can enhance its resilience against cyber threats and ensure the protection of its critical infrastructure, thereby contributing to the security and stability of the nation in the digital age.

Reference

[1] [Ababneh, 2020] Ababneh, M. A. (2020). Computer Crime and Its International Dimensions. Culture House.

[2] [Abu-Taieh et al., 2018] Abu-Taieh, E., Alfaries, A., Al-Otaibi, S., and Aldehim, G. (2018). Cyber security crime and punishment: Comparative study of the laws of jordan, kuwait, qatar, oman, and saudi arabia. International Journal of Cyber Warfare and Terrorism (IJCWT), 8(3):46–59.

[3] [Al-Flaieh,] Al-Flaieh, M. T. I. Cybercrime in jordanian law.

[4] [Al-Kasassbeh et al., 2023] Al-Kasassbeh, F. Y., Ghazleh, A. M. A., Ma'moon juma'h, M. K., et al. (2023). International and national efforts to protect cyber security: Jordan case study. International Journal of Cyber Criminology, 17(2):350–363.

[5] [Al-ma'aitah, 2022] Al-ma'aitah, M. A. (2022). Investigating the drivers of cybersecurity enhance- ment in public organizations: The case of jordan. The Electronic Journal of Information Systems in Developing Countries, 88(5):e12223.

[6] [Al-Shawabkeh, 2019] Al-Shawabkeh, M. A. A. (2019). Computer and Internet Crimes/Information Crime. Dar Al-Ilm and Al-Thafa for Publishing and Distribution.

[7] [Alhajeri, 2022] Alhajeri, M. (2022). Developing a digital competence framework for UAE law enforcement agencies to enhance cyber security of Critical Physical Infrastructure (CPI). Uni- versity of Salford (United Kingdom).

[8] [Borghard and Lonergan, 2018] Borghard, E. D. and Lonergan, S. W. (2018). Confidence building measures for the cyber domain. Strategic Studies Quarterly, 12(3):10–49.

[9] [Dash et al., 2022] Dash, B., Ansari, M. F., Sharma, P., and Ali, A. (2022). Threats and oppor- tunities with ai-based cyber security intrusion detection: a review. International Journal of Software Engineering & Applications (IJSEA), 13(5).

[10] [Demirkan et al., 2020] Demirkan, S., Demirkan, I., and McKee, A. (2020). Blockchain technology in the future of business cyber security and accounting. Journal of Management Analytics, 7(2):189–208.

[11] [Dunn Cavelty and Wenger, 2020] Dunn Cavelty, M. and Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. Contemporary Security Policy, 41(1):5–32.

[12] [Hossain et al., 2024] Hossain, S. T., Yigitcanlar, T., Nguyen, K., and Xu, Y. (2024). Local govern- ment cybersecurity landscape: A systematic review and conceptual framework. Applied Sciences, 14(13):5501.

[13] [Hussein and Al-Hunaiti, 2021a] Hussein, H. J. A. and Al-Hunaiti, M. A. R. (2021a). Cyber se- curity services legal framework, comparative study. Master's thesis, Middle East University. Master's Thesis.

[14] [Hussein and Al-Hunaiti, 2021b] Hussein, H. J. A. and Al-Hunaiti, M. A. R. (2021b). Cyber se- curity services legal framework, comparative study. Master's thesis, Middle East University. Master's Thesis.

[15] [Ibrahim et al., 2024] Ibrahim, D. M., Hidayat, Y., and Wasitaatmadja, F. F. (2024). Legal pro- tection of banking customers who are victims of information and electronic transaction crimes. Jurnal Ilmiah Penegakan Hukum, 11(1):102–120.

[16] [Johnson, 2024] Johnson, D. (2024). Leadership Fundamentals for Cybersecurity in Public Policy and Administration: Lessons for the Global South. Taylor & Francis.

[17] [Kawar et al., 2022] Kawar, M., Nimeh, Z., and Kool, T. A. (2022). From protection to transfor- mation: Understanding the landscape of formal social protection in jordan. Economic Research Forum (ERF).

[18] [Kayode-Ajala, 2023] Kayode-Ajala, O. (2023). Establishing cyber resilience in developing coun- tries: an exploratory investigation into institutional, legal, financial, and social challenges. In- ternational Journal of Sustainable Infrastructure

for Cities and Societies, 8(9):1–10.

[19] [Marune and Hartanto, 2021] Marune, A. E. M. S. and Hartanto, B. (2021). Strengthening per- sonal data protection, cyber security, and improving public awareness in indonesia: Progres- sive legal perspective. International Journal of Business, Economics, and Social Development, 2(4):143–152.

[20] [McIntosh et al., 2024] McIntosh, T. R., Susnjak, T., Liu, T., Watters, P., Xu, D., Liu, D., Nowrozy, R., and Halgamuge, M. N. (2024). From cobit to iso 42001: Evaluating cyberse- curity frameworks for opportunities, risks, and regulatory compliance in commercializing large language models. Computers & Security, 144:103964.

[21] [Mullet et al., 2021] Mullet, V., Sondi, P., and Ramat, E. (2021). A review of cybersecurity guide- lines for manufacturing factories in industry 4.0. IEEE Access, 9:23235–23263.

[22] [Qasaimeh and Jaradeh, 2022] Qasaimeh, G. M. and Jaradeh, H. E. (2022). The impact of arti- ficial intelligence on the effective applying of cyber governance in jordanian commercial banks. International Journal of Technology, Innovation and Management (IJTIM), 2(1):68–86.

[23] [Ross et al., 2019] Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., and McQuaid, R. (2019). Developing cyber resilient systems: a systems security engineering approach. Technical report, National Institute of Standards and Technology.

[24] [Saqf Al Hait, 2023] Saqf Al Hait, A. (2023). Cyber hacking: building a harmonised criminal legal framework for addressing cyber hacking in the Arab convention on combating information technology oflences: a comparative study between Jordanian & Saudi cyber laws. PhD thesis, Anglia Ruskin Research Online (ARRO).

[25] [Sarker et al., 2020] Sarker, I. H., Kayes, A. S. M., Badsha, S., Alqahtani, H., Watters, P., and Ng,

[26] A. (2020). Cybersecurity data science: an overview from machine learning perspective. Journal of Big Data, 7(1):41.

[27] [Settembre-Blundo et al., 2021] Settembre-Blundo, D., González-Sánchez, R., Medina-Salgado, S., and García-Muiña, F. E. (2021). Flexibility and resilience in corporate decision making: a new sustainability-based risk management system in uncertain times. Global Journal of Flexible Systems Management, 22(Suppl 2):107–132.

[28] [Uchendu et al., 2021] Uchendu, B., Nurse, J. R., Bada, M., and Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. Computers & Security, 109:102387.

[29] [Youssef, 2011] Youssef, A. F. (2011). Cyber And Information Crime And International and Local Eflorts To Combat Computer And Internet Crimes. Al-Wafa Legal Library.