Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

THE EVOLUTION OF NATIONAL CYBERSECURITY STRATEGIES (NCSS): A COMPARATIVE ASSESSMENT OF PROGRESS, OBSTACLES, AND TRENDS

MOHAMMED ATOUM
Department of Computer Science, University of Jordan.

WAHEEB ABU-ULBEH
Faculty of Administrative Sciences and Informatics, Al-Istiqlal University, Jericho, 10, Palestine.

MAMOUN ABU HELOU
Faculty of Administrative Sciences and Informatics, Al-Istiqlal University, Jericho, 10, Palestine.

NASHAT ALREFAI
Department of Mathematics, College of Science, & Basic and Applied Scientific Research Center, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia.

ABDULLAH MAHMMOUD
Faculty of Arts and Educational Sciences, Palestine Technical University-Kadoorie, Tulkarm, Palestine.

HANI IWIDAT
Faculty of Administrative Sciences and Informatics, Al-Istiqlal University, Jericho, 10, Palestine.

YOUSEF A. BAKER EL-EBIARY
Faculty of Informatics and Computing, UniSZA, Malaysia.

Abstract

The rapid global expansion of the Internet has made cybersecurity a critical priority, particularly for Arab nations facing evolving digital threats. Effective National Cybersecurity Strategies (NCSS) are essential to mitigate risks, safeguard institutions, and maintain public trust. This study conducts a comparative analysis of NCSS frameworks across Arab states, evaluating their strategic objectives, preparedness levels, implementation challenges, and capability gaps. Using a descriptive methodology, the paper systematically examines each nation's approach to cybersecurity governance, historical policy development, and current defensive measures. The analysis identifies key areas for regional alignment and proposes a unified strategic vision to strengthen cyber resilience. Findings emphasize the need for coordinated policy upgrades, sustainable implementation roadmaps, and cross-border collaboration to enhance collective security in the Arab world.

Keywords: Cyberspace; Cybersecurity; Cyber-Attack; National Cybersecurity Strategy (NCSS).

1. INTRODUCTION

The world is witnessing rapid advancements in the field of information and communication technology as a result of the widespread use of the internet. The web has become an essential element in all areas of life, which in turn has increased the risks and threats of cyber-attacks. To face current and emerging cybersecurity threats, in light of these ever-changing cyber threats, countries need flexible and dynamic cybersecurity strategies that cover all aspects of life, from schools, hospitals, government and private sectors, and

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

other sectors. Like the countries of the world, the Arab countries need to constantly develop and adapt their cybersecurity strategies. Cybersecurity Strategy outlines the political objectives, measures to be taken, and responsibilities to ensure the protection of networks, the internet, and cyberspace on which modern societies relying on these technologies depend.

These strategies include the confidentiality of exchanges, data integrity, system availability, and protection against technical malfunctions and cyber-attacks, through available priorities to secure the infrastructure for sensitive information via the cybersecurity strategy [1]. National cybersecurity strategies (NCSS) are the main documents for nation states to set strategic principles, guidelines, objectives, and, in some cases, specific measures in order to mitigate the risks associated with cybersecurity and support Arab citizen confidence, Therefore, developing comprehensive national strategies to protect cyberspace is the best way to protect individuals and institutions and thus preserve national security.

The importance of the Study lies in its discussion of existing national cybersecurity strategies in Arab countries, their origins, objectives, readiness, capabilities, and the challenges they face, with comparisons between them highlighting similarities and differences. This leads to formulating a unified Arab cybersecurity strategy that can be applied in reality, thereby enhancing the national security of these countries. This study contributes to the scientific content theoretically by identified as the study's subject is crucial for Arab societies at present and is of interest to many governments and governmental and non-governmental bodies.

It can significantly contribute to the possibility of developing a comprehensive strategy to address many security problems and challenges facing the cybersecurity sector, and practically by emerges in terms of the insufficiency of studies that addressed the topic of Arab cybersecurity strategies due to the novelty of the subject and the requirements for developing these strategies; and utilizing the results of comparisons between countries as a reference for Arab researchers in their future studies, with the potential for governments to benefit from this. The following table shows the group of countries that have organized a national cybersecurity strategy. See Table 1.

Study Problem

This study examines the possibility of establishing a unified Arab cybersecurity strategy for Arab countries. It reviews the experiences of Arab countries in this field, compares them with global experiences, and identifies the obstacles and challenges facing Arab countries as well as their current capabilities. Accordingly, the main problem of the study is to answer the following questions:

- What is the current state of cybersecurity in Arab countries?
- How prepared are Arab countries to develop a comprehensive, unified cybersecurity strategy?
- What challenges do Arab countries face in developing a unified strategy in this field?

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

Study Scope

The scope of the study includes all Arab countries and details of their readiness in the field of cybersecurity.

Table 1: This is a table. Tables should be placed in the main text near to the first time they are cited

AFRICA	AMERICAS	ARAB STATES	Asia-Pacific	CIS	EUROPE
Benin	Argentina	Bahrain	Afghanistan	Armenia	Albania
Botswana	Brazil	Egypt	Australia	Azerbaijan	Austria
Burkina Faso	Canada	Iraq	Bangladesh	Belarus	Belgium
Côte d'Ivoire	Chile	Jordan	Brunei	Kazakhstan	Bulgaria
Eswatini	Colombia	Libya	Darrussalam	Russian	Croatia
Gambia	Costa Rica	Mauritania	China	Federation	Cyprus
Ghana	Cuba	Morocco	Fiji	Uzbekistan	Czech Republic
Kenya	Dominican	Oman	India		Denmark
Malawi	Republic	Qatar	Indonesia		Estonia
Mauritius	Guatemala	Saudi Arabia	Iran		Finland
Mozambique	Jamaica	Syria	Japan		France
Nigeria	Mexico	Tunisia	Korea		Georgia
Rwanda	Panama	United Arab	(Republic of)		Germany
Senegal	Paraguay	Emirates	Malaysia		Greece
Sierra Leone	Peru		Nepal		Hungary
South Africa	Suriname		New Zealand		Iceland
Tanzania	Trinidad and		Philippines		Ireland
Uganda	Tobago		Samoa		Israel
Zambia	United States		Singapore		Italy
	of America		Sri Lanka		Latvia
	Uruguay		Thailand		Lithuania
			Vanuatu		Luxembourg
			Vietnam		Malta
					Moldova
					Monaco
					Montenegro
					Netherlands
					North Macedonia
					Norway
					Poland
					Portugal
					Romania
					Serbia
					Slovakia
					Slovenia
					Spain
					Sweden
					Switzerland
					Turkey
					Ukraine
					United Kingdom

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

1.1. Cybersecurity Strategies

National cybersecurity strategies aim to enhance the resilience of infrastructures and contribute to ensuring, within the digital environment, the protection of citizens, professionals, and public life actors. Various countries have developed their national security strategies by: arranging and implementing minimum requirements to protect their critical infrastructures; securing and protecting government systems; developing national and international cooperation; promoting cybersecurity awareness at the national level; enhancing human resource capabilities; developing national expertise; raising information security awareness; and updating the legal framework to support the safe use of information systems [1]. The significant development in means of transportation, especially the information network, has allowed criminals to move from one country to another. The international community has realized that it is impossible for any single country to eliminate cross-border crimes alone. International cooperation occurs through various mechanisms, including the cooperation of judicial authorities of different countries or through the International Criminal Police Organization "INTERPOL" and the emergence of various forms and means of cooperation among police agencies. At the level of regional agreements and initiatives, the African Union adopted the "Convention on Cyber Security and Personal Data Protection" following the 23rd meeting of heads of state and government of the organization held in Malabo on June 26-27, 2014. This convention, known as the "Malabo Convention," aims to establish a legal framework for cybersecurity and personal data protection. In the Arab region, the Arab Convention on Combating Information Technology Offenses was established on December 21, 2010. It consists of five main chapters, including a chapter on criminalization defining types of cybercrimes, a chapter on procedural provisions, and a chapter on legal and judicial cooperation among Arab countries. Eighteen Arab countries have signed this convention, and seven have ratified it.

1.2. What is the Global Cybersecurity Index (GCI)?

The Global Cybersecurity Index, issued by the International Telecommunication Union (ITU), tracks improvements in cybersecurity awareness and measures taken to protect it across 193 countries. It is based on several components across five main pillars: legal measures (LM), Organisational/regulatory measures (OM), technical measures (TM), capacity-building/development measures (CD), and cooperation measures (CM). These assessments help identify gaps in cybersecurity development within nations and regions, increase awareness about the need for cybersecurity support, and improve global cybersecurity practices. The GCI highlights practices that member states can adopt based on their national environment, encouraging sound practices and fostering a global cybersecurity culture. The GCI helps identify relative strengths and weaknesses in member states' cybersecurity commitments, informing them of areas where additional support may be needed or where they can offer support to others. For example, the GCI can highlight educational needs in cybersecurity within member educational systems [2]. See the 4th edition of GCI as shown in table 2 which exhibits the ranking of Arab countries [3], ITU is compiling a fifth edition which expected to release in the current year [4].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

Table 2: GCI for Arab region; * no data ** no response to the questionnaire/data collected by GCI Team

Country Name	Overall Score	LM	TM	OM	CD	CM	Regional Rank
Saudi Arabia	99.54	20	19.54	20	20	20	1
United Arab Emirates	98.06	20	19.08	18.98	20	20	2
Oman	96.04	20	16.64	20	20	19.41	3
Egypt	95.48	20	17.45	20	19.12	18.91	4
Qatar	94.5	20	16.64	18.46	20	19.41	5
Tunisia	86.23	20	19.54	12.21	16.96	17.52	6
Morocco	82.41	18.4	17.94	12.37	15.24	18.46	7
Bahrain	77.86	20	12.12	15.11	16.77	13.86	8
Kuwait	75.05	17.74	14.25	11.13	16.05	15.9	9
Jordan	70.96	18.53	10.74	15.7	11.47	14.51	10
Sudan	35.03	12.43	13.81	5.41	3.38	0	11
Algeria	33.95	12.46	2.73	1.44	10.07	7.25	12
Lebanon**	30.44	10.24	3.27	5.69	8.26	2.99	13
Libya	28.78	3.73	8.54	3.13	5.34	8.04	14
State of Palestine	25.18	9.02	11.36	2.34	2.46	0	15
Syrian Arab Republic**	22.14	9.8	7.85	4.49	0	0	16
Iraq**	20.71	0	6.75	7.75	2.14	4.26	17
Mauritania	18.94	12.55	0	6.39	0	0	18
Somalia	17.25	0	3.25	6.17	1.52	6.31	19
Comoros**	3.72	0	0	1.69	0	2.04	20
Djibouti	1.73	1.73	0	0	0	0	21
Yemen*	0	0	0	0	0	0	22

As the level of preparation and development of national cybersecurity strategies evolves, concerns about regional coordination between these countries arise from time to time. In Europe, for example, all member states have completed the process of developing their cybersecurity strategies since 2017, and since then the European Union Agency for Cybersecurity (ENISA) has been continuously involved in guiding member states to improve the maturity of these strategies [5,6]. The Organization of American States (OAS) is also making efforts to develop these countries' strategies [7]. This was also adopted in 2021 by members of the Economic Community of West African States (ECOWAS) Parliament, known as the Regional Strategy for Cybersecurity and Combating Cybercrime in the Community [8]. In the same year, the Association of Southeast Asian Nations (ASEAN) developed a cybersecurity cooperation strategy with the aim of facilitating coordination and information exchange between member states [9]. These efforts confirm the importance of having a unified platform for cybersecurity in the Arab region, where the internet penetration rate exceeds 90%, as many Arab countries have realized that cybersecurity is an integral part of their economic systems. According to the Global Cybersecurity Index of the International Telecommunication Union (ITU), as shown in Table 2, Saudi Arabia, the UAE, Oman, Egypt, and Qatar were ranked among the top 20 countries in the world, in addition to other Arab countries that ranked higher than many Arab countries.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

2. STUDY METHODS

The research team adopted a descriptive analytical approach for this study by studying and analysing texts related to the cybersecurity strategies of individual Arab countries, as found in their legislative texts and international agreements they participate in. The following in the result section are details of the national cybersecurity strategies of Arab countries based on the documents and references that were searched and obtained. This paper presents in details the efforts of Arab countries in the field of cybersecurity.

3. RESULTS

3.1. Mauritania

In March 2022, the Ministry of Digital Transformation, Innovation, and Modernization of Administration presented the digital identity project and approved the national cybersecurity strategy (2022 to 2025).

Mauritanian citizens will be able to securely access electronic/digital services provided by government entities, enabling digital signing of documents and transactions, among other electronic services.

Mauritania's National Cybersecurity Strategy 2019-2022 begins with a list of abbreviations, and the executive summary states that technological progress is taking a big step forward in Mauritania, being significantly introduced into all sectors and forms of citizens' lives, making the protection of ICT infrastructure and all data owned by the government, public and private companies, and citizens critically important. Significant efforts are needed to ensure digital trust and keep pace with this digital transformation in Mauritania.

Considering that the Mauritanian state has decided to develop its cybersecurity strategy and adopt a national action plan to achieve set goals, the objectives outlined in this new strategy aim to secure national critical infrastructure, particularly electronic services under development, provide institutions with protection means, enhance cybersecurity, develop skills, update the legal framework, and raise user awareness.

This strategy aims to provide various stakeholders with the means to protect themselves from constantly evolving threats that may jeopardize the entire development process. These threats include potential attacks on institutions or critical infrastructure, malware attacks, attacks on citizen data, and banking fraud.

To counter these threats and achieve the specified objectives, five lines of action have been identified; all government efforts and those of various stakeholders will focus on these strategic directions until 2022.

The strategy also calls for the establishment of a high-level administrative body responsible for validating and approving action plans, a National Cybersecurity Agency, and a Computer Emergency Response Team (CERT), without forgetting other operational entities implicitly involved in the national efforts [10].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

3.2. Sudan

Not far from Mauritania, Sudan does not have a national cybersecurity strategy. The National Information Security Centre, under the National Information Centre, organized a workshop aimed at discussing the development and formulation of a national cybersecurity strategy under the slogan "National Participation. Strong Shield." This initiative followed the removal of Sudan from the list of state sponsors of terrorism, which had posed a significant challenge in advancing information technology. Currently, efforts are underway to build this strategy, as Sudan faces challenges in the field of information security, which is a crucial part of national security. The National Information Centre in Sudan is collaborating with all relevant parties to establish this strategy, following significant efforts by the Ministry of Trade and Infrastructure in creating and developing the single window system in cooperation with partners in both civilian and military governance. This collaboration aims to ensure information security, combat piracy, protect information, and consequently, enhance Sudan's national security [11].

3.3. Tunisia

Following the deliberations of the National Security Council on 5/7/2018, a working group was established under the Information and Communications Security Committee emanating from the National Security Council to prepare the National Cybersecurity Strategy 2020-2025 of the National Security Council in the Presidency of the Republic, which aims to protect and develop the national cyberspace by building national capacities and ensuring digital trust.

This strategy focused on five areas: sectoral strategic directions (with the commitment of the stakeholders to strengthen the immunity of the national cyberspace and protect sensitive information infrastructure against risks and threats to national security), the legal and regulatory framework (developing legal texts with the development in the digital field such as freedom of expression on the Internet, protecting privacy and personal data, protecting children on the Internet, protecting the "digital" consumer, protecting intellectual and industrial property and patents on the Internet, protecting financial transactions on the Internet, and combating cybercrimes), and education, training and skills (by raising awareness of individuals about cyber risks and how to confront them, establishing academic training in the digital field in partnership with the industrial sector, and developing specialized competencies in the field of cyberspace safety Cyber), cyber culture and society, standards, technologies and scientific research (good preparedness for potential threats based on international standards, and motivating various stakeholders to develop the necessary capabilities and solutions for the purpose).

This strategy presented the vision and objectives, which are for the state to be able to protect itself and withstand cyber threats based on national capabilities, lead and manage the national cyberspace, support digital trust, enhance international cooperation, and achieve leadership in the digital field. It also presented the priorities for implementing these areas.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

The scope of the strategy covers the national cyberspace, which consists in particular of all services, data, networks, platforms, information systems, and vital digital structures related to the interests of the state, as well as all stakeholders from citizens, institutions, associations, and companies in the public and private sectors, civil society, academia, and research, and noted the importance of follow-up and periodic evaluation by the Communications and Information Security Committee emanating from the National Security Council. Finally, a set of conceptual terms was presented in Arabic, English, and French with their definitions in Arabic [12].

3.4. Morocco

Developing a cybersecurity strategy is an important element in the country's national and economic security strategy. National cybersecurity strategies have become more important for any country. The Moroccan cybersecurity strategy aims to assess risks to prevent cyber threats and protect information systems and infrastructures. As for the risk assessment axis, two basic programs have been identified for its implementation: First: Develop plans to assess risks and threats by defining a network to assess the degree of importance of information systems for public administrations, institutions, and vital infrastructures, to count, define, and classify these systems, and to conduct a periodic assessment of the level of risk they may be exposed to, as well as assess the risk management plans adopted by these administrations, public institutions, and vital infrastructures. Second: Develop the necessary tools to assist in decision-making by conducting investigations to collect data of a legal, technical, and procedural nature related to information systems, as well as producing statistical data and monitoring indicators, then ensuring technological, legal, and regulatory monitoring. As for the second axis, which is protecting the security of information systems and infrastructures, it is done through three programs centred around: preparing national references and standards for information systems, ensuring the security of the information system for public administrations and bodies and vital infrastructures, and strengthening structures for vigilance, detection, and response to information security incidents. The strategy explained the mechanisms for implementing the Moroccan cybersecurity strategy can be implemented through: first: strengthening national capacities in the field of cybersecurity (legal framework, organizing training programs related to the technical and legal issues raised by cybersecurity, awareness-raising "by identifying and implementing programs on cyber ethics and challenges related to cybersecurity threats and risks for the benefit of users of vitally important bodies and infrastructures, the private sector and individuals, especially children, supporting research and development in the field of information systems security), and second: national and international cooperation [13].

3.5. Algeria

Algeria does not have a national strategy yet and it is in its final stages [14]. Before that; the ministry of National Defence of Algeria Opening ceremony of the National Forum on Cybersecurity, entitled "National Cybersecurity Strategy: For a Cyber-Resilient Algeria" [15].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

First, at the national level: Algeria has included cybersecurity as one of the priorities in the program to confront cybercrime and cyberterrorism, and it has even become an integral part of defence strategies. The lessons learned from countries with experience in this field have proven that the effectiveness of implementation and the effectiveness of the standards and means used cannot be realized unless there is careful planning and coordination between the actors in the field. Accordingly, Algeria has moved to draw up its strategy, focusing on the following points: identifying risks, taking the necessary measures, identifying the bodies responsible for managing security, identifying the bodies responsible for coordination, identifying the body responsible for the technical aspect to search for loopholes and direct the investigation, so that the goal remains in increasing cybersecurity capabilities to protect information systems and enhance preventive confrontation methods, awareness (and deterrent confrontation), and prosecuting criminals. From a legal perspective, domestic legislation has been made consistent with international legislation, especially the international agreement concluded in the Hungarian capital Budapest on 23.11.2001 (including cybercrimes), and this agreement is considered the legal reference for all international legislation issued in this field. From an administrative perspective, the Algerian project has been keen to establish controls of respect in the administrative framework regulating the powers of civil, military, and technical bodies. In managing the Algerian strategy for cybersecurity by establishing the National Authority for the Prevention and Combating of Crimes Related to Global and Communication Technologies, given the sensitivity of the national defence sector: On 11.06.2015, at the level of the Department of Use and Preparation of the National People's Army Staff, the "Cyber Defence and Systems Security Monitoring Service" was created. Technically: By obtaining the best technological means, relying on competencies and the best protection methods, it is considered a solid link to avoid loopholes and resist breaches. To achieve this mission, it has become necessary for the authorities to invest in the technical aspect and encourage initiatives aimed at developing security and protection policies for the information infrastructure, especially if we know that we are on the threshold of embodying the e-government project, which has become a demand for citizens to improve services. Scientifically: By organizing training courses and providing all material and human resources, Algeria has also called on international experts to enable active cadres in the field to all best practices in security technology and general policies for electronic business in effect abroad. Missions have also been sent to attend and participate in international conferences to benefit from the expertise aimed at issuing appropriate recommendations for security and information safety in cyberspace [16].

3.6. Egypt

Cybersecurity is an essential part of the economy and national security system, and the state is committed to taking the necessary measures to preserve it in the manner regulated by law as stated in Article 31 of the Egyptian Constitution in January 2014. The strategy includes a number of programs that support the strategic objectives of cybersecurity, and it also clarifies the distribution of roles between government agencies, the private sector, business institutions, and civil society and the measures that the state will take to advance towards achieving these objectives. The strategy also presented the

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

features of an action plan that extended over the years 2017-2021 according to the objectives, while emphasizing the importance of community partnership between government agencies, the private sector, business institutions, and civil society to implement these objectives and related procedures in a way that supports the transition towards an integrated digital economy that achieves citizens' aspirations for comprehensive social and economic development and protects their interests, preserves the supreme interests of the state, and contributes to its renaissance, prosperity, and prosperity. The most important of these cyber challenges and dangers are: the risk of hacking and sabotage of communications and information technology infrastructure; the risk of terrorism and cyber warfare; and the risk of stealing digital identity and private data. The most important targeted vital sectors are: the communications and information technology sector, the financial services sector, the energy sector, the government services sector, the transportation sector, the health sector and emergency ambulance services, and the science and culture sector, in addition to the official websites of the state and sectors that have an impact on economic activity such as investment, tourism, trade, industry, agriculture, irrigation, and education at various levels. The seriousness of cyber threats is due to 3 main elements: their reliance on advanced and sophisticated technologies, the speed and ease of their spread, and the wide scope of their impact. The key pillars for preparedness to confront cyber threats are: political, strategic, and executive support; legislative framework; regulatory and executive framework; scientific research, development, and cybersecurity industry development; human resources development; international cooperation; community awareness: developing and implementing plans; and implementation mechanism. The Supreme Council for Securing Communication and Information Technology Infrastructure (Supreme Cybersecurity Council) was established by the Ministry of Communications and Information Technology. The council is chaired by the Minister of Communications and Information Technology and includes stakeholders in national security and the management and operation of vital infrastructure and public utilities, along with experts from the private sector and research and educational institutions. The council is responsible for developing a national cybersecurity strategy and overseeing its implementation, with necessary updates in line with technological advancements [17].

3.7. Kuwait

In 2017, the Kuwait Cybersecurity Strategy was outlined, and the National Cybersecurity Centre will be established after the end of the period 2017 to 2020. [18] by Amiri Decree, the National Cybersecurity Centre was established on February 5, 2022, to be chaired by the Minister of Interior, and the Supreme National Committee will be established, which is a committee established by Cabinet Resolution No. 355 in its meeting 2019/11 dated 2019/3/18, and its chairman will be the Chairman of the Centre. The committee will establish the National Cybersecurity Strategy. The concerned parties are the civil, military and security government agencies and private sector institutions within the State of Kuwait related to the Centre’s competencies, and other parties determined by the Chairman of the Centre. The centre aims to achieve the objectives emanating from the strategy, especially the following: Building an effective cybersecurity system at the

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

national level, developing and organizing it to protect the state from cybercrime threats and confront them efficiently and effectively in a way that ensures the sustainability of work and maintains national cybersecurity. Protecting vital interests in cyberspace, and supervising the building of national capabilities specialized in the field of cybersecurity. Promoting a cybersecurity culture that supports the safe and correct use of cyberspace. Protecting and monitoring vital assets and infrastructure, national information and the information network in the State of Kuwait. Providing means of cooperation, coordination and exchange of information among various local and international entities in the field of cybersecurity. Developing and implementing cybersecurity operations and providing the necessary support and advice to build cybersecurity operations teams and coordinate response efforts and intervene when needed.

Developing the regulatory framework and governance mechanisms to implement the strategy. Preparing, classifying and identifying the cybersecurity infrastructure and related entities, identifying sectors and entities related to cybersecurity, defining cybersecurity standards and controls, classifying cybersecurity incidents, and creating a database of electronic threats with the participation of relevant entities. Evaluating and developing the security aspects of e-government services, evaluating and developing cybersecurity incident response teams and issuing instructions to relevant entities, conducting cybersecurity training and competitions, regulating the work of companies, experts, consultants and others who provide cybersecurity services, granting licenses and preparing a register in which those who meet security standards are registered. In addition to developing the necessary programs to build national capabilities and expertise in the field of cybersecurity and enhance awareness at the national level, and setting the technical terms and specifications for any devices or systems related to the field of cybersecurity, and approving their use, import or circulation in the country, and issuing circulars and instructions regulating the protection of devices, programs, networks and accounts room sites from the risks of interference, breaches and access to information by those not authorized to access it. Setting the terms and job standards for filling cybersecurity positions in the relevant authorities.

Conducting technical security checks, and auditing the systems and networks of the relevant authorities to ensure their compliance with the standards and policies issued by the centre. Technical intervention if necessary to address cybersecurity incidents to which the networks and relevant authorities are exposed. Setting the necessary controls to prevent any attempts to obstruct, disrupt or sabotage communications networks and information systems in the country, and taking the necessary measures to deal with all electronic threats, whether from within or outside the country. Monitoring and observing electronic threats to the networks of the concerned parties, conducting the necessary investigations into them, and isolating them if necessary in the event of non-compliance with cybersecurity standards in order to ensure addressing any threats that may harm the national security system, the state's economy, or its international and regional relations. Providing technical support and advice to the concerned parties, through evidence, and supporting the investigation of crimes related to cybersecurity. Expressing technical opinions on issues related to cybersecurity, coordinating and cooperating with the

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

concerned parties to work in accordance with the provisions of the National Cybersecurity Governance Framework. Preparing and supporting the studies, programs, and scientific research necessary to develop the cybersecurity system in the country in coordination with local and international academic and professional institutions, following up on the implementation of obligations arising from international agreements in the field of cybersecurity, and decisions issued by international and regional organizations to which the state is a party, in coordination with the concerned parties. Studying legislation related to cybersecurity, and proposing amendments thereto, in coordination with the concerned parties. Preparing periodic and annual reports on the implementation of the strategy, and on the work of the centre, and submitting them to the Council of Ministers. Preparing periodic reports on cybersecurity issues of a national dimension and submitting them to the Council of Ministers to take the necessary action [19].

3.8. Syria

The national information security policy in the Syrian Arab Republic, under the Ministry of Communications and Technology and the National Network Services Authority, began with technical definitions. Which outlined the objectives as Identifying the basic requirements for information security and what needs to be done to protect informational assets in government entities, providing a secure environment for delivering and developing electronic services, defining tasks and responsibilities for implementing this policy in government entities, and providing a national reference for all aspects related to information security. The purpose is to secure a national reference for information security policies at government entities to ensure the protection of data (stored or transmitted) and electronic services, covering software, equipment, communication networks, individuals, and their locations. It includes fourteen areas: information security policies, information security organization, human resources security, contractor security, awareness, management of informational assets and environment, physical security, access management, and design, development, and testing of information systems [20]. In 2021, the Information Security centre conducted Regular security surveys, professional security surveys, penetration testing, information emergency response, and security awareness (including implementing various activities, providing security consultations to public entities regarding security vulnerabilities and general information security issues, issuing warnings about malware, cyberattacks, and serious vulnerabilities threatening the Syrian network). The Ministry of Communications and Technology and the National Network Services Authority are currently preparing the national cybersecurity strategy for Syria in collaboration with relevant entities, requiring an assessment of the information security status across all sectors [21].

3.9. Iraq

On February 16, 2022, the Iraqi National Security Council approved the Cybersecurity Strategy for 2022-2025. This strategy defines a clear purpose and a consistent direction for a secure, reliable, vibrant, resilient, and trustworthy community that provides opportunities for its citizens, protects national assets and interests, and promotes peaceful interactions and proactive engagement in cyberspace for national prosperity.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

The goal of this strategy is to provide a cohesive roadmap with initiatives and mechanisms for implementation to achieve the national vision for cybersecurity. In the context of national security, cybersecurity involves protecting critical information infrastructure and other crucial elements of the information system.

The current situation poses a significant national challenge, necessitating a cohesive cybersecurity framework to provide a comprehensive approach to the current and future security landscape. The security of the state and economy is rapidly evolving, moving towards digital and shifting terrains. Governmental and non-governmental actors involved in cybercrime are equipped with advanced electronic tools that cause unprecedented damage.

Incorporating cybersecurity into the cyber domain will help the country prepare for and respond to these security threats, address vulnerabilities in the digital sphere, and enhance Iraq’s capability to implement countermeasures alongside legitimate and non-governmental actors. This forms the strategic rationale for establishing the national cybersecurity policy and the context for defining Iraq's cybersecurity strategy to advance national security. The national cyber threat landscape in Iraq comprises two main components: cyber threats and national vulnerabilities.

The critical success factor for the strategy is comprehensive mobilization, engagement, and coordination of critical components to ensure a presence in cyberspace and protect vital information infrastructures. The strategy aims to establish a national roadmap with coordinated mechanisms, an executive framework, and actions to achieve the national vision and objectives related to cybersecurity. Therefore, the strategy is essential for achieving the following specified goals:

- Legislative Framework: Developing comprehensive legislation to combat cybercrime and counter-cyber threats at the national, regional, and global levels relevant to securing the country's cyberspace.
- Emergency Response: Establishing an effective mechanism for computer emergency response.
- Improvement of CERT: Enhancing the capability and development of the Iraqi Computer Emergency Response Team (CERT).
- Capacity Building and Awareness: National mechanisms for building capacity, public awareness, and skill development.
- Stakeholder Engagement: Establishing a reliable mechanism for involving multiple national and international stakeholders to collectively address cyber threats.
- Government Protection: Deterring and protecting the government from all forms of cyberattacks.
- Coordination: Coordinating cybersecurity initiatives across all governmental levels in the country [22,23].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

3.10. Lebanon

On September 26, 2018, a National Cybersecurity Coordinator was appointed by the Prime Minister, followed by the establishment of a National Committee tasked with developing a Lebanese national cybersecurity strategy. The reasons for this initiative included: lack of a unified national cybersecurity strategy, absence of laws and regulations governing cybercrime, lack of a national cybersecurity agency need to combat corruption in the digital economy, complex socio-demographic context in Lebanon, insufficient cooperation among various national departments, lack of effective private sector involvement in advancing the public sector, no high-level initiative to establish a national information system and digital transformation strategy, and the shortage of cybersecurity experts and difficulty adapting to rapid changes.

The strategy categorizes threats into: cyber-dependent crimes, crimes enabled by cyber means, state-sponsored threats, terrorist threats, threats from cyber activists, internal threats, threats from novice hackers, and attacks on social networks. It also outlines the trends in cyber threats and the challenges faced, particularly the need to develop a modern legal framework and enhance the operational capabilities of law enforcement agencies, including the military, internal security, public security, and state security. The only solution to address all cyber threats and attacks is to establish a state-level system that can coordinate a unified response within a legal and technical framework. Securing the national cyberspace requires a collective and multidimensional effort (both human and technical), involving all actors in Lebanese society. The main stakeholders in cybersecurity are: the government, companies and organizations, and individuals (as citizens, employees, and consumers). The cybersecurity strategy should be based on the following pillars, referred to as the national strategy pillars:

- Defence and Deterrence: Addressing threats from both internal and external sources.
- International Cooperation: Developing international cooperation in cybersecurity.
- Development of IT Capabilities: Continued development of the state’s capabilities to support IT and communications technology.
- Educational Capacity: Enhancing educational capacities within Lebanon.
- Industrial and Technical Capability: Strengthening industrial and technical capabilities.
- Export and Internationalization: Supporting the export and internationalization of cybersecurity companies.
- Public-Private Cooperation: Enhancing cooperation between the public and private sectors.
- Security Agencies: Strengthening the role of security and intelligence agencies and improving coordination and collaboration under high-level supervision.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

A strong, cohesive, comprehensive, institutional, and collaborative national cybersecurity strategy based on defined cybersecurity pillars is the only way to protect Lebanon, its public institutions, private sector, and citizens from the aforementioned threats. This requires a well-structured national action plan. The strategy concludes with a glossary of terms and definitions [24].

3.11. Bahrain

The National Cybersecurity Centre was established by Decree No. (65) of 2020 issued by His Majesty King Hamad bin Isa Al Khalifa, which reorganized the Ministry of Interior and established the National Cybersecurity Centre. The centre is responsible for formulating a comprehensive strategy in the cyber domain and setting effective governance standards for its implementation as a means of defence and monitoring against cyberattacks and breaches, as well as raising awareness among individuals and institutions to achieve the Economic Vision 2030 and contribute to the Sustainable Development Goals.

The strategy aims to provide a secure and reliable cyber space in the Kingdom of Bahrain. It is built on an ambitious vision with several core objectives to address cybersecurity requirements at the national level. The strategy encompasses all critical sectors as well as individuals and extends to enhancing regional and international partnerships. Five foundational pillars were identified in this strategy, each essential for achieving the kingdom's vision in cybersecurity. The needs, goals, and responsibilities of critical sectors were taken into account during the development of the national strategy to create a comprehensive plan to improve Bahrain's cybersecurity over four years. Core Pillars of Cybersecurity: The national cybersecurity strategy is based on five interconnected pillars designed to achieve a cyber-secure Kingdom. Each pillar addresses a crucial aspect of cybersecurity, collectively forming a comprehensive and coherent framework for maintaining a secure and reliable cyber space in Bahrain:

- Pillar 1: Strong and Resilient Cyber Protection
- Pillar 2: Effective Cybersecurity Governance and Standards
- Pillar 3: Building a Cybersecurity Aware Community
- Pillar 4: Enhancing Protection Through Partnerships and Cooperation
- Pillar 5: Developing National Talent

And regarding sector-specific strategies which including Six strategies were developed to support the national cybersecurity strategy, focusing on the goals and requirements of critical sectors. Below is a brief overview of each strategy:

- Financial Sector Strategy: Aims to protect financial systems and implement cybersecurity requirements to enable the sector to carry out banking and digital economy initiatives.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

- Government Sector Strategy: Focuses on enhancing the protection of government systems and networks, establishing procedures to counter cyber threats, and developing secure and reliable electronic government systems and services.
- Health Sector Strategy: Concerned with maintaining the security and privacy of health information and data, and enhancing the protection of health systems, including operational technologies and the Internet of Things.
- Information and Communications Technology Sector Strategy**:** Aims to enhance secure handling of information and communication technologies and networks, including advanced systems like 5G networks.
- Transport Sector Strategy: Highlights the importance of implementing a security program to manage cyber risks to various transportation systems and supply chains, and fosters international cooperation in cybersecurity within this sector.
- Gas, Energy, Oil, and Basic Industries Sector Strategy: Combines these sectors into one strategy due to their reliance on information technologies and operational technologies, enhancing protection for operational systems used in factories and refineries [25].

3.12. Qatar

In 2013, Qatar developed its National Cybersecurity Strategy and established the National Information Security Committee to provide a governance structure for addressing cybersecurity collaboratively at the highest levels of government. The committee developed the National Cybersecurity Strategy (NCSS), which outlines a roadmap to improve cybersecurity in Qatar. The NCSS combines good governance with a range of cybersecurity initiatives, measures, and awareness programs that will lead to effective long-term protection. Qatar's vision is to create and maintain a secure cyber space to protect national interests and uphold the fundamental rights and values of the community.

The vision supports five goals that determine where actions will be taken to benefit and improve cybersecurity in Qatar includes; protecting Critical National Information Infrastructure, responding to and managing cyber incidents and attacks through information sharing, collaboration, and timely action, creating a legal and regulatory framework for a secure and vital cyber space, promoting a cybersecurity culture that encourages safe and proper use of cyberspace, and developing and refining national cybersecurity capabilities.

Qatar's approach to cybersecurity is based on three guiding principles: The government will lead efforts to safeguard government systems and networks by implementing cybersecurity requirements while designing and adopting innovative and modern technologies; Cybersecurity is a shared responsibility among all government agencies, businesses, institutions and individuals; and Qatar will pursue cybersecurity policies and initiatives that preserve the fundamental rights and values of society, in accordance with applicable laws and regulations.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

As new, complex and global cybersecurity challenges emerge, Qatar's reliance on information and communications technology (ICT) is increasing. It is imperative for Qatar to remain vigilant and work to enhance the readiness and resilience of its cyberspace, which is reflected in this strategy.

The strategy has identified the threats as the greatest threat to cybersecurity and categorized them into: hacktivists, advanced persistent threats (APTs), malicious actors and other threats.

She mentioned a set of challenges that affect Qatar's ability to innovate and compete at the global economic level in the field of harnessing information and communications technology in the field of cybersecurity, including: a shortage of skills and services in the field of cybersecurity, a shortage of skills and services, risks of the global supply chain, linking industrial control systems, placing restrictions on the circulation of information, awareness of executive leadership, and changing expectations regarding privacy.

The Qatari government has taken a set of preventive measures in the field of infrastructure, banks, the government sector, energy networks, the transportation sector, and others. Implementation Approach:

The successful execution of the NCSS requires commitment, governance, and continuous work by various stakeholders who share the responsibility for adhering to the national approach to cybersecurity.

Qatar will review the NCSS every four years or as necessary to make coordinated updates to reflect legal, operational, and technological developments at the national and international levels. This review will aim to align Qatar's cybersecurity vision with new national strategic documents (such as development strategies) and gather stakeholder input as needed [26].

3.13. United Arab Emirates

The United Arab Emirates has undertaken significant steps to enhance its cybersecurity practices, including the adoption of the "National Cybersecurity Strategy." This strategy aims to create a secure and resilient cyber environment that helps individuals achieve their ambitions, enables businesses to grow in a safe and prosperous environment, and supports national cybersecurity standards through various mechanisms and pillars.

The updated version of the strategy was launched in 2019 by the Telecommunications and Digital Government Regulatory Authority, which oversees telecommunications and information technology in the UAE.

The strategy aims to support cybersecurity standards through various mechanisms and pillars, encourage the establishment of local start-ups in the sector, and develop the cybersecurity environment.

It was developed based on the analysis of over 50 sources of indicators and global publications, working with global experts, and benchmarking against 10 leading countries in cybersecurity systems.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

The strategy encompasses a comprehensive cybersecurity system and is based on five pillars (Cybersecurity Laws and Regulations, Integrated and Dynamic Cybersecurity Environment, National Cyber Incident Response Plan, Protection of Critical Information Infrastructure, and Partnerships) and 60 initiatives:

- Pillar 1: Addressing all types of cybercrime, protecting current and emerging technologies, enhancing protection for small and medium-sized enterprises.
- Pillar 2: Supporting start-ups and enhancing research and development, developing capabilities, increasing individual awareness, and encouraging excellence.
- Pillar 3: A unified reporting mechanism for cyber incidents, a standardized risk assessment model, and an incident response plan with information sharing among entities.
- Pillar 4: Identifying critical assets in the country, establishing global risk management standards, and creating effective reporting, compliance, and response processes.
- Pillar 5: Collaboration between the government sector, private sector, academic institutions, associations, and international organizations.

The vision is to create a secure and resilient cyber environment in the UAE that empowers individuals and enables business growth. The strategy aims to enhance community confidence in participating safely in the digital world, enable small businesses to protect themselves from cyberattacks, build a world-class human resource in cybersecurity, establish a culture of cybersecurity investment, foster innovation in cybersecurity, and protect sensitive information and national infrastructure. To optimally implement the strategy, the UAE has activated national working groups through nine sectoral committees for critical infrastructure protection: Energy, ICT, Government, Electricity and Water, Financial and Insurance, Emergency Services, Healthcare, Transport, Food and Agriculture, as well as two teams for the national cyber incident response plan: the National Cybersecurity Response Committee (NRC) and the Cyber Intelligence Unit (CIU). The Telecommunications and Digital Government Regulatory Authority monitors the progress and impact of the national cybersecurity strategy through 20 specific performance indicators.

The UAE has enacted advanced laws and regulations to combat cybercrime, including the new Information Technology Crimes Law of 2021. In this context, the announcement of the establishment of the Cybersecurity Council in November 2020 aimed to develop policies and legislation to enhance cybersecurity in the country and improve readiness across all sectors to respond to cyber threats. In March 2022, the council signed a memorandum of understanding with Deloitte to organize cooperation frameworks between the two parties and build capabilities both within the UAE and regionally and globally, contributing effectively to international efforts to combat and address cyber threats [27].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

The Cabinet approved the establishment of the Cybersecurity Council, chaired by the Chief Cybersecurity Officer of the UAE Government and reporting to the Cabinet, including representatives from federal and local entities, with the goal of developing and strengthening the national cybersecurity strategy across all critical sectors [28].

3.14. Saudi Arabia

The National Cybersecurity Authority has developed the National Cybersecurity Strategy in accordance with its defined responsibilities outlined in Regulation No. 6801 dated 11/2/1439, which mandated the Authority to prepare a National Cybersecurity Strategy 2020. The vision is to create a secure and reliable Saudi cyberspace that enables growth and prosperity. The strategy encompasses the entire cyberspace, addressing the Kingdom's needs and priorities, emphasizing the protection and resilience of technical systems, operational systems, and critical infrastructure, and enhancing national trust. The Authority aims through this strategy to achieve six main objectives to establish a comprehensive cybersecurity system in the Kingdom, covering the following areas: Integration (comprehensive cybersecurity governance at the national level), Organization (effective management of cybersecurity risks at the national level), Assurance (protection of cyberspace), Defence (enhancing national technical capabilities to defend against cybersecurity threats), Cooperation (enhancing partnerships and cooperation in cybersecurity), and Building (developing national human capabilities and advancing the cybersecurity industry in the Kingdom). This plan will be implemented over five years through three main parallel tracks, which include fourteen initiatives through 70 projects, as follows:

- Track One: High Return Projects.
- Track Two: National Entities Program.
- Track Three: National Initiatives.

To measure the effectiveness of the National Strategy in achieving its goals, a number of key performance indicators have been identified to assess the level of progress for each of the stated objectives. These key performance indicators will be calculated through a set of sub-indicators. Key performance indicators include: risk reduction, trust enhancement, and growth enablement within 5 years. (National Cybersecurity Authority [30].

3.15. Oman

The National Centre for Cybersecurity is one of Oman's digital initiatives and the focal point for security incidents in the Sultanate of Oman. Established in April 2010, it aims to provide a secure informational environment for users of both government and private sector sites. It works to build trust in using government services, develop information security strategies and policies for the benefit of both government and private sectors, and provide initial technical advice and reports to help network, system, and application administrators in both public and private sectors avoid exposing their sites to security risks.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

Given the increasing and evolving threats, information security topics are of significant importance. The National Centre for Cybersecurity was created to serve all users of information technology platforms, whether they are from government institutions, private entities, or individuals. The vision is to equip the Sultanate of Oman with world-class information security capabilities, ensuring that every computer user in the Sultanate feels secure and safe. Whereas the mission is to train national personnel in computer and internet fields to increase the ability to detect and respond to security incidents, analyse risks and security threats in the Omani internet space, and build and enhance security awareness in the computer and internet fields among public and private sector institutions, as well as citizens and residents of the Sultanate. The Centre aims to achieve the objectives; to provide a secure informational environment for using government e-services for every Omani citizen and resident, encourage individuals trained at the centre to work in the information security sector in any entity or institution in the sultanate, respond to security incidents and try to mitigate their effects, raise awareness about the importance of information security among the Omani community, act as a trusted contact centre for reporting any security incidents related to information and communication technologies, build trust in the use of government e-services, build security awareness in the Omani internet space, develop security capabilities to handle security incidents related to computers and the internet, provide accurate and up-to-date information on security threats and current or emerging vulnerabilities, analyse potential security threats and their impacts, provide proactive measures to reduce security incidents, respond to security incidents and mitigate their effects, encourage research and development in the field of information security. Coordinate with, and computer emergency response centres at the regional and international levels. The Centre also provides several services, such as; training Omani personnel specialized in this field, monitoring live sites to detect any potential threats, offering courses, workshops, and training sessions for all targeted individuals, proactive and reactive response to any issues directly, and protecting and addressing any system issues by providing guidance. The centre Values are:

- Trust: Gaining and maintaining user trust to be the contact centre for reporting any security incidents related to information and communication security within the Sultanate of Oman.
- Participation: Seeking to involve all service beneficiaries to achieve our mission.
- Relations: Establishing strong and beneficial relationships at both the local and international levels.
- Excellence: Adopting quality and excellence standards that align with global best practices.
- Results: Providing measurable results and working to enhance our services in accordance with the best global applications.

It is worth noting that the services provided by the Centre are available to individuals, the public and private sectors, and sensitive national infrastructures in the country [31].

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

3.16. Yemen

Yemen does not have a national strategy yet and it is in the maturity stage, the strategy project is part of the outcomes of the First National Cybersecurity Conference held in 2021 under the theme "Towards a National Cybersecurity Strategy." A joint committee of specialists from relevant entities was formed to prepare the strategy project, guided by best practices from Arab and international standards. (Meeting at the Ministry of Communications Discusses the National Cybersecurity Strategy Project – Public Telecommunications Corporation [32]. Under the theme "Towards a National Cybersecurity Strategy," the Ministry of Communications and Information Technology held the First National Cybersecurity Conference in Yemen, in collaboration with several relevant government entities (Presidency of the Republic, Ministry of Defence, Ministry of Interior, Security and Intelligence Agency, Public Telecommunications Corporation, Yemen International Telecommunications Company – TeleYemen) and a number of cybersecurity experts and academics. The conference, which took place from June 7 to 9, 2021, in the capital Sana'a, involved many government entities across various sectors, several public and private universities, civil society organizations, as well as telecommunications and information technology companies, mobile network operators, experts, and cybersecurity enthusiasts. The aim was to understand the state of cybersecurity in Yemen, the challenges it faces, plans for its advancement, and to draft a National Cybersecurity Strategy.

The conference goals were:

- Strengthen the role of the Ministry of Communications and Information Technology and related entities in the field of cybersecurity.
- Identify areas of collaboration between ministries, government institutions, and the private sector to handle cybersecurity incidents.
- Enhance preparedness and readiness to address various electronic risks and threats that may affect the Republic’s information system and the best methods to handle potential security incidents.
- Develop a plan to train national personnel in emergency management and dealing with cybersecurity threats.
- Promote secure use of information technology tools and raise awareness among the Yemeni community about the procedures and measures to handle cybersecurity risks and threats. (First National Cybersecurity Conference [33].

Scientific papers discussed included: evaluating Yemen's cybersecurity status, requirements for a national cybersecurity strategy plan, legal and legislative measures to combat cybercrime, cybersecurity challenges in Yemen, and technical procedures for protecting information security in the national telecommunications network.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

3.17. Jordan

The National Strategy for Information Security and Cybersecurity, which was in effect from 2012 to 2017, identified the urgent need to develop a new strategy covering the next five years. Consequently, the National Cybersecurity Strategy 2018-2023 was prepared. In 2019, Jordan enacted Cybersecurity Law No. 16, defining relevant terms and establishing the National Cybersecurity Council. This council, consisting of ten members, is responsible for approving strategies, policies, and standards related to cybersecurity. Its aim is to build, develop, and protect an effective national cybersecurity system, among other tasks [34]. The National Cybersecurity Strategy 2018-2023 outlines the roles assigned to the government to achieve its vision. This strategy will be in effect until 2023 and will review the progress made toward the goals set in 2012 for information security and cybersecurity. The National Cybersecurity Program was established to focus on achieving strategic goals and national priorities as outlined in the National Information Security and Cybersecurity Strategy 2012. Its implementation has led to the following achievements:

- Completion of a critical network risk assessment program, leading to the establishment of information security standards and necessary policies.
- Formation of national cybersecurity incident response teams and implementation of a cybersecurity training program.
- Creation of public key infrastructure for secure information exchange, identity verification, and electronic signatures; initiation of an international cooperation program in information security.

The implementation of the 2012 strategy faced several challenges, including the need for a suitable legal and regulatory framework due to the complexities in the field and the international dimension of potential threats. The government acknowledges the rapid advancements in the internet world and thus sees the need to update the strategy to address growing challenges. The strategy identifies emerging threats and highlights their sources and potential impact on information assets and people. Major threats to Jordan include: foreign intelligence services, terrorism and geopolitical unrest, hacktivists, insiders, and crime and corruption. Cybersecurity challenges include: Internet of Things, ransomware, artificial intelligence, server less software, sensitive infrastructure, advanced phishing campaigns, strategic use of information operations, cloud computing, cybersecurity awareness, paid hacking services, and skills shortages. The vision is to achieve Jordan is confident and secure in the digital world and resilient to cyber threats.

The strategic goals were:

- Protection: Enhance trust and resilience among the government, critical national infrastructure, business sectors, and the public to face and respond to cyber threats.
- Detection and Investigation: Improve understanding and interception of hostile actions targeting the kingdom and its information assets

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

- Response: Develop and deploy appropriate capabilities to respond to cyberattacks similarly to other national security threats.
- Development: Foster sustainable and suitable sovereign knowledge, skills, and capabilities to maintain robust cybersecurity through academic, private sector, research and development partnerships, and international collaboration.

The strategy is based on the following principles; government management of cybersecurity at the highest levels as an urgent national priority given the threats facing national security, establishing appropriate levels of national governance models, coordination, and control, prioritizing cybersecurity measures for institutions and systems, recognizing cybersecurity as a shared responsibility among all government entities, academic institutions, businesses, and individuals, government leadership in protecting critical infrastructure, ensuring individuals understand how to protect themselves online, connecting with public policies for telecommunications and e-government strategies is crucial for the strategy's success, emphasizing cybersecurity culture as vital for the strategy's success, digital risk management as the responsibility of corporate boards, explicitly incorporating cybersecurity in all individual and organizational decisions, and ensuring security in network and infrastructure design. The strategy concludes by noting the difficulty in measuring success in achieving national cybersecurity goals due to variations in defining security incidents, vulnerabilities, and threats. It ends with a glossary of terms and abbreviations [35]. Jordan is currently preparing to launch the National Cybersecurity Strategy for the next 5 years through launching the national dialogue for cybersecurity strategy 2024-2028, which will be launched soon before the end of the year 2024 [36].

3.18. Palestine

Cybersecurity initiatives are still timid in Palestine. The Ministry of Communications and Information Technology has launched the Internet Security and Safety Initiative, and other limited initiatives. The Palestinian Cabinet decided in its session No. 16 of 2015 to approve the internal regulations for the work of the Palestinian Computer Emergency Response Team. The team works to achieve the following objectives: Creating a safe and reliable Palestinian computer information environment using the latest technology, building a reliable point of contact for government cadres in computer information security and communications, so that the team is the national central point of contact for coordination with all concerned parties, building capacities in the field of cybersecurity to increase the ability to detect computer information security incidents and respond to any emergency and respond to such incidents, enhancing the culture of awareness in cybersecurity in public and private sector institutions, including citizens, preparing cybersecurity policies, programs and strategies and working to implement them, creating a sound legal legislative environment regulating cybersecurity and combating cybercrimes, with regard to technical and administrative aspects, developing executive and financial plans to advance the work of the team and its sustainability.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

The Cabinet's decision to establish the National Cybersecurity Authority can be viewed (The Cabinet decides to establish the National Cybersecurity Authority and assigns A government team to prepare for this [37].

Preparations are currently underway to select the team tasked with preparing the national strategy for cybersecurity in Palestine.

3.19. Libya

Libya has recently started building its cybersecurity strategy, despite the scarcity of resources on this topic, we summarize the following.

The vision is to providing a safe environment for digital transformation and building the necessary capabilities to confront the risks associated with it, and enabling individuals and institutions to succeed in safely benefiting from cyberspace.

The related scope of the strategy is including everything related to protecting and securing the interests and rights of the nation and humanity in cyberspace.

The Strategy objectives are; strengthening and developing the legal and legislative framework and ensuring the consolidation of good governance of cyberspace, building and raising the necessary human and material capabilities to protect and secure cyberspace and digital transformation, enhancing the reliability, security, and reliability of electronic transactions, to localize the cybersecurity industry, encouraging cooperation with the interior and exterior, individuals and institutions, in an effort to support the trend towards digital transformation by spreading the culture of cybersecurity in society.

The areas of strategy implementation are;

1. A program to prepare the general frameworks and the legal and legislative environment for cyberspace.
2. A program to establish and develop integrated mechanisms to protect cyberspace security and secure vital infrastructure for communications and information technology.
3. A program to prepare the national environment for encryption technologies, digital signatures, and authentication of electronic transactions.
4. A program to build human capacities and national expertise in the field of cybersecurity in various sectors.
5. A program to support scientific research, enhance the spirit of initiative and innovation, and localize the cybersecurity industry.
6. The national program to enhance the culture of cybersecurity in society to achieve the best benefit from technology.
7. A program to qualify and ensure the commitment of national institutions to local and international cybersecurity standards, controls, and policies.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

8. A program to enhance international, regional, and local partnerships and cooperation to secure cyberspace.
9. A program to raise the readiness of information and communications technology infrastructure for national institutions to confront emergencies, recover from them, and ensure business continuity [38].

3.20. Somalia, Djibouti, and Comoros

There is not enough information about these countries in the field of national cybersecurity strategies and they do not have them yet.

4. DISCUSSION

Authors should discuss the results and how they can be interpreted from the perspective of previous studies and of the working hypotheses. The findings and their implications should be discussed in the broadest context possible. Future research directions may also be highlighted. Since 2021, nations have, on average, increased the number of cybersecurity-related measures they have taken and strengthened their cybersecurity commitments. The average country score worldwide is now 65.7 out of 100. The majority of nations excel in the legal pillar out of the five GCI pillars. The typical nation, on the other hand, performs the worst in the technical and capacity-development pillars. Unlike the country classification in the fourth edition, the Global Cybersecurity Index 2024 5th Edition was published during the writing of the final part of this research, and the classification was based on the distribution of countries in the form of tiers, five tiers are used to measure a country's performance, with Tier 1 being the best performance and Tier 5 the lowest. These levels offer peer groups according to scores to assist nations in comprehending and identifying ideals for development, see figure 1 [39].

Figure 1: GCI pillars

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

As mentioned at the beginning of this research, the answer to the research questions is as follows:

1. What is the current state of cybersecurity in Arab countries?

As exhibited in the current release of GCI, there are high- and low-performing nations in almost every region. The top tier, Tier 1 (T1), is occupied by 46 countries according to this edition of the GCI. Thirty countries would have been in T1 if the tier-based system had been used for the GCI7's fourth edition.

Countries in Europe, Asia and the Pacific, the Arab States, and Africa account for a large portion of the T1 migration. Since the previous edition, these nations have significantly improved in all five GCI pillars. The majority of the nations (105), which represent the numerous nations that have been advancing digital services and putting people online, were grouped into T3 and T4, signifying the work that has to be done to guarantee that cybersecurity is integrated into their meaningful connectivity goals, A large cyber-capacity gap exists in many of these nations as well.

They want to improve their cybersecurity but are constrained by issues with staffing, equipment availability, and long-term finance, see figure 2.

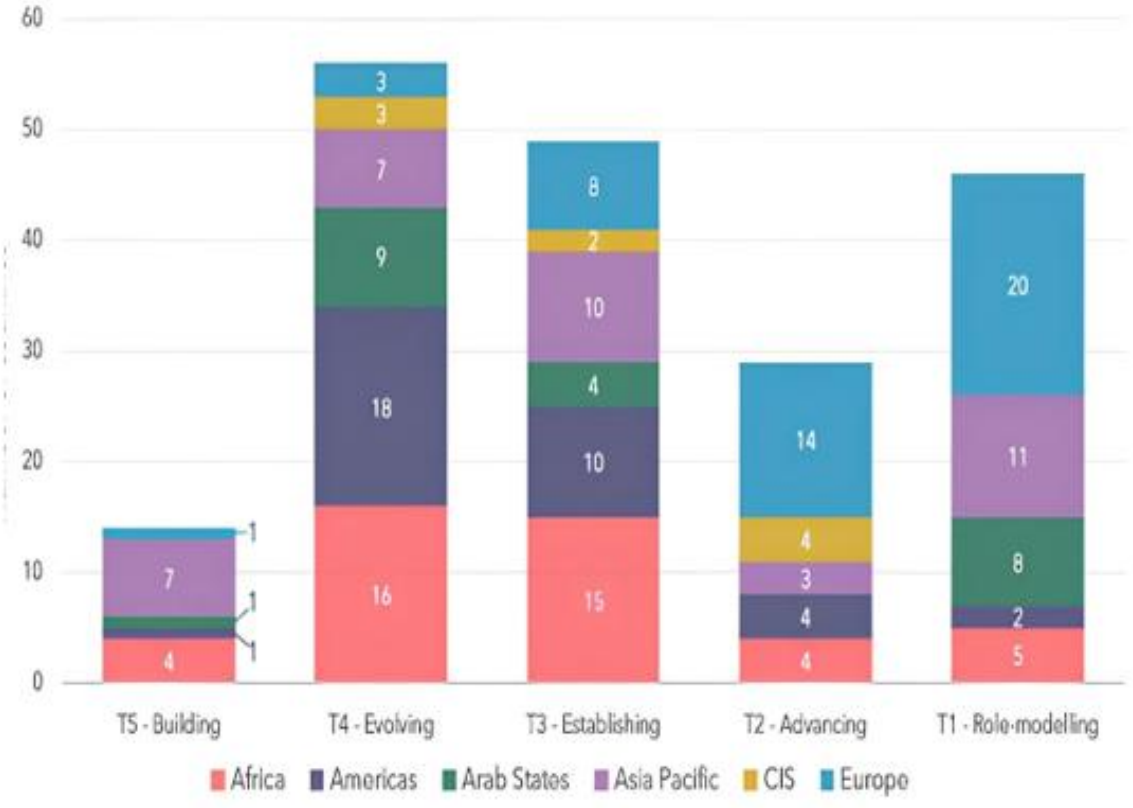

Figure 1: GCI tier performance by region

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

Referring to the figure above, we find that the distribution of Arab countries came in 4 tiers: the first, third, fourth, and fifth, see table 3.

Table 3: GCI 5th Edition for Arab region

Country Name	(GCI)5thEdition	LM	TM	OM	CD	CM	Regional Rank
Saudi Arabia	100	20	20	20	20	20	1
United Arab Emirates	100	20	20	20	20	20	2
Egypt	100	20	20	20	20	20	3
Qatar	100	20	20	20	20	20	4
Jordan	98.6	20	19.38	19.22	20	20	5
Bahrain	97.94	20	20	20	20	17.94	6
Morocco	97.5	20	18.12	20	19.38	20	7
Oman	97.01	19.59	18.39	20	19.03	20	8
Tunisia	82	19.18	17.8	14.23	14.97	15.82	9
Libya	68.09	16.75	11.2	14	15.75	10.39	10
Algeria	65.87	19.18	8.57	11.02	13.91	13.19	11
Kuwait	60.58	16.9	5.8	11.88	12.16	13.84	12
Iraq	53.07	11.21	9.6	15.77	8.38	8.11	13
Syrian Arab Republic	51.39	15.6	8.74	12.4	9.17	5.48	14
Sudan	48.17	15.57	14.47	6.41	4.37	7.35	15
Mauritania	39.33	17.39	1.39	10.59	1.09	8.87	16
Comoros	39.15	18.03	7.92	7.29	4.39	1.52	17
State of Palestine	37.72	14.24	9.6	2.38	9.04	2.46	18
Somalia	37.38	6.49	4.79	10.64	4.29	11.17	19
Lebanon	32.37	12.08	1.39	10.52	5.02	3.36	20
Djibouti	31.49	11.84	3.54	5.57	1.67	8.87	21
Yemen	7.19	5.29	1.9	0	0	0	22

If we compare the fourth and fifth editions of the Global Cybersecurity Index (GCI) for all Arab countries, we find that all countries, without exception, have improved their index, with the exception of Kuwait and Tunisia.

Following its placement as sixth in the Arab world (86.23%) in the previous edition, Tunisia, fell to 9th in this edition (82%), due to a decline in its rating in the 4 pillars: legal, technical, cooperation, and capacity development, with a slight increase in the organization index. In the same way, Kuwait fell from 9th in the Arab world (75.05) in the previous index to 12th in the current ranking (60.58), for the same reason.

Saudi Arabia maintained its first place in the lead after obtaining a full mark of 100% in the index, and the UAE shared the same mark with it, and Egypt and Qatar joined them and moved up one place. After Egypt was in fourth place and Qatar in fifth place in the previous version, they moved up one place, so that Saudi Arabia, the UAE, Egypt and Qatar became in first place, repeating with a full mark. Jordan moved up 5 places, from 10th place (70.96%) to 5th place (98.6%) in this edition.

Bahrain also improved its ranking from 8th place (77.86%) to 6th place (97.94%) in this edition. Despite its 15-point advance in the index (82.41% to 97.5%), it remained in 7th place in the Arab world.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

Despite its one-point advance in the index, Oman dropped from 3rd place (96.04%) in the previous index to 8th place (97.01%) in the current index, due to the progress of some other Arab countries more than Oman. Libya, Algeria, Iraq and Syria jumped to 10th, 11th, 13th and 14th places respectively. Despite their improvement in the GCI, Sudan, Palestine and Lebanon fell from 11th, 15th and 13th places (GCI 2020) to 15th, 18th and 20th places (GCI 2024). The remaining countries can be compared in Tables 2 and 3.

2. How Prepared are Arab Countries to Develop A Comprehensive, Unified Cybersecurity Strategy?

The GCIv5 edition depicts country performance in tiers rather than ranks, as mentioned in the methodology section regarding the switch to a tier-based model. While discrepancies between nation ratings might be quite small and involve an error range based on the accuracy of questionnaire replies, clarifications given, or country engagement, tiers offer numerous advantages over ranks. Every tier presents a collection of peers with comparable performance by grouping countries with similar scores together.

Every tier presents a collection of peers with comparable performance by grouping countries with similar scores together. For total scoring, a tier-based methodology has been established. Countries with comparable scores may yet differ significantly on a pillar, indicator, sub-indicator, or micro indicator level because the total score is a weighted average of a nation's cybersecurity efforts across all five pillars in the questionnaire. The quality and impact of a country's actions across all pillars and indicators will differ; these are aspects that the GCI does not measure. Every tier presents a collection of peers with comparable performance by grouping countries with similar scores together. Nations have the option to create their own GCI tiers or rankings; it should be mentioned, though, that the ITU does not support other methods of national comparison.

If we discuss the readiness of Arab countries to develop a comprehensive and unified strategy for cybersecurity, and based on the data and indicators that were discussed, we find that there is a disparity in readiness between Arab countries in this field. The eight Arab countries Role Modelling (Saudi Arabia, the Emirates, Egypt, Qatar, Jordan, Oman, Morocco and Bahrain) that were ranked in the first trier have complete and almost complete readiness to adapt their national strategies and form a unified Arab strategy in cybersecurity, because they have a strategy implemented in their countries and all the measurements and measures related to it are present.

This is clearly evident by returning to their global cybersecurity index, as they are complete or almost complete, and only need to discuss the technical procedures to join the unified strategy. By showcasing a strong cybersecurity commitment to coordinated, government-driven actions that include assessing, establishing, and implementing specific widely accepted cybersecurity measures across all five pillars or up to all indicators, these countries were able to achieve an overall GCI score of at least 95/100.

As for the four Arab countries establishing (Algeria, Libya, Kuwait and Tunisia) that were presented in the third trier. Establishing designates nations with an overall score of at least 55/100 that have proven they are committed to government-driven cybersecurity

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

initiatives, such as assessing, establishing, or putting into practice a set of widely accepted cybersecurity measures across a moderate number of pillars or indicators, It needs to make further progress to mature its national strategies first, and then move on to researching the unified Arab strategy.

Nine Arab countries fell into the fourth tier in the Global Cybersecurity Index under the title "Evolving", which shows nations that met the minimum requirements for a government-driven cybersecurity commitment, as well as those that achieved an overall score of at least 20/100 by evaluating, establishing, or putting into practice certain widely accepted cybersecurity measures in at least one pillar, or multiple indicators and/or sub-indicators. It needs to work hard and fundamentally to develop its national strategies, which are in the early stages. Yemen came in the last level, fifth tier, which is labelled "building", which, by demonstrating a basic cybersecurity commitment to government-driven actions that encompass evaluating, establishing, or implementing certain generally accepted cybersecurity measures in at least one indicator and/or sub indicator, represents nations that received an overall score below 20/100. It requires double effort to establish the foundations of a national cybersecurity strategy.

3. What Challenges do Arab Countries Face in Developing a Unified Strategy in This Field?

Based on the analysis of the cybersecurity situation of Arab countries, the challenges facing Arab countries to develop a unified cybersecurity strategy can be summarized as follows: Securing the communications infrastructure; protecting the application development process; implementing comprehensive cybersecurity governance in the Arab digital space; securing data management; supervising the Arab cyberspace; coordinated work and harmonious development between modern technologies and regulatory frameworks.

The unified Arab cybersecurity strategy will determine how to overcome this challenge by establishing information exchange mechanisms to enable the exchange of information and vigilance about cyber threats that can be exploited in the public and private sectors. The unified strategy will also determine a common methodology for managing cybersecurity risks, ensuring effectiveness and consistency among all organizations.

4.1. Implications

We are fully convinced that, in the realm of cybersecurity, many Arab countries are making significant efforts. However, the path remains long to effectively address the increasing cybersecurity threats day by day. This situation requires unified efforts at the Arab, regional, and international levels to find comprehensive and sustainable solutions. Today, more than ever, we need to accelerate our steps towards forging strong cooperative relationships to create a collaborative approach that enhances an open, free, and secure digital space for everyone in the Arab world.

We, as the information technology community, aspire to be the link between Arab countries in the field of information safety and cybersecurity. We look forward to

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

collaborating with all Arab countries and active entities in this field to achieve our common goals. The region suffers from a severe lack of capabilities in responding to and managing cyber crises and in adopting a national strategy for digital resilience. Transferring the American and European experiences in adopting national cybersecurity policies and related regulations is critically important at present. Additionally, it is crucial to establish an association that unites countries around the world, particularly in the Middle East and North Africa, around cybersecurity capabilities.

This association would connect emergency response centres for training, capacity building, and information exchange. The improvement of indicators for some Arab countries is attributed to the efforts made over recent years to build cybersecurity capabilities. Many Arab countries have advanced in their rankings in the International Telecommunication Union's cybersecurity indices. For example, Saudi Arabia has made a remarkable leap from 46th to 2nd place globally within just three years.

The limitations of the study are that it was dependent on media-presented documents, official government websites, and the Internet; also, no supplementary data was available particularly for several Arab countries that are categorized as fourth or fifth tier. Also; as more nations move up to the top tier over time, there may be less room for differentiation between them. While a nation's absolute score may rise, its relative standing may fall, which would discourage more cybersecurity efforts. Researchers in future studies must keep up with developments in Arab and foreign countries in the field of cybersecurity to learn about everything new in this field.

5. CONCLUSIONS

This section is not mandatory but can be added to the manuscript if the discussion is unusually long or complex. Based on the above, it is evident that cybersecurity strategies have become a top priority for countries, as social networks and the internet have rapidly evolved into fundamental pillars of economic, social, and cultural activities worldwide. This shift necessitates a redefinition of traditional strategies to adapt to these changes. There is a widespread lack of awareness about information security among many citizens and employees in both the public and private sectors, who are considered the weakest link in the information system, even with advanced protection systems in place.

This situation exacerbates the issues related to threats and information breaches. The strategy should help build a digital environment that citizens and organizations can trust. (The Guide - NCS guide, 2020). Cybersecurity must go hand in hand with digital transformation policies, plans and strategies as the cyber threat landscape rapidly evolves.

Cybersecurity must be a priority supported at all levels of governance. Coordinating cybersecurity initiatives and sharing essential information will significantly enhance security, safety, resilience and trust within the Arab cyberspace. The Arab region will be well positioned to reap the benefits of digital transformation, multi-stakeholder innovation and the virtual economy.

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

Author Contributions

Six researchers contributed to this research. Dr. Waheeb Abu-ulbeh and Dr. Mamoun Abu Helou played a conceptual role, which included formulating and developing the objectives for the overall research purposes.

They also wrote the original draft, specifically writing the first draft (including thematic translation).

Dr. Mohammed Atoum proposed the design of the methodology used and assumed responsibility for supervision, including external guidance for the core team, and returned to summarize the study data. Dr. Nashat Alrefai assumed responsibility for managing and coordinating the planning and implementation of the research activity. Dr. Hani Awidat and Dr. Abdullah Mahmmoud played a role in verifying the accuracy of the information collected, whether as part of the activity or separately, from replication and other research outcomes.

In the final writing stage, the six researchers participated in this role by reviewing, editing, and submitting the work published by the members of the research group, specifically critical reviews and reviews in the pre-publication stages. “All authors have read and approved the version of the manuscript.”

Data Availability Statement

Data Availability Statement: We, the researchers of this study, are happy to share any data that other researchers or any official body need by contacting the corresponding author at the official email shown in the affiliation.

Acknowledgments

This study was conducted with self-funding from the authors.

Conflicts of Interest

The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

APTs	Advanced Persistent Threats
ASEAN	Association of Southeast Asian Nations
CD	Capacity-building/Development Measures
CERT	Computer Emergency Response Team
CIS	Commonwealth of Independent States
CIU	Cyber Intelligence Unit
CM	Cooperation Measures
ECOWAS	Economic Community of West African States
ENISA	European Union Agency for Cybersecurity
GCI	Global Cybersecurity Index
ICT	Information and Communications Technology
ITU	International Telecommunication Union
LM	Legal Measures
NCSS	National Cybersecurity Strategies
NRC	National Cybersecurity Response Committee
OAS	Organization of American States
OM	Organisational/regulatory Measures
TM	Technical Measures
UAE	United Arab Emirates

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

References

1) Abdel Wahid Al-Bidiri, Cybersecurity Strategy: A Case Study of Morocco, Journal of Strategic and Military Studies 2021, Issue 11, Democratic Arab Center for Strategic, Political, and Economic Studies, Germany - Berlin, First Edition.

2) Arabic_GOAT.pdf, 2021, Available online: https://cybilportal.org/wp-content/uploads/2021/12/Arabic_GOAT.pdf (accessed on 26 07 2024).

3) Global cybersecurity index, 2021, Available online: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E (accessed on 29 09 2024).

4) ITU-D Cybersecurity Program Global Cybersecurity Index – GCIv5 Reference Model (Methodology), 2024, Available online: 513560_2E.pdf (itu.int) (accessed on 02 10 2024).

5) National Capabilities Assessment Framework, 2020. National Cybersecurity Assessment Framework (NCAF) Tool — ENISA (europa.eu), © 2005-2024 by the European Union Agency for Cybersecurity.

6) Good Practices in Innovation under NCSS Good Practices in Innovation on Cybersecurity Under the National Cyber Security Strategies, 2019. Good practices in innovation on Cybersecurity under the NCSS — ENISA (europa.eu), © 2005-2024 by the European Union Agency for Cybersecurity.

7) Organisation of American States (OAS) – Cybersecurity program, 2016. https://www.oas.org/es/sms/cicte/IGF-OAS.pdf. cybersecurity@oas.org.

8) ECOWAS Regional Cybersecurity and Cybercrime Strategy, 2021. ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf (ocwarc.eu). © OCWAR-C 2020. All rights reserved.

9) ASEAN Cybersecurity COOPERATION Strategy, 2021. Asean Cybersecurity Cooperation Strategy. © 2024 ASEAN Secretariat. All rights Reserved.

10) Mauritanian Cybersecurity Strategy, Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/strat-cybersecu-mauritanie300519.pdf (accessed on 17 10 2024).

11) Sudan seeks to build a national strategy for cybersecurity, 2020, Available online: السودان يسعى لبناء استراتيجية وطنية للأمن السيبراني | مصراوى (accessed on 17 09 2024).

12) Tunisian National Cybersecurity Strategy 2020 – 2025, Available online: https://www.ancs.tn/sites/default/files/ncss24/ (accessed on 17 08 2024).

13) The National Strategy for Information Society and Digital Economy, 2013. Morocco_2013_Maroc_CyberSecurity_2013_ENG.pdf (itu.int). @ Digital Morocco the National Strategy for Information Society and Digital Economy - 2009-2013.

14) الإذاعة الجزائرية (radioalgerie.dz), 2024. Available online: "بلغت مرحلتها النهائية"استراتيجية أمن الأنظمة المعلوماتية | https://news.radioalgerie.dz/ar/node/48040 (accessed on 03 12 2024).

15) الإستراتيجية الوطنية " السيد رئيس الجمهورية، القائد الأعلى للقوات المسلحة، وزير الدفاع الوطني يترأس مراسم افتتاح الملتقى الوطني حول "للأمن السيبراني: من أجل جزائر صامدة سيبرانيا -الجزائر - وزارة الدفاع الوطني (mdn.dz), Available online: https://www.mdn.dz/site_principal/sommaire/actualites/ar/2023/juin/cna07062023ar.php (accessed on 03 12 2024).

16) Jamal Bouazid, The Algerian Strategy for Combatting Cybercrimes: Challenges and Future Prospects, Journal of Legal and Political Sciences **2019**, Volume 10, Issue 01, pp. 1262 – 1293.

17) National Cybersecurity Strategy of Egypt, 2017, Available online: https://mcit.gov.eg/Upcont/Documents/swf/AR_National_Cybersecurity_Strategy_2017_2021/inde.html (accessed on 16 08 2024).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

18) National Cybersecurity Strategy of Kuwait 2017 – 2020, Available online: https://www.citra.gov.kw/sites/ar/LegalReferences/Cyber%20Security.pdf (accessed on 15 07 2024).

19) Al-Anbaa Newspaper, February 6, 2022, Available online: https://www.alanba.com.kw/1100125 (accessed on 25 07 2024).

20) National Information Security Policy, Syria, Ministry of Communications and Technology, National Network Services Authority, 2014, Available online: https://www.nans.gov.sy/ar/page/information_security_center_documents (accessed on 24 07 2024).

21) Contribution to the Preparation of the Cybersecurity Strategy, General Authority for Network Services, Ministry of Communications and Technology, 2021. Available online: https://www.nans.gov.sy/ar/article/contribution_to_preparing_the_strategy_f (accessed on 15 08 2024).

22) Iraqi Cybersecurity Strategy, Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf (accessed on 23 08 2024).

23) Decisions of the Iraqi National Security Council, February 16, 2022, Available online: https://www.pmo.iq/press2022/16-2-202203.htm (accessed on 23 08 2024).

24) Lebanese Cybersecurity Strategy, Available online: http://www.pcm.gov.lb/Library/Files/LRF/tamim/Strategie_Liban_Cyber_AR_V20_Lg.pdf (accessed on 13 09 2024).

25) National Cybersecurity Strategy of the Kingdom of Bahrain, Available online: https://www.ncsc.gov.bh/ar/national-strategy.html (accessed on 23 08 2024).

26) Qatar Cybersecurity Strategy, Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Qatar_2014_national_cyber_security_strategy.pdf (accessed on 27 08 2024).

27) Thinkers of the Emirates, 2022, Available online: https://mufakirualemarat.ecssr.ae/publications/edaat/detail/603 (accessed on 22 08 2024).

28) National Cybersecurity Strategy - Telecommunications and Digital Government Regulatory Authority, 2019, Available online: https://tdra.gov.ae/ar/national-cybersecurity-strategy (accessed on 15 08 2024).

29) International Telecommunication Union (ITU), World Bank, Commonwealth Secretariat (ComSec), Commonwealth Telecommunications Organization (CTO), and NATO Cooperative Cyber Defence Centre of Excellence 2020 (COE CCD NATO). Guide to Developing a National Cybersecurity Strategy - Strategic Commitment to Cybersecurity. The Guide - NCS guide, 2020, Available online: https://ncsguide.org/the-guide/ (accessed on 15 10 2024).

30) National Cybersecurity Authority, 2020, Available online: https://nca.gov.sa/strategic (accessed on 02 09 2024).

31) Oman National CERT, 2022, Available online: https://cert.gov.om/ (accessed on 04 09 2024).

32) Meeting at the Ministry of Communications Discusses the National Cybersecurity Strategy Project - Public Telecommunications Corporation, 2022, Available online: https://ptc.gov.ye/?p=8208 (accessed on 15 09 2024).

33) First National Cybersecurity Conference (ncsc.ye), 2021, Available online: https://ncsc.ye/ (accessed on 15 12 2024).

Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/
Journal of Tianjin University Science and Technology
ISSN (Online):0493-2137
E-Publication: Online Open Access
Vol: 58 Issue: 07:2025
DOI: 10.5281/zenodo.15845018

34) Jordanian Cybersecurity Law, 2019, Available online: https://ncsc.jo/ebv4.0/root_storage/ar/eb_list_page/0-قانون_الأمن_السيبراني.pdf (accessed on 01 10 2024).

35) Legislation and Policies - Ministry of Digital Economy and Entrepreneurship, National Cybersecurity Strategy 2018-2023, Available online: https://modee.gov.jo/Ar/List/تشريعات_والسياسات (accessed on 28 09 2024).

36) Launching the National Dialogue for Cybersecurity Strategy 2024-2028, Available online: إطلاق الحوار الوطني لاستراتيجية الأمن السيبراني 2024-2028 المركز الوطني للأمن السيبراني (ncsc.jo) (accessed on 06 10 2024).

37) The Council of Ministers Decides to Establish the National Cybersecurity Authority and Assigns a Government Team to Prepare for It | PNN, 2022, https://pnn.ps/news/666105.

38) Libyan National Cyber Security Strategy, Available online: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/National_CyberSecurity_Strategy_Liby a_CERT.pdf (accessed on 22 10 2024).

39) Global cybersecurity index 5th Edition, International Telecommunication Union (ITU) - Development Sector 2024, Available online: https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 (accessed on 29 11 2024).