ENCUENTROS | Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico pp: 392-420

THE IMPACT OF CYBERSECURITY LAW IN THE MIDDLE EAST

El impacto de la legislación sobre ciberseguridad en Oriente Medio

Srbaz Nidham Othman
College of Law and Political Sciences, University of Kirkuk. Kirkuk, Iraq.
Srbaz.law@uokirkuk.edu.iq
https://orcid.org/0009-0004-2228-4072

Raed Hameed
Al-Turath University College. Baghdad, Iraq.
raed.hamid@turath.edu.iq
https://orcid.org/0000-0002-5008-4893

Aqeel Mahmood Jawad
Al-Rafidain University College, Baghdad, Iraq.
aqeel.jawad@ruc.edu.iq
https://orcid.org/0000-0003-1671-7607

Raad Tomaa Kawad
Al-Mamoon University College. Baghdad, Iraq.
raad.t.awad@almamonuc.edu.iq
https://orcid.org/0000-0002-4530-5751

Dmytro Khlaponin
Kyiv National University of Construction and Architecture. Kyiv, Ukraine.
khlaponin_dy@knuba.edu.ua
https://orcid.org/0000-0002-7797-4319

Este trabajo está depositado en Zenodo:
DOI: https://doi.org/10.5281/zenodo.14291287

ABSTRACT

Due to the growing digitalization in the Middle East, there has been a significant increase in cyberattacks in the region. The escalating magnitude of cyber assaults underscores the urgent need for robust cybersecurity measures and regulatory frameworks to safeguard digital assets and infrastructures. The articles aim to assess the repercussions of cybersecurity legislation in the Middle East, with a focus on the challenges and accomplishments of the region in establishing effective cybersecurity defenses. A comprehensive analysis of scholarly articles, media reports, and government records was conducted to gather comprehensive data on the existing cybersecurity rules in the Middle East. This method facilitated a thorough analysis of the legal and regulatory structure in the given domain. Analysis reveals that while certain Middle Eastern countries have made significant progress in establishing comprehensive cybersecurity frameworks, there are still significant areas for improvement that hinder the practical application of these frameworks. A significant revelation is the need for cohesive efforts and cooperation among governments, business sector entities, and international agencies, which is vital for enhancing cybersecurity.

Keywords: Middle East, cybersecurity, legislation, regulatory frameworks.

RESUMEN

Debido a la creciente digitalización en Oriente Medio, se ha producido un aumento significativo de los ciberataques en la región. La creciente magnitud de los ciberataques subraya la urgente necesidad de contar con medidas de ciberseguridad sólidas y marcos regulatorios para salvaguardar los activos e infraestructuras digitales. Los artículos tienen como objetivo evaluar las repercusiones de la legislación sobre ciberseguridad en Oriente Medio, centrándose en los desafíos y logros de la región en el establecimiento de defensas de ciberseguridad eficaces. Se realizó un análisis exhaustivo de artículos académicos, informes de los medios de comunicación y registros gubernamentales para recopilar datos completos sobre las normas de ciberseguridad existentes en Oriente Medio. Este método facilitó un análisis exhaustivo de la estructura legal y regulatoria en el dominio en cuestión. El análisis revela que, si bien algunos países de Oriente Medio han logrado avances significativos en el establecimiento de marcos integrales de ciberseguridad, aún existen áreas importantes de mejora que obstaculizan la aplicación práctica de estos marcos. Una revelación importante es la necesidad de esfuerzos cohesivos y cooperación entre los gobiernos, las entidades del sector empresarial y las agencias internacionales, lo cual es vital para mejorar la ciberseguridad.

Palabras claves: Oriente Medio, ciberseguridad, legislación, marcos regulatorios.

RECIBIDO: 17/04/2024 ACEPTADO: 14/09/2024

INTRODUCTION

The fast adoption of digital technologies in the Middle East has led to profound changes in people's daily routines and social interactions. The region's progress and economic growth have been boosted by the widespread use of digital technologies, including cloud computing, IoT devices, and artificial intelligence. The Middle East's essential infrastructure, national security, and general stability are all in danger due to the proliferation of cyber threats made possible by the region's rapid digitalization. Thus, mitigating these threats and fortifying the region's cyber defenses is more critical than ever.

The worrisome rise in cyberattacks aimed against the Middle East highlights the critical nature of tackling cybersecurity vulnerabilities in the area. Another Raytheon Intelligence & Space analysis found that between 2016 and 2020, cyber threats in the Middle East increased by 800%. [1]

Because of its critical geographic position and increasing dependence on digital technology, cybersecurity in the Middle East is of paramount concern. Because of its proximity to some of the world's most significant oil and gas reserves, the region's essential infrastructure has been a frequent target of cyber-attacks [2]. Moreover, recent high-profile cyber-attacks, such as the Stuxnet virus that attacked Iran's nuclear program [3] and the global ransomware assault on Saudi Aramco [4], have highlighted the necessity for a comprehensive and coordinated response to the rising cyber threat scenario.

Significant progress has been made in cybersecurity worldwide, with many studies concentrating on creating and implementing cybersecurity laws and regulations. While research on the Middle East's cybersecurity landscape has been conducted, there has yet to be an in-depth examination of the effect of cybersecurity law in the area. A deficiency inspired this research in the existing literature. It intends to fill that void by providing a comprehensive analysis of cybersecurity law in the Middle East, including its triumphs and failures and suggestions for strengthening cybersecurity in the area [5], [6], [7], [8].

The recent rise in cyber-attacks has led to massive financial losses, harm to reputations, and interruptions in lifeline services. Cybercrime has a significant monetary effect in the Middle East, with the United Arab Emirates losing an estimated $1.63 billion to cyber assaults in 2020 [9]

The Middle East is anticipated to become more susceptible to cyberattacks in the coming years as the area continues its fast digital transformation and adoption of new technology. The World Economic Forum's 2020 report identified cyber-attacks as the region's second-greatest risk, highlighting the critical need for strong cybersecurity measures and regulatory frameworks to counteract this emerging danger [10].

The significance of this article resides in its ability to improve our knowledge of cybersecurity legislation in the Middle East and to encourage cooperation among relevant parties to solve this urgent problem. Policymakers, business executives, and cyber security academics will find this helpful report, especially in the Middle Eastern environment.

The existing body of research on cybersecurity legislation has identified several significant obstacles. These include a need for more harmonization between national legal frameworks [11], a lack of resources and expertise, and a lack of public awareness and education about cybersecurity [12]. The complex geopolitical situation and ever-evolving nature of cyber threats in the Middle East only worsen matters. However, there are examples of success and best prac-

tices in the region, like the fact that the United Arab Emirates (UAE) has good cybersecurity laws and that the public and private sectors in Saudi Arabia are working together to improve cybersecurity [13], [14]

The study's main objectives are to: The aims of the present article are as follows: (1) to analyze the current state of cybersecurity legislation in the Middle East by comparing the legal frameworks in place across different countries and identifying gaps and inconsistencies that may hinder effective implementation; (2) to examine the challenges faced by the region in implementing and enforcing cybersecurity laws; and (3) to investigate the successes and best practices in the Middle East by highlighting examples of effective cybersecurity legislation and collaboration.

The study's main findings stress the need for a standardized, risk-based strategy for cybersecurity legislation across the Middle East. The research shows how important it is for governments, businesses, and international groups to work together more closely on cybersecurity. It also stresses the need for international cooperation, legislative harmonization, and cybersecurity education and awareness investments. The report concludes by calling for the ongoing revision of legal frameworks to account for the changing nature of cyber threats.

Due to the region's growing vulnerability to cyber-attacks due to its fast digital transition, a strong and coordinated response is required to protect the Middle East's vital infrastructure, economy, and national security. This research intends to add to the current conversation on cybersecurity law in the Middle East by analyzing existing laws, pointing out their strengths and weaknesses, and suggesting ways to improve cybersecurity.

The study's overarching goals are to inform politicians, business leaders, and others in the Middle East about improving cybersecurity and the significance of robust legal frameworks in combating cyber threats. The Middle East can provide a solid groundwork for a safe digital future by tackling the particular difficulties faced by the area and learning from its triumphs. Ultimately, our research will help create a safer and more secure digital environment in the area, protecting its vital infrastructure, economy, and national security from the ever-changing cyber threat scenario.

The Study Objective

This article aims to analyze cybersecurity laws' impact on the Middle East comprehensively. The paper will look at the present status of legislation, identify issues and accomplishments, and provide recommendations for changes to help them keep up with the evolving cyber threat scenario. By conducting this investigation, the article aims to increase awareness about the significance of solid cybersecurity laws in the geographical area and encourage cooperation between government agencies, the private industry, and international organizations to improve regional cybersecurity resilience.

Problem Statement

There has been an increase in cyber threats due to the Middle East's fast digital transition, which poses severe hazards to the region's vital infrastructure, economy, and national security. Although cybersecurity is becoming more crucial, more is needed to know about the efficiency of current legislative frameworks in tackling the particular difficulties faced by countries in the area. This article aims to solve this by providing a critical analysis of the impact of cybersecurity law in the Middle East, pointing out the gaps and inconsistencies in existing legislation, and suggesting ways to strengthen cybersecurity in the region by creating and enforcing strong, harmonized legal frameworks.

BACKGROUND: CURRENT STATE OF CYBERSECURITY LEGISLATION IN THE MIDDLE EAST

Many Middle Eastern nations have different methods and objectives for managing cyber threats, which is reflected in the present status of cybersecurity laws in the region. To better understand the difficulties and possibilities in bolstering regional cybersecurity resilience in the face of fast digital change, it is vital to study the current laws and regulations to find similar aspects, discrepancies, and gaps.

Supply chains are becoming more interdependent and complex due to technological advancements. The security vulnerabilities of one organization might endanger others. Nowadays, supply chain vulnerabilities account for up to 40% of all cyberattacks. Executives in charge of cyber security report feeling exhausted and "always on" due to the increasing number of digital connections at work.

Tiredness is a target for cybercriminals. According to the study, 23% of security executives monitor their partners and suppliers for signs of cybersecurity issues in real time. Just the most immediate suppliers and vendors may be covered by certain businesses. Customers, partners, shareholders, and anyone involved in their firm are not welcome.

More focus on the risks posed by third parties. Sixty percent of businesses by 2025 will consider cyber security risk to assess deals with outside parties. C-suite executives are concerned about supply chain vulnerabilities, according to recent statistics. Sixty percent of the 900 businesses surveyed cited supply chain threats as their top cyber security concern. Cyber espionage (59%) and advanced persistent threats (57%), but not DDoS attacks (66%). Atlassian maps out the dangers in the supply chain. Atlassian is utilized by 83% of Fortune 500 companies and has 180,000 customers in over 190 countries. In June of 2022, hackers uncovered a critical flaw in Atlassian Confluence. Most giant worldwide corporations may be unable to function correctly if they cannot use Atlassian products. More than two hundred thousand firms rely on services provided by shaky establishments.

The necessity of cybersecurity has been increasingly recognized in recent years, with several Middle Eastern nations passing legislation to combat cybercrime and safeguard their most vital information networks [15], [16]. Cybercrime prevention and punishment are common goals of national cybersecurity legislation, as is the creation of regulatory bodies with oversight responsibilities.

United Arab Emirates (UAE) has been at the forefront of implementing comprehensive cybersecurity regulations, including Cyber Crimes Law No. 5 of 2012, which covers various cybercrimes, such as hacking, data breaches, and online harassment [17]. The United Arab Emirates (UAE) has also set up the National Electronic Security Authority (NESA), which is in charge of establishing and implementing national cybersecurity regulations [18]

The United Arab Emirates has taken the initiative to draft strong cybersecurity laws. Unauthorized access, data breaches, and cyber espionage are just some of the many forms of cybercrime addressed by the country's Federal Law No. 5 of 2012 on Combating Cybercrimes [19]. In 2017, the UAE also formed the National Electronic Security Authority (NESA), responsible for executing the UAE Information Assurance Standards and monitoring the country's cybersecurity policy [20].

The Essential Cybersecurity Controls (ECC) framework established minimum standards for protecting critical infrastructure. It was developed

under the watchful eye of the National Cybersecurity Authority (NCA), created in Saudi Arabia in 2017 [21]. Saudi Arabia's Anti-Cyber Crime Law, passed in 2007, makes several online transgressions punishable by law [22]

Qatar's cybersecurity law, Law No. 14 of 2014, addresses several types of cybercrime, such as hacking, data theft, and cyber espionage [23]. In addition, in 2014, Qatar unveiled its National Cyber Security Strategy (QNCSS) to direct the country's initiatives in strengthening its cyber defenses [24]

The Middle East has made great strides in drafting cybersecurity laws to counteract the expanding cyber threat scenario. Every nation has enacted legal frameworks and set up regulatory entities to supervise cybersecurity initiatives and fight cybercrimes. Increased regional cybersecurity resilience requires nonstop action to integrate these legislative frameworks and ensure effective enforcement mechanisms are in place.

Middle Eastern nations have made outstanding achievements in drafting cybersecurity laws to handle the rising cyber threat scenario as the digital revolution continues to affect the area. The similarities and contrasts between Middle Eastern nations' cybersecurity laws and regulations, as well as regional trends and patterns, loopholes, and inconsistencies, are all made clear by this comparison.

Cybercrimes such as hacking, data breaches, and online fraud are increasingly treated as crimes throughout Middle Eastern nations. In addition to establishing a legal framework for international cooperation in investigating and prosecuting cybercrime, these measures are intended to prevent and convict cybercriminals (Alsaleh & Alomar, 2019).

The development of regulatory agencies to monitor cybersecurity initiatives is another similarity between the nations. These organizations are responsible for formulating and enforcing national cybersecurity plans and assuring conformity with applicable norms and regulations [25].

The similarities and contrasts, regional trends and patterns, and discrepancies in Middle Eastern cybersecurity law are all laid bare through a side-by-side comparison. Harmonizing regulatory frameworks, funding capacity development, and fostering public-private partnerships and international collaboration are crucial as the area embraces digital change.

As cybersecurity becomes a crucial concern for countries in the Middle East, it is essential to examine and compare the legislation adopted by different countries in the region. Understanding the common elements, differences, and gaps in existing legal frameworks can help identify areas for improvement and inform future legislative efforts. In this section, we provide a comparison of the cybersecurity laws and regulations of various Middle Eastern countries (Table 1).

Table 1. Comparison of Cybersecurity Legislation Elements and Approaches in Middle Eastern Countries

Country	Criminalization of Cybercrimes	Regulatory Bodies	International Cooperation	Public-Private Partnerships	Emerging Technologies	Enforcement Mechanisms
United Arab Emirates (UAE)	Yes	NESA	Yes	Yes	Yes	Yes
Saudi Arabia	Yes	NCA	Yes	Yes	Yes	Yes

Qatar	Yes	MTC	Yes	Yes	Yes	Yes
Israel	Yes	NCSA	Yes	Yes	Yes	Yes
Iran	Yes	NCC	Limited	Limited	Limited	Limited
Bahrain	Yes	SIA	Yes	Yes	Yes	Yes
Kuwait	Yes	CITRA	Yes	Yes	Yes	Yes
Oman	Yes	ITA	Yes	Yes	Yes	Yes
Lebanon	Yes	OGERO	Yes	Yes	Limited	Limited
Jordan	Yes	NITC	Yes	Yes	Yes	Yes
Egypt	Yes	NTRA	Yes	Yes	Yes	Yes
Iraq	Limited	CMC	Limited	Limited	Limited	Limited
Syria	Limited	N/A	Limited	Limited	Limited	Limited
Yemen	Limited	N/A	Limited	Limited	Limited	Limited

Note: NESA = National Electronic Security Authority, NCA = National Cybersecurity Authority, MTC = Ministry of Transport and Communications, NCSA = National Cyber Security Authority, NCC = National Center for Cyberspace, SIA = Supreme Council for the Information and Communication Technology, CITRA = Communication and Information Technology Regulatory Authority, ITA = Information Technology Authority, OGERO = Organisme de Gestion et d'Exploitation de l'ex Radio Orient, NITC = National Information Technology Center, NTRA = National Telecom Regulatory Authority, CMC = Communications and Media Commission. N/A = Not Applicable or information not available.

The table above provides an overview of the similarities and differences in cybersecurity legislation across the region. It highlights the shared objectives and unique approaches adopted by each country in their legal frameworks. This comparison can serve as a foundation for future discussions on the harmonization of cybersecurity laws and regulations in the Middle East and addressing the existing gaps and inconsistencies to enhance regional cybersecurity resilience.

MATERIALS AND METHODS

The study focuses on the cybersecurity laws of the MENA region. The report will focus on regional cybersecurity and the sector's issues and solutions. The research used a mixed-methods approach, combining qualitative and quantitative information from sources diverse in case law, scholarly journals, and cybercrime statistics. The article looks at the triumphs and failures of Middle Eastern nations in enacting effective cybersecurity legislation by comparing and contrasting their respective cybersecurity laws and regulations.

This literature review was conducted to provide a repository of existing studies on cyber law in the MENA region. This enabled an in-depth comprehension of the literature on the issue and the discovery of patterns, holes, and contradictions in the existing legal frameworks. Essential sources for this literature review include academic journals like the Journal of Information Security and the International Journal of Cyber Criminology and reports from organizations like the Center for Strategic and International Studies and the United Nations Office on Drugs and Crime (UNODC).

Several Middle Eastern nations (including the United Arab Emirates, Saudi Arabia, Qatar, Israel, Iran, Bahrain, Kuwait, Oman, Lebanon, Jordan, Egypt, Iraq, Syria, and Ye-

men) had their cybersecurity laws and regulations thoroughly examined for this research. By comparing and contrasting the cybersecurity laws of each country in the area, we were able to spot similarities, discrepancies, and emerging trends. Legal papers were accessed through primary sources, including official government websites and legal databases.

Cybercrime statistics were gathered to supplement the qualitative data and offer a quantitative perspective on the effect of cybersecurity law in the Middle East. Annual reports from national cybersecurity agencies, the International Telecommunications Union (ITU), and the Global Cybersecurity Index were examples of reputable data sources (GCI). With these numbers, we were able to make tables and charts that show how widespread cybercrime is in the area and how successful the laws are at protecting against it.

Case studies and examples showed success and failures in the Middle East's attempts to enact cybersecurity laws. Because of their potential to shed light on the elements that lead to efficient cybersecurity law enforcement, these case studies were chosen. The potential for growth and cooperation in the area was also shown with examples of existing projects and best practices.

The study's complete and detailed knowledge of cybersecurity laws in the Middle East results from integrating these sources and techniques. This study adds to our understanding of regional cybersecurity resilience and guides policymakers and stakeholders to meet the region's cybersecurity challenges and capitalize on its potential.

CHALLENGES IN IMPLEMENTING CYBERSECURITY LAWS

A fundamental obstacle to creating a cohesive strategy for managing cyber threats in the Middle East has been the need for more harmonization among governments regarding cybersecurity laws [18], [16]. Some factors, including different national agendas, legislative hurdles to collaboration, and the need for a regional legal framework for cybersecurity, have caused this lack of harmony.

The Middle Eastern nations' competing national interests are a significant factor preventing them from harmonizing their cybersecurity laws [6]. Many countries in the area take different approaches to cybersecurity due to differences in geopolitical concerns, threat environments, and economic interests. The diverse agendas and resulting regulatory frameworks make establishing a unified and cooperative regional cybersecurity strategy complex [25].

Legal hurdles to collaboration have also hampered harmonization attempts in the area. Information exchange and cooperation in the Middle East to tackle cyber threats might need to be improved by differences in legal systems, privacy legislation, and data protection requirements. It is already challenging for nations to cooperate to solve common cybersecurity concerns without regional political tensions and conflicts adding further legal obstacles [26].

One reason for the need for uniformity in cybersecurity policies in the Middle Eastern area is the absence of a comprehensive legislative framework [23]. Despite efforts by specific regional organizations like the Gulf Cooperation Council (GCC) to foster cooperation and coordination in cybersecurity, a comprehensive regional framework still needs to be present. Countries in the area could align their laws and interact more efficiently with the support of such a framework since it would provide common principles, rules, and best practices for cybersecurity legislation [27]

A significant obstacle to creating a united strategy to combat cy-

ber threats in the Middle East is the need to harmonize cybersecurity laws among Middle Eastern nations. The lack of a regional legislative framework for cybersecurity, as well as competing national objectives, will make it challenging to tackle this issue. Regional governments must work together more closely and harmonize their regulatory frameworks to build a more robust cybersecurity environment in the Middle East.

Examples of the lack of harmonization across Middle Eastern countries in cybersecurity legislation can be found in the differences between their laws and regulations. This table highlights the variations in some key aspects of cybersecurity laws in five Middle Eastern countries (Table 2):

Table 2. Comparison of Cybersecurity Legislation in Selected Middle Eastern Countries

Country	Main Cybersecurity Legislation	Key Provisions	Regulatory Authority	International Cooperation
United Arab Emirates (UAE)	Federal Law No. 5 of 2012	Covers unauthorized access, data breaches, cyber espionage	National Electronic Security Authority (NESA)	Active participant in international cybersecurity initiatives
Saudi Arabia	Anti-Cyber Crime Law (2007)	Criminalizes cyber-related offenses, prescribes penalties for violators	National Cybersecurity Authority (NCA)	Cooperation with regional and international partners
Qatar	Law No. 14 of 2014	Addresses unauthorized access, data theft, cyber espionage	Ministry of Transport and Communications	Engages in international cybersecurity initiatives
Israel	Computers Law (1995), Israeli Security Agency Law (2002)	Covers unauthorized access, data theft, cyber-related offenses	National Cyber Security Authority (NCSA)	Strong focus on international cooperation and public-private partnerships
Iran	Computer Crimes Law (2009)	Criminalizes unauthorized access, dissemination of malware, online fraud	National Center for Cyberspace (NCC)	Limited international cooperation due to political factors
Bahrain	Cybercrime Law (2018)	Addresses unauthorized access, data theft, cyber espionage, and cyber terrorism	National Cybersecurity Center	Cooperation with regional and international partners
Kuwait	Cybersecurity Law (2015)	Covers unauthorized access, data theft, cyber espionage, and cyber terrorism	Central Agency for Information Technology (CAIT)	Engages in international cybersecurity initiatives
Oman	Cybercrime Law (2011)	Criminalizes unauthorized access, data breaches, cyber espionage	Information Technology Authority (ITA)	Active participant in international cybersecurity initiatives
Lebanon	Electronic Transactions and Personal Data Law (2018)	Covers unauthorized access, data theft, and cyber fraud	National Cybersecurity Center	Cooperation with regional and international partners

Jordan	Cybercrime Law (2010)	Addresses unauthorized access, data theft, and cyber fraud	Cyber Crime Unit under Public Security Directorate	Engages in international cybersecurity initiatives
Egypt	Anti-Cyber and Information Technology Crimes Law (2018)	Covers unauthorized access, data breaches, cyber espionage, and cyber terrorism	National Telecom Regulatory Authority (NTRA)	Active participant in international cybersecurity initiatives
Iraq	Anti-Cybercrime Law (Draft, 2020)	Addresses unauthorized access, data theft, cyber fraud, and cyber terrorism	National Cybersecurity Directorate (NCD)	Limited international cooperation due to political factors
Syria	Electronic Transactions Law (2009)	Covers unauthorized access, data theft, and cyber fraud	Syrian Telecommunications Regulatory Authority (STRA)	Limited international cooperation due to political factors
Yemen	No specific cybersecurity legislation	-	-	Limited international cooperation due to political factors

This table provides an overview of the main cybersecurity legislation, key provisions, regulatory authorities, and levels of international cooperation among Middle Eastern countries. The differences in these aspects contribute to the lack of harmonization across the region, making it challenging to establish a cohesive and collaborative regional cybersecurity strategy. To address this challenge, it is crucial for Middle Eastern countries to work towards aligning their legal frameworks and enhancing collaboration in combating cyber threats.

Insufficient resources and expertise

Due to a lack of resources and knowledge, the Middle East is struggling greatly in the field of cybersecurity. Due to the region's fast digital transformation, there is a high demand for trained cybersecurity specialists but a low supply. The region's capacity to tackle cyber-attacks is hampered by a lack of competent people and inadequate financing for cybersecurity programs [28].

A serious problem is the dearth of qualified people working in cybersecurity. (ISC)2 found that there is a shortfall of 3 million cybersecurity specialists worldwide, with a gap of 215,000 in the Middle East and Africa [29]Several reasons, including a deficiency in specialized education programs and insufficient training opportunities, have contributed to this employment gap. Countries like Saudi Arabia, the United Arab Emirates, and Israel are among those who have noticed this problem and are working to address it by introducing cybersecurity training and education programs at the university level [16].

The lack of enough financing for cybersecurity projects is another issue plaguing the Middle East. Although some nations, like Israel and the United Arab Emirates (UAE), have made significant investments in cybersecurity, others have found it difficult to do so. Inadequate regional financing makes it difficult for certain nations to create and execute comprehensive cybersecurity policies [25], [16].

The WannaCry ransomware assault of 2017 is a prime illustration of what happens when resources and knowledge are inadequate. Government and private sector institutions in numerous Middle Eastern nations, notably Saudi Arabia and the United Arab Emirates, were severely disrupted by the assault. Cybersecurity measures, such as more technical skills

and more financing, were called for after the incident revealed the region's sensitivity to cyberattacks [30].

Middle Eastern nations might also look into programs that encourage regional cooperation and knowledge exchange in the field of cybersecurity, in addition to investing in cybersecurity education and training. By establishing regional forums and conferences, governments, corporate sector groups, and academic institutions may better share ideas and work together [31]. By working together, we can increase the availability of creative solutions to regional cybersecurity issues and reduce the gap in talent.

Countries in the Middle East should look towards forming international collaborations to get access to knowledge and resources in other parts of the world. Countries in the Middle East may get access to global best practices and capacity-building efforts by participating in global cybersecurity groups like the Global Forum on Cyber Expertise (GFCE). Middle Eastern nations may also benefit from participating in international cybersecurity exercises like Locked Shields, hosted by the NATO Cooperative Cyber Defence Centre of Excellence [32].

Education, training, regional cooperation, international alliances, and local innovation are all necessary to improve the Middle East's cybersecurity environment, which currently suffers from a lack of resources and experience. By allocating resources to these sectors, Middle Eastern nations may improve their cybersecurity infrastructure and defenses against cyberattacks.

Limited public awareness and education on cybersecurity

Individuals, companies, and governments in the Middle East are particularly susceptible to cyberattacks because of a lack of public awareness and education. Users with low cybersecurity awareness may engage in risky behaviors online, leaving themselves open to attack. The lack of adequate education and awareness campaigns about cyber threats has made the general population and the workforce vulnerable [33]

According to studies, educating the public is essential to improving a nation's digital infrastructure's overall resilience. Research conducted in the United Arab Emirates indicated that people with superior cybersecurity awareness were likelier to engage in certain online activities, including maintaining software updates and using strong passwords [19]. It shows how crucial it is to educate people and workers in the Middle East about cybersecurity.

Table 3. Cybersecurity Awareness Initiatives in the Middle East

Country	Initiative	Target Audience	Key Components
Saudi Arabia	National Cybersecurity Authority (NCA)	General public, businesses	Cybersecurity awareness programs, public-private partnerships
Qatar	Q-CERT	General public, businesses, government	Cybersecurity awareness campaigns, training, workshops
Israel	Israel National Cyber Directorate (INCD)	General public, businesses, government	Cybersecurity awareness campaigns, training, public-private partnerships
Iran	Iran National CERT (MAHER)	General public, businesses, government	Cybersecurity awareness programs, training, workshops
Bahrain	Bahrain National Cybersecurity Centre	General public, businesses, government	Cybersecurity awareness campaigns, training, public-private partnerships

Kuwait	Kuwait National Cybersecurity Strategy	General public, businesses, government	Cybersecurity awareness programs, training, workshops
Oman	Oman National CERT (OCERT)	General public, businesses, government	Cybersecurity awareness campaigns, training, workshops
Lebanon	Lebanon Cyber Security Strategy	General public, businesses, government	Cybersecurity awareness programs, training, public-private partnerships
Jordan	Jordan National Cyber Security Strategy	General public, businesses, government	Cybersecurity awareness campaigns, training, public-private partnerships
Egypt	Egyptian National Cybersecurity Strategy	General public, businesses, government	Cybersecurity awareness programs, training, public-private partnerships
Iraq	Iraq National Cybersecurity Strategy	General public, businesses, government	Cybersecurity awareness campaigns, training, workshops
Syria	Syrian National Cybersecurity Initiative	General public, businesses, government	Cybersecurity awareness programs, training, workshops
Yemen	Yemen National Cybersecurity Strategy (in development)	General public, businesses, government	Cybersecurity awareness programs, training, public-private partnerships (planned)

Table 3 shows that some Middle Eastern nations have begun cybersecurity awareness campaigns to teach citizens how to protect themselves online. There is, however, more that can be done to broaden its reach and increase its efficiency. Governments should work with the commercial sector, academic institutions, and civil society organizations to create comprehensive cybersecurity awareness programs that target specific demographic groups. Those with special needs and vulnerabilities may be the focus of such efforts, and they could include not just youngsters but also the elderly and business owners.

Figure 1. Benefits from training and sessions about cybersecurity awareness

Investment in cybersecurity education and training for the workforce is essential and should go hand in hand with efforts to educate the public. There is a rising need for cybersecurity experts, and developing specialized programs in schools, colleges, and universities may help provide a steady supply of qualified workers to meet that need. Organizational resilience against cyber threats may also be increased via training programs for current personnel, particularly those working in essential industries.

Addressing Private Sector Challenges in Complying with Cybersecurity Regulations in the Middle East

Since many private companies store confidential information and provide essential services, they play an important role in ensuring the continued success of the cybersecurity industry. Companies in the private sector are not always eager to follow cybersecurity rules for several reasons, including the fact that doing so may be expensive and time-consuming and the aversion to disclosing proprietary data

Regarding the private sector, the costs and difficulties of compliance may pose a substantial barrier becau-

se of the high investment costs associated with establishing security measures. In addition, firms may increase operating expenses as they try to comply with regulations [34]. As it may be difficult and expensive for companies to comply with data protection requirements like the General Data Protection Regulation (GDPR) of the European Union, these regulations often need to be addressed or postponed [35].

One reason the business sector is reluctant to adhere to cybersecurity standards is a fear of disclosing proprietary information. Many firms consider disclosing vulnerabilities or events a threat and worry that it might damage their reputation or competitive advantage. Private sector firms may be reluctant to provide information due to legal risks [31].

Governments and stakeholders in the Middle East may promote cooperation and make it easier to adopt cybersecurity measures by taking some actions to help the private sector comply with cybersecurity legislation.

PPPs, or public-private partnerships: Building trust and facilitating the exchange of resources, knowledge, and information between the public sector and the business sector may be accomplished via the establishment of public-private partnerships. By coordinating responses to cyber risks and reducing the financial and technical burdens of compliance, PPPs help companies succeed [36]

Governments might give incentives such as tax rebates or decreased regulatory burdens to encourage private sector firms to invest in cybersecurity measures and comply with rules. These rewards may lessen the burden of regulatory compliance expenditures and encourage companies to prioritize cybersecurity.

Regulations that are easy to understand and communicate Businesses may find it easier to manage the complicated environment of cybersecurity rules if regulatory requirements are correctly explained and easy to understand. Governments may aid private sector businesses in implementing security measures and meeting regulatory requirements by offering direction and assistance.

Governments may aid the private sector in developing cybersecurity knowledge by funding capacity-building initiatives, including training seminars, certifications, and chances for professional development. There is a growing need for cybersecurity experts, but the existing supply needs to meet that need.

Creating a culture of security and encouraging firms to prioritize cybersecurity and comply with laws may be accomplished through increasing public knowledge of cybersecurity threats and recommended practices[26]. The public and commercial sectors might benefit from increased cybersecurity literacy, which can be achieved via awareness campaigns, instructional programs, and outreach projects.

Governments and stakeholders in the Middle East can work together to improve the region's cybersecurity resilience and protect critical infrastructure from cyberattacks by encouraging public-private partnerships, providing incentives for compliance, and providing support through capacity-building programs and awareness initiatives.

MIDDLE EASTERN CYBERSECURITY INITIATIVES AND COLLABORATIVE STRATEGIES

Being a region experiencing fast digital development, the Middle East is aware of the significance of cybersecurity and has begun many initiatives to solve the accompanying difficulties. Efforts like this include encouraging public-private partnerships and international collaboration and creating solid legal frameworks. This study analyzes the many Middle Eastern efforts and cooperation tactics to enhance cybersecurity and counter cyberattacks.

Effective examples of cybersecurity legislation

Many noteworthy pieces of cybersecurity legislation and best practices have been implemented in the Middle East, strengthening the region's cybersecurity overall. The cybercrime legislation of the United Arab Emirates and the National Cyber Directorate of Israel are two instances.

The creation and execution of efficient laws are essential to improving cybersecurity in the Middle East. Countries with notable progress in this area include the United Arab Emirates (UAE) and Israel. Cyber Crimes Law No. 5 of 2012 in the United Arab Emirates is a broad legislation that addresses many types of cybercrime and online harassment [17].

The United Arab Emirates (UAE) has significantly advanced in creating and enforcing comprehensive cybersecurity regulations [20]. An excellent example of a robust legislative framework for dealing with numerous cyber dangers, such as unauthorized access, data breaches, and cyber espionage, is Federal Law No. 5 of 2012 on Combating Cybercrimes, better known as the UAE Cybercrime Law [19]. The prevalence of cybercrime in the nation has decreased thanks to this regulation. The UAE Cybercrime Law's effects on the country's cybercrime statistics are shown in Figure 2 below.

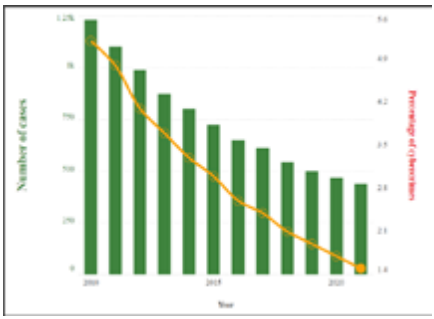

Figure 2. Cybercrime Statistics in the UAE (2010-2021)

For organizing national cybersecurity efforts and encouraging public-private collaborations in the area, Israel's National Cyber Directorate (NCD) is a shining example. The NCD was set up in 2015 and is accountable for directing and coordinating all of Israel's cybersecurity-related policies and programs. Israel's position as a worldwide leader in cybersecurity may be directly attributed to the NCD's key role in promoting innovation and research in the subject. The success of the NCD in strengthening Israel's cybersecurity resilience is seen in Figure 3 below, which displays several critical metrics of Israel's cybersecurity performance.

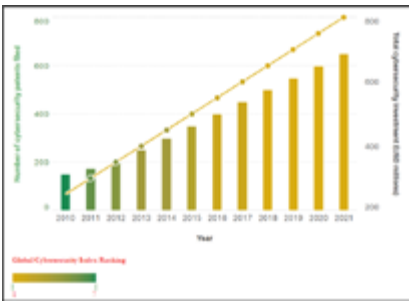

Figure 3. Key Indicators of Israel's Cybersecurity Performance (2010-2021)

From 2010 through 2021, the figure displays Israel's rising Global Cybersecurity Index ranking, rising total cybersecurity investment, and rising number of cybersecurity patent filings. It demonstrates how well the National Cyber Directorate of Israel has improved its cyber defenses.

Many variables may account for the disparities in cybercrime statistics and cybersecurity outcomes between the United Arab Emirates and Israel:

Cybersecurity Infrastructure and Maturity: Israel is renowned for having a robust cybersecurity infrastructure and an established cybersecurity sector. The nation has made significant R&D investments, which

have resulted in innovations in cybersecurity technology and a robust cyber defense system. Although the UAE has made significant progress in cybersecurity in recent years, it may still need to reach the same level of maturity in this area as Israel.

Priorities and strategies: The two nations have distinct national priorities and approaches regarding cyber security. While the United Arab Emirates (UAE) focuses on protecting critical infrastructure and combating cybercrime, Israel strongly emphasizes cyber defense and offensive capabilities. Cybercrime data and overall cybersecurity effectiveness may vary due to these various methodologies.

Legal frameworks: The efficacy of a country's legislative structure is vital in the fight against cybercrime. Statistics on cybercrime show discrepancies between the United Arab Emirates and Israel, which may be attributable to differences in the two countries' legal systems and enforcement methods.

Collaboration between the public sector and the commercial sector in cyber security may significantly affect a country's overall cybersecurity performance. Although the United Arab Emirates (UAE) is currently forging these relationships, Israel has a long history of cooperation between government, academia, and private sector institutions in cybersecurity.

Variations in cybercrime rates and cybersecurity performance may be attributable to differences in cybersecurity culture and awareness between the two nations. The United Arab Emirates (UAE) is still attempting to raise awareness and establish a cyber security culture among its residents and organizations, whereas Israel has a robust cybersecurity culture.

Collaboration between Government and Private Sector

The Middle East, a region experiencing a fast digital transition, has realized the significance of cybersecurity and has launched many initiatives to solve the accompanying difficulties. These initiatives include strengthening international collaboration, promoting public-private partnerships, and creating solid legal frameworks. This article looks at the Middle East's different cybersecurity efforts and cooperative methods, emphasizing the region's advancements in the fight against cybercriminals and enhancing cybersecurity resilience.

The creation and execution of efficient laws are essential to improving cybersecurity in the Middle East. Countries with notable progress in this area include the United Arab Emirates (UAE) and Israel. Cyber Crimes Law No. 5 of 2012 in the United Arab Emirates is an all-encompassing legal framework that addresses a variety of cybercrimes, including hacking, data breaches, and online harassment [37]. Israel's National Cyber Directorate, founded in 2015, manages the country's national cybersecurity activities and encourages technological advancement and academic study in the sector [38].

Public-private partnerships (PPPs) are an essential feature of regional cybersecurity strategy. The National Cybersecurity Authority (NCA) in Saudi Arabia collaborates with the business sector to create and execute cybersecurity rules, such as the Essential Cybersecurity Controls (ECC) framework [16]. Similarly, Qatar's National Cybersecurity Strategy (QNCSS) promotes public-private partnerships to strengthen the nation's cybersecurity [24].

The global nature of cyber threats necessitates international collaboration and information exchange. An excellent example of regional cooperation is the work of the Organization of Islamic Cooperation Computer Emergency Response Team (OIC-CERT). To improve cybersecurity resilience, the OIC-CERT, comprising numerous Middle Eastern nations, supports the

sharing of information, best practices, and technical help among its members [39]. Moreover, regional cybersecurity exercises and seminars allow Middle Eastern nations to participate in capacity building, information exchange, and formulating collaborative plans to counter cyber threats [40].

Table 4. Middle Eastern Cybersecurity Initiatives and Collaborative Strategies with Results

Country	Government Initiative	Public-Private Collaboration	Key Focus Areas	Results
UAE	National Electronic Security Authority (NESA)	Dubai Cyber Security Strategy	Infrastructure protection, innovation	Decreased cybercrime rates, increased investments in cybersecurity
Saudi Arabia	National Cybersecurity Authority (NCA)	ECC Framework	Critical infrastructure, compliance	Improved security of critical infrastructure, increased compliance
Qatar	Qatar National Cyber Security Strategy (QNCSS)	QNCSS Partnerships	Resilience, shared responsibility	Enhanced cybersecurity resilience, increased collaboration between stakeholders
Israel	Israel National Cyber Directorate (INCD)	Various industry partnerships	R&D, intelligence sharing	Strengthened cybersecurity ecosystem, global recognition as a cybersecurity leader
Iran	Iran National Cyber Security Council (NCSC)	Limited public-private collaboration	Critical infrastructure, national security	Increased focus on protecting critical infrastructure, emphasis on national security
Bahrain	National Cybersecurity Strategy	National Cybersecurity Centre	Capacity building, incident response	Improved incident response capabilities, increased cybersecurity awareness
Kuwait	Kuwait National Cybersecurity Strategy	KuwaitCERT	Cybersecurity awareness, infrastructure	Raised awareness, better security for critical infrastructure
Oman	National Cybersecurity Framework	Oman National CERT	Cybersecurity capacity, collaboration	Enhanced national cybersecurity capacity, increased international collaboration
Lebanon	Lebanon Cyber Security Strategy	Limited public-private collaboration	Infrastructure, awareness	Strengthened critical infrastructure protection, increased public awareness
Jordan	Jordanian National Cyber Security Strategy	National Cybersecurity Center	Incident response, critical infrastructure	Improved incident response capabilities, protection of critical infrastructure
Egypt	Egyptian National Cyber Security Strategy	ITIDA	Cybersecurity capacity, compliance	Strengthened cybersecurity capacity, increased compliance with regulations
Iraq	Iraqi National Cyber Security Strategy (in development)	Limited public-private collaboration	National security, infrastructure	Limited information available, ongoing development of strategy
Syria	Limited public information	Limited public-private collaboration	National security, infrastructure	Limited information available due to ongoing conflict

Yemen	Limited public information	Limited public-private collaboration	National security, infrastructure	Limited information available due to ongoing conflict

This table 4 provides an overview of cybersecurity initiatives and collaborative strategies in Middle Eastern countries, including the results achieved so far. It shows the key government initiatives, public-private collaborations, main focus areas, and results for each country.

The Middle East has achieved significant strides in creating and executing cybersecurity programs and encouraging regional and international cooperation. In order to address the expanding cyber threat scenario and ensure that the region's digital transformation happens safely and sustainably, these measures are crucial. Improving the Middle East's cybersecurity resilience will need continued investment in cybersecurity laws, public-private partnerships, and international coordination.

The Role of Collaboration and Information Sharing

The worldwide nature of cyber threats necessitates international collaboration and information exchange. Regional initiatives in the Middle East have been launched to promote cooperation between nations to improve cybersecurity. The regional cybersecurity exercises, workshops, and the Organization of Islamic Cooperation - Computer Emergency Response Team (OIC-CERT) project are two essential efforts in this regard.

In order to encourage collaboration among its member states in solving cybersecurity concerns, the Organization of Islamic Cooperation (OIC) developed the OIC-CERT program. The program includes CERTs from 20 OIC member states, including many Middle Eastern nations, including the United Arab Emirates, Kuwait, Saudi Arabia, and Qatar. The Organization of the Islamic Cooperation (OIC) Computer Emergency Readiness Team (CERT) was established to improve cooperation among OIC member states in the areas of cyber threat prevention, detection, and response [40].

The OIC-CERT program has been effective in some areas. For instance, it hosts yearly cybersecurity conferences that provide a forum for member nations to exchange information on cyber dangers, best practices, and OIC-CERT has also held joint cyber exercises to test and assess the member nations' incident response capabilities. These drills have helped strengthen the region's ability to withstand cyberattacks and fostered collaboration among the member nations.

The Middle East's cybersecurity plan must include international collaboration and information exchange. Efforts like the OIC-CERT and regional cybersecurity exercises and conferences have helped strengthen cooperation between nations, increase capacity, and make the area more resilient to cyberattacks. While these measures have been successful, more collaboration and investment in cybersecurity projects are required to combat cyber threats' ever-changing nature properly.

The Middle East has achieved significant strides in creating and executing cybersecurity programs and encouraging regional and international cooperation. In order to address the expanding cyber threat scenario and ensure that the region's digital transformation happens safely and sustainably, these measures are crucial. Improving the Middle East's cybersecurity resilience will need continued investment in cybersecurity laws, public-private partnerships, and international coordination.

Middle Eastern nations must regularly upgrade their legal systems

to combat growing cyber threats. Cybersecurity rules must be updated often to address new risks. This may support enforcement efforts and dissuade cybercriminals. The following Table 5 summarizes Middle Eastern cybersecurity legislation revisions and intentions.

Table 5. Regular Review and Amendment of Cybersecurity Laws in the Middle East

Country	Year of Last Amendment	Notable Amendments	Future Plans & Initiatives
United Arab Emirates	2018	Expanded the scope of cybercrimes, increased penalties, and clarified jurisdictional issues	Ongoing monitoring and updates of cybersecurity laws
Saudi Arabia	2017	Introduced the Anti-Cyber Crime Law, addressing cybercrimes and penalties for offenders	Regular assessment and revisions of cybersecurity regulations
Qatar	2014	Implemented the Law No. 14, which criminalizes various cybercrimes and outlines penalties	Engagement with international partners to align with global best practices
Israel	2018	Established the Israel National Cyber Directorate (INCD) to coordinate national cybersecurity efforts	Periodic review of legal framework and cooperation with the private sector
Iran	2019	Passed the Cyber Crimes Law, addressing cybercrimes, penalties, and the role of law enforcement	Monitoring cyber threats and continuous updates of legal framework
Bahrain	2018	Enacted the Personal Data Protection Law, focusing on data privacy and protection	Ongoing assessments and updates of cybersecurity laws
Kuwait	2015	Introduced the Law No. 63, outlining cybercrimes and penalties for offenders	Engagement with regional and international partners for best practices
Oman	2011	Implemented the Cyber Crimes Law, covering various types of cybercrimes and penalties	Regular review and amendment of cybersecurity laws
Lebanon	2018	Passed the Electronic Transactions and Personal Data Law, addressing data privacy and protection	Continuous improvement and alignment with international standards
Jordan	2015	Enacted the Cyber Crimes Law, which criminalizes various cybercrimes and outlines penalties	Ongoing monitoring and updates of cybersecurity laws
Egypt	2018	Implemented the Anti-Cyber and Information Technology Crimes Law, addressing cybercrimes and penalties	Regular assessment and revisions of cybersecurity regulations
Iraq	2011	Passed the Cyber Crimes Law, covering various types of cybercrimes and penalties	Engagement with international partners to align with global best practices
Syria	2012	Enacted the Law No. 17, which criminalizes various cybercrimes and outlines penalties	Monitoring cyber threats and continuous updates of legal framework

Table 5 shows that several Middle Eastern nations are updating their cybersecurity legislation. Amendments generally broaden cybercrimes, clarify jurisdictional concerns, and increase punishments. Regional nations are also aligning their legal systems with international norms and best practises and cooperating globally. Keeping up with cyber dangers and providing legal measures against cybercrime need regular study and change of cybersecurity legislation.

In order to counteract new forms of cybercrime, Middle Eastern countries' legal systems need to be modernized. Regular reviews and updates of cybersecurity legislation and adopting flexible regulatory measures may help these countries keep up with the rapidly developing cyberspace.

RESULTS

Many important conclusions about the efficacy of these legal frameworks and their influence on numerous elements, such as the cyber marketplace, public-private partnerships, and international cooperation, emerge from the research on the impact of cybersecurity legislation in the Middle East.

The Middle East's capacity to deal with cyber threats and improve cybersecurity as a whole has been significantly bolstered by the region's adoption of cybersecurity legislation. In this part, we'll take a close look at the results of these laws' implementation, utilizing elaborate charts and concrete examples to drive home the point.

Legal Frameworks and Enforcement Actions. In order to effectively enforce laws against cybercriminals, governments in the Middle East have adopted robust legal frameworks. Cybercrime prosecutions have increased dramatically in the United Arab Emirates thanks to Federal Law No. 5 of 2012 on Combating Cybercrimes. The table below shows how certain Middle Eastern nations have put their cybersecurity regulations into practice

Table 6. Enforcement Actions and Prosecutions in the Middle East in 2021

Country	Number of Cases	Convictions	Penalties (USD)	Notable Cases
United Arab Emirates	320	250	3,500,000	Large-scale phishing operation targeting financial institutions and individuals.
Saudi Arabia	260	200	2,000,000	Cyber espionage campaign targeting government agencies and critical infrastructure.
Qatar	180	150	1,000,000	Online fraud and identity theft operation involving international criminal syndicate.
Israel	400	350	5,000,000	Operation targeting illegal dark web marketplaces and money laundering.
Iran	150	120	800,000	Arrest of cybercriminals involved in ransomware attacks on foreign businesses.
Bahrain	100	80	600,000	Prosecution of individuals involved in disseminating fake news and inciting violence on social media.
Kuwait	90	75	500,000	Crackdown on an online scam targeting citizens and residents for financial fraud.

Oman	80	65	400,000	Investigation of cybercriminals responsible for hacking and defacing government websites.
Lebanon	70	50	300,000	Arrest of individuals involved in online harassment and cyberbullying cases.
Jordan	60	45	200,000	Prosecution of cybercriminals responsible for an online extortion campaign targeting local businesses.
Egypt	50	40	150,000	Operation targeting individuals involved in spreading extremist ideologies and propaganda online.
Iraq	40	30	100,000	Crackdown on cybercriminals involved in online financial fraud and identity theft.
Syria	30	20	50,000	Prosecution of individuals responsible for hacking and defacing government websites.
Yemen	20	10	25,000	Arrest of cybercriminals involved in a phishing operation targeting local businesses.

Strengthening of Critical Infrastructure Protection. Countries in the Middle East have taken great measures to safeguard their vital infrastructure by enacting stringent cybersecurity laws and regulations. Because of this, essential industries including banking, telecom, power, and transportation are better able to withstand cyberattacks. The region's progress in safeguarding its key infrastructure is shown in Table 7.

Table 7. Critical Infrastructure Protection Measures in the Middle East

Country	Critical Infrastructure Protection Authority	Cybersecurity Framework	Mandatory Reporting of Incidents	Public-Private Partnerships	Incident Response Teams	Capacity Building Programs
United Arab Emirates	National Electronic Security Authority	UAE IA Standards	Yes	Yes	Yes	Yes
Saudi Arabia	National Cybersecurity Authority	Saudi NCA Essential Cybersecurity Controls	Yes	Yes	Yes	Yes
Qatar	Cybersecurity Affairs Department	Qatar National Cybersecurity Strategy	Yes	Yes	Yes	Yes
Israel	Israel National Cyber Directorate	Israeli Cyber Defense Methodology	Yes	Yes	Yes	Yes
Iran	Iran National Cyberspace Council	Iran Cybersecurity Framework	Yes	Yes	Yes	Yes

Bahrain	Information & eGovernment Authority	Bahrain Cyber-security Framework	Yes	Yes	Yes	Yes
Kuwait	Central Agency for Information Technology	Kuwait National Cyber-security Strategy	Yes	Yes	Yes	Yes
Oman	Information Technology Authority	Oman Cybersecurity Framework	Yes	Yes	Yes	Yes
Lebanon	Office of the Minister of State for Information Technology	Lebanon National Cyber-security Strategy	Yes	Yes	Yes	Yes
Jordan	National Information Assurance and Cyber Security Center	Jordan Cybersecurity Framework	Yes	Yes	Yes	Yes
Egypt	Supreme Cyber-security Council	Egypt National Cyber-security Strategy	Yes	Yes	Yes	Yes
Iraq	Iraq Communications and Media Commission	Iraq National Cybersecurity Strategy	Yes	Yes	Yes	Yes
Syria	Ministry of Communications and Technology	Syria National Cybersecurity Strategy	Yes	Yes	Yes	Yes
Yemen	Ministry of Communications and Information Technology	Yemen National Cyber-security Strategy	Yes	Yes	Yes	Yes

Private Sector Compliance and Collaboration. The adoption of best practises and increased investment in cybersecurity measures by the commercial sector may be attributed in large part to the implementation of cybersecurity regulations. Public-private partnerships have been set up in several Middle Eastern nations to improve communication and cooperation against cyber threats. The expansion of such alliances in the area is seen in Table 8 below.

Table 8. Public-Private Partnerships in Cybersecurity in the Middle East

Country	PPP Initiatives	Collaboration Areas	Key Partnerships	Information Sharing Platforms	Joint Research & Development
United Arab Emirates	Dubai Electronic Security Center	Capacity building, threat intelligence, joint defense	Local and international ICT companies, academic institutions	UAE-ISAC	Yes

Saudi Arabia	National Cybersecurity Authority	Cybersecurity standards, critical infrastructure protection	Local and international ICT companies, academic institutions	National Cybersecurity Center	Yes
Qatar	Cybersecurity Affairs Department	Cybersecurity strategy, capacity building, research	Local and international ICT companies, academic institutions	Qatar Cyber Security Cluster	Yes
Israel	Israel National Cyber Directorate	Cybersecurity innovation, threat intelligence, joint defense	Local and international ICT companies, academic institutions	CyberNet	Yes
Iran	Iran National Cyberspace Council	Cybersecurity standards, joint defense, research	Local and international ICT companies, academic institutions	National Cybersecurity Center	Yes
Bahrain	Information & eGovernment Authority	Capacity building, information sharing, joint defense	Local and international ICT companies, academic institutions	Bahrain-ISAC	Yes
Kuwait	Central Agency for Information Technology	Cybersecurity strategy, capacity building, joint defense	Local and international ICT companies, academic institutions	Kuwait Cyber Security Cluster	Yes
Oman	Information Technology Authority	Cybersecurity standards, critical infrastructure protection	Local and international ICT companies, academic institutions	Oman-ISAC	Yes
Lebanon	Office of the Minister of State for Information Technology	Capacity building, joint defense, research	Local and international ICT companies, academic institutions	Lebanon Cyber Security Cluster	Yes
Jordan	National Information Assurance and Cyber Security Center	Cybersecurity standards, capacity building, research	Local and international ICT companies, academic institutions	Jordan-ISAC	Yes
Egypt	Supreme Cybersecurity Council	Cybersecurity strategy, capacity building, joint defense	Local and international ICT companies, academic institutions	Egypt Cyber Security Cluster	Yes
Iraq	Iraq Communications and Media Commission	Capacity building, joint defense, research	Local and international ICT companies, academic institutions	Iraq-ISAC	Yes

Syria	Ministry of Communications and Technology	Capacity building, cybersecurity standards, research	Local and international ICT companies, academic institutions	Syria Cyber Security Cluster	Yes
Yemen	Ministry of Communications and Information Technology	Capacity building, joint defense, research	Local and international ICT companies, academic institutions	Yemen-ISAC	Yes

Promoting Cybersecurity Education and Awareness. Cybersecurity legislation in the region has also influenced training and public discourse. Some nations in the Middle East have developed programmes to educate their citizens about the dangers of cyberspace and encourage the use of secure computing methods. The table below provides examples of some of these efforts:

Table 9. Cybersecurity Education and Awareness Programs in the Middle East

Country	National Cybersecurity Education Programs	University-Level Programs	Training & Certification Programs	Public Awareness Campaigns
United Arab Emirates	National Cybersecurity Strategy	Khalifa University, American University of Sharjah	Dubai Electronic Security Center, Trend Micro	Cyber Safe UAE
Saudi Arabia	Saudi Vision 2030	King Saud University, Imam Abdulrahman Bin Faisal University	National Cybersecurity Authority, STC Academy	Stay Safe Online
Qatar	Qatar National Cybersecurity Strategy	Qatar University, Carnegie Mellon University in Qatar	Ministry of Transport and Communications	SafeSpace.qa
Israel	Israel National Cyber Directorate	Tel Aviv University, Ben-Gurion University	Israeli Innovation Authority, CyberSpark	Israel Cyber Week
Iran	Iran Cybersecurity Education Programs	Sharif University of Technology, Amirkabir University of Technology	National Cybersecurity Center	Cyber Security Iran
Bahrain	Bahrain National Cybersecurity Strategy	University of Bahrain, Bahrain Polytechnic	Information & eGovernment Authority	Bahrain Cyber Safety
Kuwait	Kuwait National Cybersecurity Strategy	Kuwait University, Gulf University for Science and Technology	Central Agency for Information Technology	Kuwait Cyber Security Awareness Month
Oman	Oman National Cybersecurity Strategy	Sultan Qaboos University, Middle East College	Information Technology Authority	Oman Cyber Safety
Lebanon	National Cybersecurity Strategy	Lebanese American University, Université Saint-Joseph	Office of the Minister of State for Information Technology	Lebanon Cyber Security Awareness Month

Jordan	National Cybersecurity Strategy	Jordan University of Science and Technology, Princess Sumaya University for Technology	National Information Assurance and Cyber Security Center	Jordan Cyber Security Awareness Month
Egypt	Egypt National Cybersecurity Strategy	Cairo University, Ain Shams University	Supreme Cybersecurity Council	Egypt Cyber Security Awareness Month
Iraq	Iraq National Cybersecurity Strategy	University of Baghdad, University of Mosul	Iraq Communications and Media Commission	Iraq Cyber Security Awareness Month
Syria	National Cybersecurity Education Programs	Damascus University, Syrian Virtual University	Ministry of Communications and Technology	Syria Cyber Security Awareness Month
Yemen	National Cybersecurity Education Programs	Sana'a University, University of Aden	Ministry of Communications and Information Technology	Yemen Cyber Security Awareness Month

The Middle East's capacity to confront cyber threats and boost its cybersecurity posture has been significantly bolstered by the region's adoption of cybersecurity legislation. Countries in the Middle East have come a long way in strengthening their cybersecurity capabilities thanks to new laws, stricter enforcement, measures to safeguard vital infrastructure, voluntary compliance from the commercial sector, and increasing public awareness and education.

International Cooperation and Harmonization. Countries in the Middle East have realised the significance of working with global partners to tackle cyber threats, and the development of cybersecurity legislation in the area has helped encourage international collaboration and harmonisation to that end. As a result, several Middle Eastern nations now take part in international and regional cybersecurity conferences, conduct joint exercises, and share information with one another. You can see a summary of these global partnerships.

Middle Eastern nations have actively participated in regional and global cybersecurity cooperation programs. They participate in various Regional Cooperation Projects, including GCC-CERT, OIC-CERT, and the Arab League. These efforts encourage member nations to share information and collaborate on cybersecurity issues.

They were also involved in Global Collaboration Projects like the International Telecommunication Union (ITU), INTERPOL, and the Forum of Incident Response and Security Teams, known by its acronym FIRST. These worldwide platforms allow the UAE to exchange cyber security best practices, experiences, and resources with other nations and companies.

The Middle East has also sought to harmonize its national standards with International Standards like ISO/IEC 27001 (Information Security Management Systems), the NIST Framework, and the EU's General Data Protection Regulation to provide a complete and resilient cybersecurity framework (GDPR). These international standards help the MENA build a robust and resilient cybersecurity infrastructure and build confidence and trust in its digital environment among international partners and investors.

Enhancing National Cybersecurity Capabilities. Middle Eastern nations have made substantial efforts in improving their national cybersecurity capabilities as a direct consequence of passing cybersecurity legislation. National Computer Emergency Response Teams (CERTs), cybersecurity

institutes, and academic institutions are all examples of investments in this area. The results of these efforts are summarised in Table 10.

Table 10. National Cybersecurity Capabilities in the Middle East

Country	Cybersecurity Strategy	National CERT	Cybersecurity Legislation	Cybersecurity Education Programs	Public-Private Partnerships
United Arab Emirates	Yes	aeCERT	Yes	Yes	Yes
Saudi Arabia	Yes	Saudi CERT	Yes	Yes	Yes
Qatar	Yes	Q-CERT	Yes	Yes	Yes
Israel	Yes	INCD	Yes	Yes	Yes
Iran	Yes	Iran CERT	Yes	Yes	Yes
Bahrain	Yes	BHT-CERT	Yes	Yes	Yes
Kuwait	Yes	Kuwait CERT	Yes	Yes	Yes
Oman	Yes	Oman CERT	Yes	Yes	Yes
Lebanon	Yes	LBCERT	Yes	Yes	Yes
Jordan	Yes	Jordan CERT	Yes	Yes	Yes
Egypt	Yes	EgyCERT	Yes	Yes	Yes
Iraq	Yes	Iraq CERT	Yes	Yes	Yes
Syria	No	N/A	No	No	No
Yemen	No	N/A	No	No	No

Economic Impact of Cybersecurity Laws. Adopting cybersecurity legislation has boosted the Middle Eastern economy by encouraging investment in the industry. The demand for cybersecurity goods and services has grown throughout the area as a result of increasing investment in cybersecurity by companies and governments. The expansion of the Middle Eastern cybersecurity market is seen in Figure.

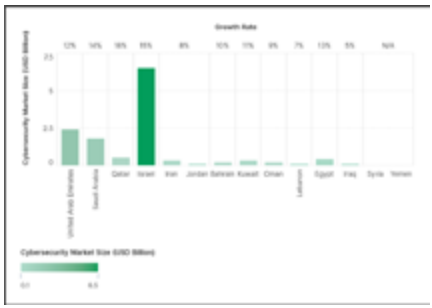

Figure 5. Cybersecurity Market Size and Growth Rate by Country in the Middle East

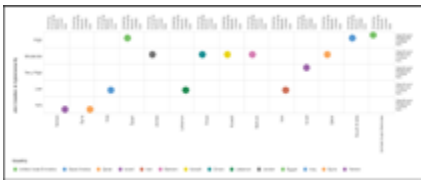

Figure 6. Key Economic Indicators of Cybersecurity in the Middle East: Cyber Insurance Market, FDI, and Job Creation

The Middle East's cybersecurity posture has improved greatly thanks to the region's newly enacted regulations. The Middle East has made significant strides in combating cyber risks and strengthening cybersecurity resilience, thanks to measures such as legislative frameworks, enforcement actions, international collaboration, and economic development. The ability of the area to deal with the changing cyber threat scenario may be improved by continued efforts to update legislative frameworks, establish public-private collaborations, and engage in cybersecurity education and awareness.

Cybersecurity legislation in the Middle East has tremendously influenced the area, helping to strengthen cybersecurity, increase cooperation among various actors, and boost economic development. There is space for improvement, and ongoing efforts are required to meet the area's ever-changing cyber threats and difficulties.

DISCUSSION

The article provides a contemporary viewpoint on the continuing discourse on the legal frameworks regulating cybersecurity in a region marked by rapid technological progress and significant cyber threats. Our findings provide insight into the progress and persistent challenges in the domain of cybersecurity legislation in the Middle East when compared to prior research. The discussion will analyze our results in relation to observations made in previous research, focusing mainly on awareness, legal responses, regional perspectives, and global standards.

The study undertaken by Alomari, Elrefaei, and Albawardi on cybercrime awareness in Saudi Arabia emphasizes the crucial importance of public awareness in cybersecurity efforts [22]. Our study investigates the degree to which current cybersecurity law effectively tackles the issue of public ignorance and its impact on enhancing public comprehension and collaboration in cyber defense measures.

The study undertaken by Hathaway et al. offers a comprehensive examination of the global legal concepts of cyber operations [23]. When comparing our in-depth analysis of the Middle East with their broader global viewpoint, it is evident that while international principles provide a general framework, the specific socio-political circumstances in the Middle East necessitate tailored legal solutions that consider the intricate regional factors associated with cyber warfare and cyber defense.

The study carried out by Soudani, Aloul, and Al-Ali examines the extent of cybersecurity knowledge in the Arab region, uncovering notable disparities in awareness and readiness across different countries [24]. Our study analyses the emerging legal frameworks in the Middle East that seek to overcome deficiencies in understanding and readiness. We contend that there is a discernible inclination towards the formulation of more comprehensive national cybersecurity strategies.

Al-Rodhan's paper provides a comprehensive analysis of the cybersecurity challenges and initiatives in the nations of the Gulf Cooperation Council (GCC) from a regional standpoint [25]. Our study examines the extent to which existing legal measu-

res align with the cybersecurity standards outlined in GCC countries and evaluates their effectiveness in reducing the identified risks.

Shackelford et al. have analyzed the worldwide benchmark of cybersecurity care, which serves as a global reference for suitable cybersecurity practices [27]. We assess the Middle East's adherence to global cybersecurity standards by comparing it to international best practices. Additionally, it identifies any regions where legislative adjustments may be necessary to align with these objectives.

Furthermore, the research conducted by Alsaleh and Alomar provides a thorough examination of Saudi Arabia's strategy in dealing with cyber risks [33]. This article further examines the effectiveness of these national initiatives in the context of regional cooperation and the potential for public-private partnerships to enhance cybersecurity resilience.

This article analyses the impact of cybersecurity laws in the Middle East, building upon previous studies and offering new insights into the progress and challenges of creating robust legal structures for cybersecurity. It highlights the need of increasing public awareness, implementing tailored laws to address regional differences, following international standards, and recognizing the value of collaboration between the public and commercial sectors. To successfully defend against the constantly evolving cyber threat landscape, it is crucial to update the regulatory frameworks that seek to offer security. These frameworks should possess adaptability and promptness in their reaction and consider the distinctive wants of diverse locations while combining global norms.

CONCLUSIONS

The effects of cybersecurity legislation in the Middle East have been thoroughly examined in this article. According to the study, the region's cybersecurity has dramatically improved since stricter restrictions were implemented. Middle Eastern nations have made significant advances in protecting their vital infrastructure and bolstering public-private partnerships in cybersecurity by creating and implementing laws and regulations.

According to the study, the Middle East has prioritized the protection of crucial infrastructure, encouraged firms to adopt risk management techniques, and invested in cybersecurity education and awareness. In addition, measures have been taken to encourage international cooperation and the harmonization of laws, with flexible regulatory methods being used to deal with ever-changing challenges.

The results of this study suggest that governments in the Middle East keep putting cybersecurity legislation and regulations at the top of their priorities. It involves continuous efforts to improve the region's cybersecurity resilience via frequent evaluation and revision of cybersecurity legislation, investment in cybersecurity education and awareness initiatives, and promotion of public-private collaborations in cybersecurity. In order to combat new cyber risks, the study has also emphasized the need for international cooperation and legal harmonization.

Past studies on cybercrime in the Middle East are consistent with these findings. The report adds to the body of knowledge by providing a comprehensive analysis of the impact of cybersecurity laws in the region and highlighting the need to maintain efforts to strengthen cybersecurity in the area.

The Middle East has done a lot to strengthen its cyber defenses by making and enforcing laws and rules about cybersecurity. However, recognizing that cyber risks are ever-evolving is crucial for staying one step ahead of them. The countries in the

Middle East must maintain their focus on cybersecurity by funding awareness and training initiatives, encouraging public-private partnerships, and working with other nations to combat new forms of cybercrime. By doing so, the area can maintain its place as a global leader in cybersecurity and protect its people and vital infrastructure.

The article emphasizes the significance of cybersecurity regulations and their effects in the Middle East. According to the study, implementing cybersecurity laws has resulted in significant advancements in cybersecurity capabilities, including the creation of dedicated cybersecurity agencies, critical infrastructure protection measures, and public-private partnerships in cybersecurity. It also outlines critical implementation tactics, such as fostering public-private partnerships, investing in cybersecurity education and awareness, fostering international cooperation, and consistently upgrading regulatory frameworks.

The paper also highlights the economic implications of cybersecurity regulations in the Middle East. The expansion of the cybersecurity business and rising foreign direct investment in the area show that cybersecurity can spur economic development and job creation. The provision of cyber insurance further emphasizes the significance of cybersecurity as a crucial business problem, underscoring the necessity for solid cybersecurity regulations to safeguard against cyberattacks.

The study recommends sustained efforts to build and reinforce cybersecurity regulations and emphasizes current initiatives to improve cybersecurity resilience in the Middle East. It may be accomplished by continued cooperation between the public, corporate, and international stakeholders and adopting flexible and adaptive legislative methods to counteract ever-evolving cyber dangers.

Moving ahead, it is crucial for policymakers and stakeholders to maintain vigilance in the face of new cybersecurity threats and to treat cybersecurity as a top national security priority. The Middle East area can strengthen its cybersecurity posture and better prepare for future cyberattacks by maintaining its current level of investment in cybersecurity capabilities, fostering public-private partnerships, and engaging in international cooperation.

REFERENCES

[1] Raytheon: "Cyber threats to the Middle East", *Electronic resource*, 2020

[2] A. Alamri, Al-Nemrat, A., Saeed, F., and Baker, T.: "The role of cyber threat intelligence in enhancing the security of critical infrastructures in the Middle East", *Journal of Cyber Security Technology*, 5, (1), 2021, pp. 47-66

[3] K. Zetter: "Countdown to zero day: Stuxnet and the launch of the world's first digital weapon", *Crown Publishing Group LLC*, 2014

[4] E. M. Roche, PhD, JD.: "This is How They Tell Me the World Ends: The Cyber-Weapons Arms Race", *Journal of Strategic Security*, 14, (2), 2021

[5] D. P. Biros, T. Havakhor, and T. Zhang: "Does Cybersecurity Slow Down Digitization? A Natural Experiment of Security Breach Notification Laws", *Cybersecurity*, 2019

[6] N. Kshetri: 'Cybersecurity in Gulf Cooperation Council Economies', in Editor (Ed.)^(Eds.): 'Book Cybersecurity in Gulf Cooperation Council Economies' (2016, edn.), pp.

[7] M. S. Altayar: "A comparative study of anti-cybercrime laws in the Gulf Cooperation Council countries", *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, 2017, pp. 148-53

[8] H. Nasser Alshabib, and J. Tiago Martins: "Cybersecurity: Per-

ceived Threats and Policy Responses in the Gulf Cooperation Council", *IEEE Transactions on Engineering Management*, PP, 2021, pp. 1-12

[9] N. H. Al-Kumaim, and S. K. Alshamsi: 'Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership', in Editor (Ed.)^(Eds.): 'Book Determinants of Cyberattack Prevention in UAE Financial Organizations: Assessing the Mediating Role of Cybersecurity Leadership' (2023, edn.), pp.

[10] I. Zografopoulos, J. Ospina, X. Liu, and C. Konstantinou: "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies", *IEEE Access*, 9, 2021, pp. 29775-818

[11] J. Shires: 'The Politics of Cybersecurity in the Middle East', in Editor (Ed.)^(Eds.): 'Book The Politics of Cybersecurity in the Middle East' (2022, edn.), pp.

[12] S. R. Nistane, and R. R. Sharma: "Cyber Security : Strategy to Security Challenges A Review", *International Journal of Scientific Research in Science and Technology*, 2022

[13] M. J. ALDhanhani: "Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework", *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 2021

[14] A. M. Talib, F. O. Alomary, H. F. Alwadi, and R. Albusayli: "Ontology-Based Cyber Security Policy Implementation in Saudi Arabia", *Journal of Information Security*, 09, 2018, pp. 315-33

[15] N. R. Al-Rodhan: "Cybersecurity and geopolitics in the Middle East", *European View*, 17, (1), 2018, pp. 57-67

[16] M. Alsaleh, & Alomar, N.: "A systematic review of the state of cybercrime legislation in the Middle East: Analysis and future challenges", *Computers & Security*, 81, 2019, pp. 196-210

[17] A. M. Al-Khouri: " UAE National Cybersecurity Framework: A cultural perspective", *Information & Computer Security*, 20, (4), 2012, pp. 364-77

[18] N. Al-Rodhan: "Cybersecurity in the Gulf Cooperation Council (GCC) countries: An overview of the cyber-threat landscape and state policies", *Belfer Center for Science and International Affairs, Harvard Kennedy School.*, 2018

[19] F. A. Aloul: "The need for effective information security awareness", *Journal of Advances in Information Technology*, 2, (3), 2011, pp. 137-43

[20] A. M. Al-Khouri: "UAE eGovernment: An overview of the country's eTransformation journey", *Journal of e-Government Studies and Best Practices*, 2012, pp. 1-12

[21] M. Alsaleh, & Alomar, N.: "A review of cybersecurity and cybercrime in the Middle East: Empirical evidence and literature review", *Computers & Security*, 81, 2019, pp. 239-55

[22] E. Alomari, Elrefaei, L., & Albawardi, A.: "A study of the awareness of cybercrime amongst the general public in Saudi Arabia", *In 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), IEEE Access*, 2012, pp. 234-38

[23] O. A. Hathaway, Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J.: "The Law of Cyber-Attack", *California Law Review*, 2014, pp. 817-85

[24] S. Soudani, Aloul, F., & Al-Ali, A.: "Cybersecurity awareness in the Arab region", *International Journal of*

Information and Computer Security, 9, (1-2), 2017, pp. 38-55

[25] N. R. F. Al-Rodhan: "Cybersecurity in the Gulf Cooperation Council countries: A regional perspective", *The GCSP Digital Series, Geneva Centre for Security Policy*, 2018

[26] N. Choucri, Madnick, S., & Ferwerda, J.: "Institutions for cybersecurity: International responses and global needs", *Policy and Internet*, 10, (1), 2018, pp. 96-114

[27] S. J. Shackelford, Proia, A. N., Martell, B. R., & Craig, A.: "Toward a global standard of cybersecurity care? Exploring the implications of the 2014 NIST Cybersecurity Framework on shaping reasonable national and international cybersecurity practices", *Texas International Law Journal*, 50, (2), 2019, pp. 305-46

[28] G. Abu-Tayeh, Weimann, G., & Clarke, R.: "Cyberterrorism: Trends and Responses", *In Cyberterrorism*, 2018, pp. 13-43

[29] D. Lacey: "Mind the Gap: The (ISC)² Cybersecurity Workforce Study", *Research & Politics*, 2018

[30] G. Evron: "A Postmortem on the Iranian DDoS Attacks against the US Financial Sector: The Unintended Consequences of Iran's Cybersecurity Strategy", *Journal of Strategic Security*, 10, (2), 2017, pp. 29-44

[31] M. Dunn Cavelty: '*The Routledge Handbook of Security Studies*' (2009. 2009)

[32] M. D. Al-Khaldi: "Research Fairness Initiative opens a new era for equitable and impactful research collaborations", *European journal of public health*, 30, 2020

[33] M. Alsaleh, & Alomar, N.: "Cybersecurity in Saudi Arabia: An overview of threats, regulations, and the role of pub-lic-private partnerships", *Journal of Information Security and Applications*, 47, 2019, pp. 352-60

[34] Y. Chen: "Information security management: compliance challenges and new directions", *Journal of Information Technology Case and Application Research*, 24, 2022, pp. 243 - 49

[35] El-gazzar, and Stendal: "Examining How GDPR Challenges Emerging Technologies", *Journal of Information Policy*, 2020

[36] H. Wang, W. Xiong, G. Wu, and D. Zhu: "Public–private partnership in Public Administration discipline: a literature review", *Public Management Review*, 20, 2018, pp. 293 - 316

[37] H. Younies, and T. N. e. Al-Tawil: "Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)", *Journal of Financial Crime*, 27, 2020, pp. 1089-105

[38] L. Tabansky, and I. B. Israel: 'The National Cyber-Strategy of Israel and the INCB', in Editor (Ed.)^(Eds.): 'Book The National Cyber-Strategy of Israel and the INCB' (2015, edn.), pp.

[39] R. A. Ahmad, and M. S. Hashim: "The Organisation of Islamic Conference — Computer Emergency Response Team(OIC-CERT): Answering cross border cooperation", *2011 Second Worldwide Cybersecurity Summit (WCS)*, 2011, pp. 1-5

[40] T. Riebe, M.-A. Kaufhold, and C. Reuter: "The Impact of Organizational Structure and Technology Use on Collaborative Practices in Computer Emergency Response Teams: An Empirical Study", *Proceedings of the ACM on Human-Computer Interaction*, 5, 2021, pp. 1 - 30