Gyancity Journal of Electronics and Computer Science,
Vol.9, No.2, pp. 1-25, September 2024
ISSN: 2446-2918 DOI: 10.21058/gjecs.2024.92001

NATIONAL CYBERSECURITY STRATEGY, OPPORTUNITIES AND OBJECTIVES

Waheeb Abu-ulbeh

Faculty of Administrative Sciences and Informatics, Al-Istiqlal University, Jericho, 10, Palestine
w.abuulbeh@pass.ps

Abstract

The world has witnessed rapid progress in modern technologies, making technical systems an essential element in all areas of life for individuals and the work of institutions—a means of protection and countering cyber risks. The cybersecurity initiatives in Palestine are still timid. The Ministry of Communications and Information Technology launched the Internet Security and Safety Initiative. The initiative dealt with allocating time in schools to talk about the initiative and raise awareness about the safe use of the Internet. It is known that the Global Cybersecurity Index (GCI), which was issued for the first time in 2015, helps countries identify areas for improvement in the field of cybersecurity, which in turn leads to an increase in the general level of cybersecurity around the world, and Palestine ranked first. "122" internationally and "15" Arabs, in its latest edition. In order to confront current and emerging cybersecurity threats, and to identify areas for improvement in cybersecurity, the State of Palestine needs to expedite drawing up a comprehensive national strategy. National Cybersecurity Strategies are the main documents for nation-states to establish strategic principles, guidelines, and objectives and, in some cases, specific measures in order to mitigate risks associated with cybersecurity and support the confidence of the Palestinian citizen. This paper discusses the importance and challenges of having a Palestinian cybersecurity strategy by improving cooperation measures, capacity building measures, organizational, technical, and legal measures in order to achieve the vision of a "safe Palestinian cyberspace as part of the Arab cyberspace".

Keywords: *Cyberspace, Cybersecurity, Global Cybersecurity Index (GCI), Cyber risks, Cybersecurity strategy.*

1. Introduction

The world is witnessing a rapid and intense development in the use of information and communication technologies across all fields and by all categories, both in the public and private sectors, impacting the daily lives of citizens in various areas. While these technologies have provided an interconnected digital environment, they also bring with them risks to cyberspace, along with internal and external threats targeting rights, freedoms, and national security. This technological advancement has introduced new and evolving concepts such as big data, cloud computing, the Internet of Things, 5G communications, social networks, artificial intelligence, and blockchain, among others. These developments have led to an increase in the level and variety of cyber threats and attacks, especially in the context of digital openness at the regional and international levels. Figure 1 illustrates the amount of data created on the internet every minute.

Although technological development has established new rules (cyberspace), allowing countries, organizations, peoples, and nations to communicate directly across all fields, this added value has hindered the protection of the rights of institutions and individuals to freely utilize this space within a legal framework. The excessive use of communication technologies and the rapid flow of data (information revolution) have doubled the incidence of breaches and espionage methods, initially affecting personal security. This has made people's lives and privacy vulnerable to unprecedented extortion and increased blackmail operations, leaving no one exempt, whether they are officials or ordinary citizens. Breaches aimed at espionage and sabotage have also targeted security institutions, ministries of defense, government institutions, companies, and banks in major countries around the world.

In response to this borderless and diverse threat (cybercrimes, cyber terrorism, and cyber wars), international decision-makers have sounded alarms to build technical barriers and walls to prevent these attacks (cybersecurity). This response is crucial, as extortion operations have reached levels that could harm national, regional, and global security.

The term "cybersecurity" has recently emerged with various national and international definitions. According to the International Telecommunication Union (ITU), "cybersecurity" refers to "a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the availability, integrity, and confidentiality of assets in the connected environment, including computing devices, personnel, infrastructure, applications, services, telecommunications systems, and data" (ITU, 2020: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-CYB_GUIDE.01-2018-PDF-A.pdf).

To organize and direct cybersecurity operations, a comprehensive strategy is required to define political objectives, necessary measures, and responsibilities to ensure the protection of data, networks, the internet, and cyberspace, which modern societies increasingly depend on. These strategies include ensuring the confidentiality of data exchanges, data integrity, system availability, and protection against technical failures and cyber-attacks, through the prioritization of securing infrastructure.

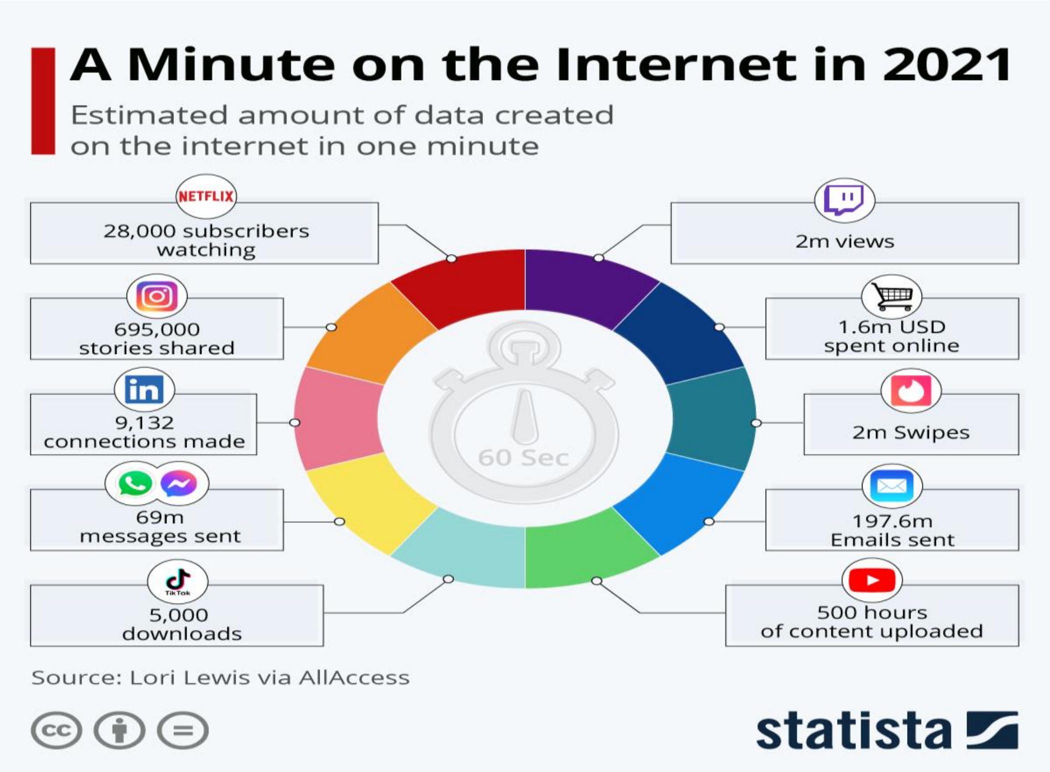


Figure 1: The amount of data created on the internet every minute (Chart: A Minute on the Internet in 2021 | Statista, 2021);
(https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf, 2022)

Table 1 shows the group of countries that have organized a national cybersecurity strategy. See Table (1).

Importance of the Study

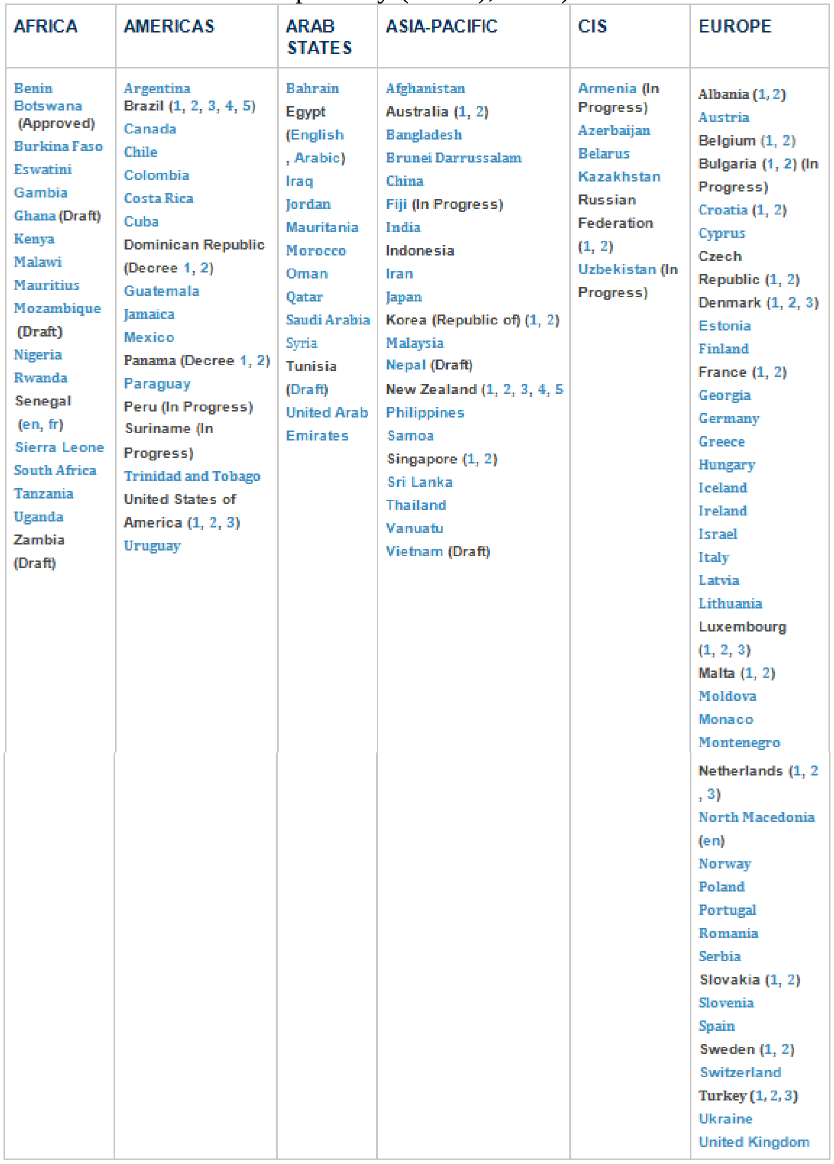
The importance of the study lies in addressing the topic of digital safety in communities and clarifying the mechanisms and necessary steps to achieve digital security and safety in Palestine, relying on successful experiences in regional and international countries and joining international and regional agreements and treaties.

To counter the increasingly advanced and dangerous threats facing countries due to the availability of sophisticated exploitation tools and techniques, national strategies have been adopted to ensure countries protect their information security and infrastructure from various risks and threats. As a result, these threats have necessitated the creation of international cooperation mechanisms.

Decision-makers in major countries such as the United States, the European Union, Russia, China, and India now prioritize cybersecurity as a key component of their national defense strategies. More than 131 countries have announced the allocation of specific scenarios for cyber wars and attacks within their national security teams.

Countries today are striving to develop their cybersecurity strategies, protect their critical information infrastructure, and deter cybercrime by establishing national cooperation between the government and the telecommunications and information technology industries. They are also creating national capacities for computer management (Gaidan and Al-Rubaie, 2020).

Table 1: ITU Member States with National Cybersecurity Strategy. (National Cybersecurity Strategies Repository (itu.int), 2022)



AFRICA	AMERICAS	ARAB STATES	ASIA-PACIFIC	CIS	EUROPE
Benin Botswana (Approved) Burkina Faso Eswatini Gambia Ghana (Draft) Kenya Malawi Mauritius Mozambique (Draft) Nigeria Rwanda Senegal (en, fr) Sierra Leone South Africa Tanzania Uganda Zambia (Draft)	Argentina Brazil (1, 2, 3, 4, 5) Canada Chile Colombia Costa Rica Cuba Dominican Republic (Decree 1, 2) Guatemala Jamaica Mexico Panama (Decree 1, 2) Paraguay Peru (In Progress) Suriname (In Progress) Trinidad and Tobago United States of America (1, 2, 3) Uruguay	Bahrain Egypt (English , Arabic) Iraq Jordan Mauritania Morocco Oman Qatar Saudi Arabia Syria Tunisia (Draft) United Arab Emirates	Afghanistan Australia (1, 2) Bangladesh Brunei Darrussalam China Fiji (In Progress) India Indonesia Iran Japan Korea (Republic of) (1, 2) Malaysia Nepal (Draft) New Zealand (1, 2, 3, 4, 5 Philippines Samoa Singapore (1, 2) Sri Lanka Thailand Vanuatu Vietnam (Draft)	Armenia (In Progress) Azerbaijan Belarus Kazakhstan Russian Federation (1, 2) Uzbekistan (In Progress)	Albania (1, 2) Austria Belgium (1, 2) Bulgaria (1, 2) (In Progress) Croatia (1, 2) Cyprus Czech Republic (1, 2) Denmark (1, 2, 3) Estonia Finland France (1, 2) Georgia Germany Greece Hungary Iceland Ireland Israel Italy Latvia Lithuania Luxembourg (1, 2, 3) Malta (1, 2) Moldova Monaco Montenegro Netherlands (1, 2 , 3) North Macedonia (en) Norway Poland Portugal Romania Serbia Slovakia (1, 2) Slovenia Spain Sweden (1, 2) Switzerland Turkey (1, 2, 3) Ukraine United Kingdom

The U.S. Department of Defense "Pentagon" has classified the internet as the fourth domain of warfare after air, sea, and land. China is the first country in the world to introduce the concept of sovereign internet, which means the state's absolute control over the internet, monitoring data exchange, and blocking external sites harmful to national security. The operation of the internet in China is governed by the so-called "Great Firewall" (Al-Baidiri, 2021).

The importance of the study can be summarized from two aspects:

- Scientific Importance: The scientific importance of the current study lies in the fact that the topic of digital safety and cybersecurity is crucial for societies today. It has attracted the attention of many researchers as it is highly relied upon to address many problems and challenges related to information security and protection from cyber threats.
- Practical Importance: The practical importance of the study is highlighted by:

o The scarcity of studies on the topic of cybersecurity in Palestine, especially regarding cybersecurity requirements. The researchers believe this study will establish a starting point for future research, impacting various administrative aspects of contemporary organizations and their information security.

o Drawing the attention of decision-makers and professionals to the current study's importance in clarifying the requirements institutions must prepare to implement the concept of cybersecurity.

o The need to establish a roadmap and practical guide for developing a national cybersecurity strategy.

Study Problem:

This research primarily highlights the importance of cybersecurity, especially in Palestine. It examines Palestinian experiences in this field and compares them with Arab and international experiences. The study also explores the importance of adopting a new strategy in cooperation with regional and global countries to build a secure cyber space, identifying local obstacles, challenges, and capabilities that can help in constructing a national strategy. Based on the above, the main problem of the study lies in answering the following questions:

- What is the reality of cybersecurity in Palestine?

o What is the reality of Arab and international cybersecurity?

- What is the readiness of Palestinian capabilities to prepare a comprehensive national cybersecurity strategy?

o What steps should be taken to enhance the security system to protect data and cyberspace?

Study Methodology:

The researcher adopted the descriptive-analytical method for this study by studying and analysing texts related to cybersecurity strategies and data found in literary texts, legislation, and international agreements.

Study Plan:

The study is divided into three demands, detailed as follows:

1. First Demand: The Concept of Cybersecurity and Its Issues.

o According to Kaspersky (2022), the term "cybersecurity safety" refers to the steps computer and device users can take to enhance their online security and maintain system integrity. Cybersecurity safety means adopting security-centric habits and mindsets to help individuals and organizations mitigate potential online violations. One of the fundamental principles of cybersecurity safety is making it part of the daily routine.

o Kaspersky (2021) states that cybersecurity safety aims "to maintain the basic safety and security of devices and software, ensuring protection from threats such as malware. Regular practice of cybersecurity safety helps keep data safe and secure. Just like any habit you want to establish, cybersecurity safety requires routine and repetition."

o Common problems that cybersecurity safety is designed to address include:

□ Security breaches: Including threats caused by hackers, phishing, malware, and viruses.

□ Data loss: Hard drives and online cloud storage that haven't been backed up are vulnerable to breaches, damage, or other issues that could lead to data loss.

□ Outdated software: Which can make your device more susceptible to online attacks.

□ Updated antivirus software: Security programs that haven't been updated will be less effective at protecting against the latest cyber threats.

o In the end, according to Kaspersky (2021), cybersecurity safety means "developing a preventive routine to keep personal and financial information secure when using a computer or mobile device. Using strong passwords and changing them regularly, keeping software and operating systems updated, erasing hard drive data, and using comprehensive antivirus software like Kaspersky Total Security helps stay ahead of the latest cyber threats."

o Measuring the network's ability to maintain digital resilience using metrics is not limited to tracking alone. Cyber hygiene (2022) emphasizes that cybersecurity is everyone's responsibility, meaning that while organizations need to prioritize cybersecurity, individual users must do the same.

o Given that individual and organizational security components are integral parts of a national cybersecurity strategy, attention must be paid to the importance of cybersecurity in producing a comprehensive national cybersecurity strategy. Organizations like the Cybersecurity and Infrastructure Security Agency (CISA) provide various cybersecurity safety services, often for free, to reduce cybersecurity risks in the United States. These services are offered to government agencies and critical infrastructure organizations in both the public and private sectors (Okta, 2022).

2. Second Demand: The Reality and Challenges of Cybersecurity in Palestine

o Cybersecurity has become a critical and sensitive issue, topping national and strategic security concerns for all countries. Misusing information networks and underestimating their security leads to numerous informational, financial, and social damages and disasters. Therefore, it is crucial to take all possible precautions to secure ourselves, our institutions, and our country to avoid falling victim to cyber-attacks or extortion attempts, especially as technology has become indispensable. Information security, starting from individuals and extending to institutions and the state, remains a cohesive link.

o Cybersecurity initiatives in Palestine are still modest. The Ministry of Communications and Information Technology launched the Internet Safety and Security Initiative, dedicating time in schools to discuss the initiative and raise awareness about safe internet use (Mousa, 2018).

o 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 technological means used, 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, Promoting a 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 electronic crimes, with regard to technical and administrative aspects, Developing executive and financial plans to advance the work of the team and its sustainability (Qanon website (qanon.ps), 2015).

o Another aspect is creating new job opportunities, a new world in employment pathways, and reducing cyber unemployment. This begins with building a comprehensive national cybersecurity strategy. Risks associated with remote work security and increasing ransomware attacks have heightened the need for online specialists, creating new job opportunities in digital business protection and leading to real job creation.

The Importance of Cybersecurity Career Paths for Palestine

o As the state plans to develop early-stage cybersecurity experts, this will become valuable and make the state more effective. As the state advances digitally in this modern field, it will become prominent in cybersecurity, exporting this national industry abroad and rapidly building it domestically.

o Like any industry, the country's culture and leadership play a crucial role in business success. Examples of opportunities in this field include, but are not limited to, Chief Information Security Officers and domain managers (maannews.net, 2022).

o The Palestinian Cabinet decided to establish the National Cybersecurity Authority and assigned a government team to prepare for it (PNN, 2022).

o Palestine's Membership in the International Telecommunication Union (ITU)

 In 2018, during the 99th session of the Plenipotentiary Conference held in Dubai, Palestine's membership in the ITU was accepted. This followed Palestine's participation in the 2006 Regional Radio Communication Conference in Geneva, meeting Palestinian requirements for the digital radio plan. Palestine committed to informing the ITU Secretary-General of its acceptance of the arising rights and obligations. This is in addition to the ongoing developments in the ICT sector under Palestinian Authority responsibility, its efforts to restructure the sector, and its membership in the Arab League, Organization of Islamic Cooperation, Non-Aligned

Movement, and UNESCO. Many ITU member states, though not all, recognize the State of Palestine. Therefore, Palestine's delegation participates in all ITU conferences, assemblies, and meetings, including treaty-authorized conferences.

- In the 125th session, it was decided to provide assistance and support to Palestine for rebuilding its communication networks by urging member states to exert all possible efforts to preserve Palestinian communication infrastructure, facilitate Palestine in establishing its international access networks, including ground stations, submarine cables, fiber optic systems, and microwave systems, and provide all forms of support and assistance to Palestine to rebuild, repair, and develop its communication network (Dubai, 2018).

o International Cooperation in Cybersecurity

- The significant development in transportation and, particularly, the information network has allowed criminals to move from one country to another. The international community realized that it is impossible for any single country to eradicate cross-border crimes, as the general procedures of police forces in each country make it challenging to track and follow criminals if they cross state borders. Hence, the need for cooperation among police forces across countries to coordinate and chase criminals (zahrain, 2020).
- Notable international cooperation includes the Budapest Convention on Cybercrime, dated November 23, 2001, which is the first international treaty on cybercrime. This treaty, effective from July 1, 2004, aims to coordinate national legislation on cybercrime, improve national capabilities to investigate these crimes, and facilitate cooperation in this field. It deals with gathering informational evidence in various types of crimes, not just cybercrimes (ESCWA Cybercrime Report, 2015). Many countries from different continents are part of this treaty, and by 2021, 65 countries had ratified it, while three others signed but had not yet ratified it (Full list, coe.int, 2001).
- International cooperation also occurs through judicial authorities of different countries or through the International Criminal Police Organization (Interpol), leading to various forms of police cooperation.
- In the Arab region, the Arab Convention on Combating Information Technology Offences was established on December 21, 2010. It includes five main chapters, with one dedicated to criminalization, specifying types of cybercrimes, another dealing with procedural provisions, and a chapter on legal and judicial cooperation among Arab countries. Eighteen Arab countries signed this convention, with seven ratifying it.
- ESCWA prepared the ESCWA Guidelines for Cyber Legislation during the "Coordination of Cyber Legislation to Stimulate the Knowledge Society in the Arab Region" project, implemented from 2009 to 2012. These guidelines serve as legislative models for the region, covering, in addition to cybercrimes, electronic communications and freedom of expression, electronic signatures and transactions, e-commerce and consumer protection, personal data processing, and intellectual property rights in the information and cyber domain (ESCWA Cybersecurity Report, 2015).

2. The Global Cybersecurity Index (GCI) for the State of Palestine

The Global Cybersecurity Index (GCI), first released in 2015, assists countries in identifying areas for improvement in cybersecurity, thereby raising the overall level of cybersecurity worldwide. Through data collection, the GCI highlights practices that member states can adopt that suit their national environments, encouraging good practices and building a global cybersecurity culture. (512525A.pdf, 2022)

The GCI was launched in 2015 by the International Telecommunication Union (ITU) to measure the cybersecurity commitment of 193 member states, including Palestine, as per Resolution 99 at the 2018 Plenipotentiary Conferences in Dubai (itu.int, 2018). This initiative helps countries identify areas for improvement and encourages them to take necessary actions by raising awareness of the state of cybersecurity globally. As cybersecurity risks, priorities, and resources evolve, the GCI has also adapted to provide a more accurate analysis of the cybersecurity measures taken by countries.

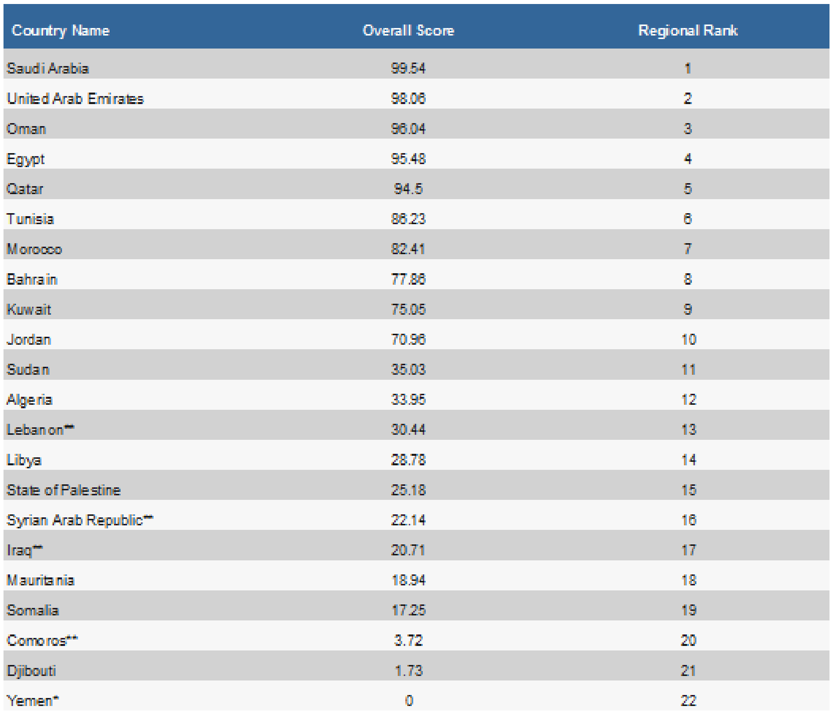
The GCI supports countries in identifying areas for improvement in cybersecurity, encouraging them to take actions to improve their ranking, thereby raising the overall level of cybersecurity globally. The scope, framework, and questionnaire of the GCI, from which indicators and sub-indicators are derived, are prepared and approved through a consultative process regarding "Securing Information and Communication Networks: Best Practices for Building a Cybersecurity Culture." The survey is managed via an electronic platform that gathers supporting evidence.

The ITU published its report on the Global Cybersecurity Index, where Palestine ranked lower compared to neighboring countries. Cybersecurity has become a critical priority for governments, institutions, and citizens alike. A country without adequate cybersecurity negatively impacts national security, digital transformation, and all internet-related activities. In the 2020 report, Palestine ranked 122nd globally and 15th among Arab countries, highlighting the need for collective efforts to improve Palestinian cybersecurity. Palestine scored 25.18 points in the latest cycle, which is 5 points less than the 30.7 scored in 2018. A formal invitation is sent to all ITU member states, including Palestine, to inform them of the initiative and request the responsible contact to gather all relevant data and complete the GCI questionnaire online. (cmcgaza.ps, 2022)

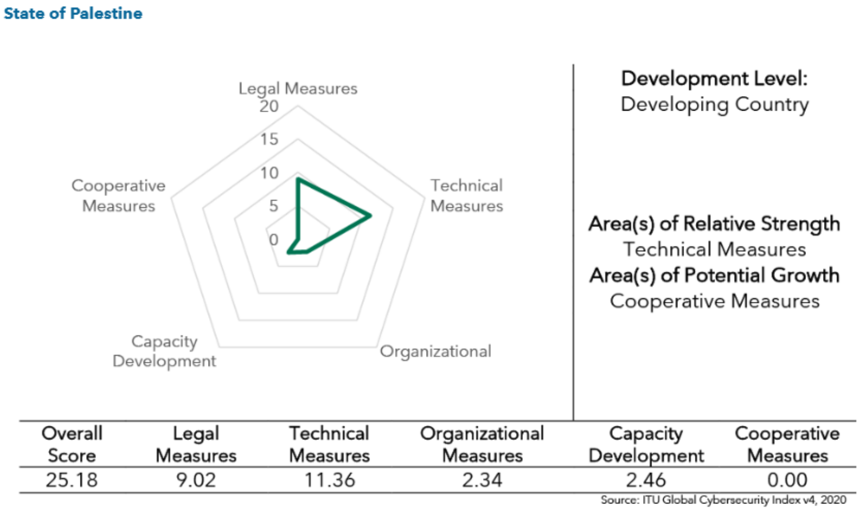
The main pillars of the Global Cybersecurity Index (GCI) include:

- Legal measures
- Technical measures
- Organizational measures
- Capacity development measures
- Cooperation measures

Table 2: Global Cybersecurity Index for Arab Countries



Country Name	Overall Score	Regional Rank
Saudi Arabia	99.54	1
United Arab Emirates	98.06	2
Oman	96.04	3
Egypt	95.48	4
Qatar	94.5	5
Tunisia	86.23	6
Morocco	82.41	7
Bahrain	77.86	8
Kuwait	75.05	9
Jordan	70.96	10
Sudan	35.03	11
Algeria	33.95	12
Lebanon**	30.44	13
Libya	28.78	14
State of Palestine	25.18	15
Syrian Arab Republic**	22.14	16
Iraq**	20.71	17
Mauritania	18.94	18
Somalia	17.25	19
Comoros**	3.72	20
Djibouti	1.73	21
Yemen*	0	22



Development Level:
Developing Country

Area(s) of Relative Strength
Technical Measures
Area(s) of Potential Growth
Cooperative Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
25.18	9.02	11.36	2.34	2.46	0.00

Source: ITU Global Cybersecurity Index v4, 2020

Figure 2: Palestine's profile in the Global Cybersecurity Report 4 (ITU Publications, 2021)

The adoption of these indicators in member countries facilitates global cooperation and supports:

- Discussions through formally established forums that enable self-assessment and better coordination.
- Gathering insights on comprehensive national initiatives and resources used to manage cybersecurity at the national level.
- Comparison with best practices and regional partners and neighbours.

- Raising awareness among various stakeholders about the need for coordination at the national level.

See the ranking of Arab countries by the Global Cybersecurity Index in Table 2.

These assessments help identify gaps in cybersecurity development within nations and regions, as well as raise awareness of which countries most need support regarding cybersecurity worldwide. This assessment also aids in improving their cybersecurity posture. Through data collection, the GCI highlights practice that member states can adopt that suit their national environments, encouraging good practices and building a global cybersecurity culture.

The GCI assessment also helps identify the relative strengths and weaknesses in member states' cybersecurity commitments, informing them of areas where they may need additional support in capacity building, or areas where they can provide support to others. For example, the ITU can identify educational needs in cybersecurity within the educational systems of its members through the GCI assessment (Arabic_GOAT.pdf, 2021). See Palestine's profile and the five pillars in Figure (2).

3. Challenges Facing the Establishment of a Palestinian Cybersecurity System

The Palestinian legislative and regulatory system, similar to other Arab countries, is experiencing slow progress. This makes it lacking in many sensitive aspects of the cyber space. Many threat cases are addressed by activating punitive measures, such as adding new provisions or amending existing laws. This approach contradicts global guidelines on flexibility and development. There is an imbalance in human resources between the existing scarcity of qualified personnel to cover deficiencies and the needs arising from the rapid technological advancements. The mechanisms employed for implementing security measures in the technological world are not suitable and do not meet global standards. The statistics available from the International Telecommunication Union (ITU) are undeniable evidence of this issue, highlighting the bureaucratic difficulties and obstacles. This discrepancy is evident when comparing the global metrics between developed countries and the third world, painting a clear picture of the absence of international cooperation. The lack of serious internal cooperation, as reflected in the statistics reported by security agencies on the increasing rate of cyber breaches, indicates an inability of coordination bodies to manage the cybersecurity portfolio effectively.

Given the above, cybersecurity strategy has become a top priority for countries, as social networks and the internet have quickly become fundamental pillars of economic, social, and cultural activities worldwide. This shift necessitates a redefinition of traditional strategies to adapt to these changes.

Therefore, it is crucial to expedite the development of a comprehensive Palestinian national strategy. This strategy should promote a culture of risk management among technology users in both the public and private sectors, enabling them to engage with practical and security measures to combat cyber attackers. This includes organizing training courses on the correct applications of the information revolution according to international standards recommended by the ITU, with the involvement of all stakeholders in the security and information sectors.

However, implementing this strategy faces several obstacles. The most challenging aspect is the ever-evolving nature of security threats, compounded by the lack of a timeline for implementing the strategy and the absence of specific budgets and resources necessary for its success. Additionally, there is a widespread lack of awareness about information security among a large segment of citizens and public and private sector employees, who are considered the weakest link in the information system despite the presence of advanced protection systems. This gap will exacerbate the problem of threats and cyber breaches.

3. Key Arab, Regional, and Global Experiences

The Arab Regional Cybersecurity Center

The Arab Regional Cybersecurity Center (ITU-ARCC) was established by the International Telecommunication Union (ITU) and the Sultanate of Oman, represented by the Ministry of Technology and Communications (formerly the Information Technology Authority), in December 2012. Its vision is to create a more secure and cooperative cybersecurity environment in the Arab region and to enhance the role of the ITU in building trust and security in the use of information and communication technologies in the region. In line with the ITU's Global Cybersecurity Agenda, the official launch of the regional center took place on March 3, 2013, at the Knowledge Oasis Muscat.

Objectives:

- Oversee the implementation of the ITU's general cybersecurity program across the Arab region.
- Respond to cybersecurity requirements amidst the latest developments.
- Serve as a management hub and platform for achieving cybersecurity objectives.
- Provide a unified center for member states to manage cybersecurity initiative programs.
- Develop frameworks and plans in cybersecurity through conducting regional studies and workshops.
- Raise awareness and expertise in cybersecurity within the information infrastructure sector.

Mission: The mission of the center is to create a more secure and cooperative cybersecurity environment in the Arab region and to enhance the ITU's role in building trust and security in the use of information and communication technologies in the Arab region.

Vision: To be recognized as a leading reference center for cybersecurity in the Arab region.

Services Provided by the Center (Service Guide):

1. Cybersecurity Strategy and Governance: Experts at the Arab Regional Cybersecurity Center work closely with the public and private sectors to develop

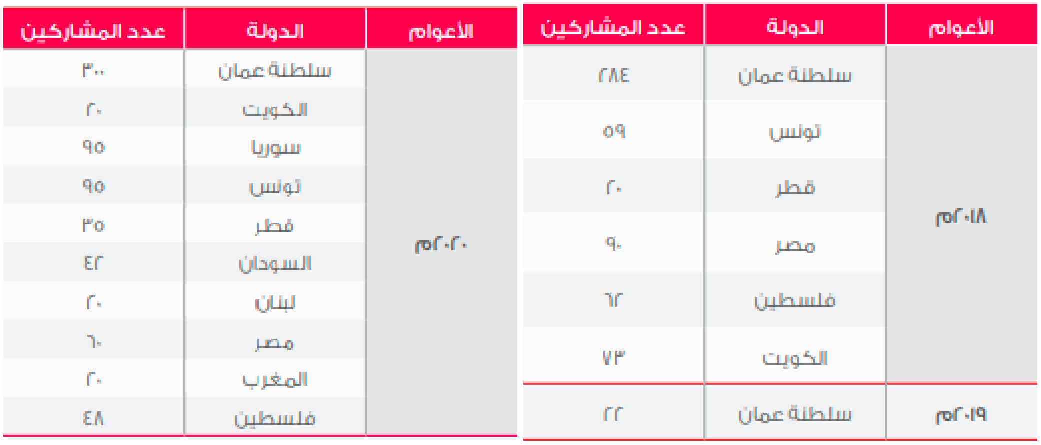
national cybersecurity strategies with clear responsibilities. These strategies include effective programs to enhance cybersecurity capabilities and address gaps in the cybersecurity environment (e.g., National Cybersecurity Strategy, Legal Work Strategy and Policies, Online Child Protection Strategy, Protection of Critical National Information Infrastructure).

2. Cybersecurity Assurance and Techniques: The cybersecurity assurance services aim to provide technical measures and compliance with standards. Experts at the Arab Regional Cybersecurity Center use global technical standards such as ISO 27001, which enable member states to identify areas that need security improvement (e.g., Digital Evidence Lab, Cybersecurity Assessment, Threat Alert and Notification Service, Cybersecurity Competitions, Malware Analysis Lab).
3. Cybersecurity Capacity Building: Capacity-building in cybersecurity helps organizations build institutional cybersecurity capabilities and develop effective solutions and programs (e.g., Cybersecurity Training Courses and Workshops, Cybersecurity Conferences and Seminars, Cybersecurity Awareness Sessions).
4. Cyber Incident Management: The Arab Regional Cybersecurity Center team collaborates with partners to assist and encourage ITU member states in establishing national emergency response teams for security incidents. These teams take on a national responsibility to act as a trusted coordination center for cybersecurity efforts. This service also helps assess the capabilities of security incident response teams in governments and the public sector, identify gaps, and provide a roadmap for improving these teams (e.g., Assessment of Emergency Response Centers and Security Incident Teams, Establishing Emergency Response and Security Incident Teams, Readiness Assessment for Establishing Emergency Response Teams, Cyber Exercises).

Target Countries: All Arab countries, including Palestine (arcc.om, 2022)

In its latest report, which reviewed the achievements of the centre from 2018 to 2020, the Arab Regional Cybersecurity Centre organized several events over three years, from 2018 to 2020. These events included various competitions aimed at qualifying national cadres, honing their skills in the field of cybersecurity, and enhancing their capabilities to compete at the regional and international levels. Among the most significant competitions were:

- Vulnerability Hunter Competition in partnership with Silensec. This competition is organized in some member countries of the centre, after which the winners from each country qualify for the regional competition. At the local level in each country, including Palestine, the competition was organized as follows:



عدد المشاركين	الدولة	الأعوام
٢٨٤	سلطنة عمان	٢٠١٨م
٥٩	تونس	
٢٠	قطر	
٩٠	مصر	
٦٢	فلسطين	
٧٣	الكويت	
٢٢	سلطنة عمان	٢٠١٩م

عدد المشاركين	الدولة	الأعوام
٣٠٠	سلطنة عمان	٢٠٢٠م
٢٠	الكويت	
٩٥	سوريا	
٩٥	تونس	
٣٥	قطر	
٤٢	السودان	
٢٠	لبنان	
٦٠	مصر	
٢٠	المغرب	
٤٨	فلسطين	

Figure 3: Palestine’s participation in the Threat Hunter competition

The centre organized regional Bug Bounty competitions as follows:

- 2018: Participated by 10 Arab countries: Oman, Tunisia, Egypt, Kuwait, Qatar, Libya, Palestine, Jordan, Algeria, and Saudi Arabia.
- 2019: Participated by 7 Arab countries: Oman, Tunisia, Kuwait, Libya, Palestine, Lebanon, and Sudan.
- 2020: Participated by 10 Arab countries: Oman, Kuwait, Egypt, Qatar, Palestine, Syria, Sudan, Tunisia, Morocco, and Lebanon. The 2020 edition was distinguished by the development of scenarios simulating the security challenges arising from the COVID-19 pandemic in the field of cybersecurity. This was aimed at preparing the next generation of cybersecurity enthusiasts and professionals and enhancing their abilities to compete at regional and international levels. The competition focused on several questions and challenges in various cybersecurity fields, including ethical hacking, protecting critical information and communication systems, malware analysis, and digital forensics.

Additionally, the centre contributed to the establishment of the PALCERT Cyber Incident Response Team Centre for Palestine, and assisted in training specialists in the Palestinian Ministry of Communications and Information Technology to provide initial security incident response services for institutions and departments. The centre conducted workshops and training courses to build capacity and enhance the readiness of the cybersecurity incident response team. The training included several core aspects, such as: emergency and cybersecurity incident response training, implementing, reviewing, and testing tools necessary for the centre’s operation, improving threat anticipation and identification, and developing solutions for beneficiary institutions. It also involved ensuring the effective operation of the centre by building a high-efficiency response system for addressing cybersecurity threats, increasing the ability to confirm the effectiveness of security measures and controls, and readiness for rapid response to security incidents. Training also covered implementing, reviewing, and testing processes and procedures for emergency and cybersecurity incident response centres. (ARCC-AR-LAYOUT(N)-A-1.pdf, 2021)

Arab Vision for Cybersecurity

Amid the rapid digital developments witnessed by the global economy, Arab countries have begun transitioning from traditional to digital economies. Some countries have made significant progress in digitizing various fields and sectors. A study published by the Arab Monetary Fund in 2020 indicated that the digital economy, for example, has reduced the cost of providing government services by up to 88% in some countries, while others are still slowly engaging in digital transformations. The digital divide is expected to widen the economic gap between countries in the region.

In light of this, cybersecurity has become a strategic priority for Arab countries. The openness of cyberspace to its surroundings has increasingly posed numerous challenges, especially as cybercrime relies on the latest technologies (artificial intelligence, Internet of Things).

Despite the varying states of Arab countries in adopting national cybersecurity strategies and related legislations, several initiatives have emerged at the level of Arab joint action within various organizational and institutional frameworks. These initiatives aim to support and contribute to implementing the outcomes of an Arab cybersecurity vision, particularly its action plan. One of the most significant of these initiatives is the ratification within the framework of the Arab League of the Arab Convention on Combating Information Technology Crimes dated December 21, 2010. Several Arab member states ratified this convention, which entered into force on February 6, 2014. Palestine was among the first countries to ratify this convention. The convention aims to enhance and support cooperation among Arab countries in combating information technology crimes to safeguard the security of Arab states, their interests, communities, and individuals. It provides a framework for investigating and prosecuting these crimes. The following acts are listed as information technology crimes:

- Unauthorized access to all or part of information technology or continuing such access.
- Attacking the integrity and confidentiality of information by intentionally destroying, deleting, impairing, modifying, or concealing data without legal justification.
- Misusing information technology by producing, selling, importing, distributing, providing, or possessing tools or programs designed for committing IT crimes or breaking passwords or access codes.
- Forgery using information technology to alter the truth in data.
- Fraud to achieve benefits unlawfully using information technology for oneself or others.
- Pornography by producing, displaying, distributing, publishing, purchasing, selling, or importing pornographic materials using information technology.
- Terrorism by spreading the ideas and principles of terrorist groups, advocating for them, funding terrorist operations, training on them, publishing methods for making explosives, spreading sectarianism and strife, and attacking religions and beliefs.

- Money laundering or requesting assistance or publishing methods for money laundering, promoting drugs and their types, trafficking in humans, human organs, and weapons.
- Copyright infringement.
- Unlawful use of electronic tools.
- Attempting or participating in committing crimes.

Here is the link to the Arab Convention on Combating Cybercrime. (lasportal.org, 2010), and Figure 4 shows the countries that signed this convention, including Palestine.

Not all cyber-attacks are criminalized in some countries' penal laws, despite the damages they cause. In some cases, they are considered merely inappropriate behavior that requires cyber safety plans. When these actions are partially criminalized, such disturbances are classified as cybercrimes and necessitate a national plan to combat cybercrime. If attacks escalate to threaten national security, a cybersecurity strategy is required to ensure a reliable and secure cyber space, enabling the country to confront attacks on data and systems.

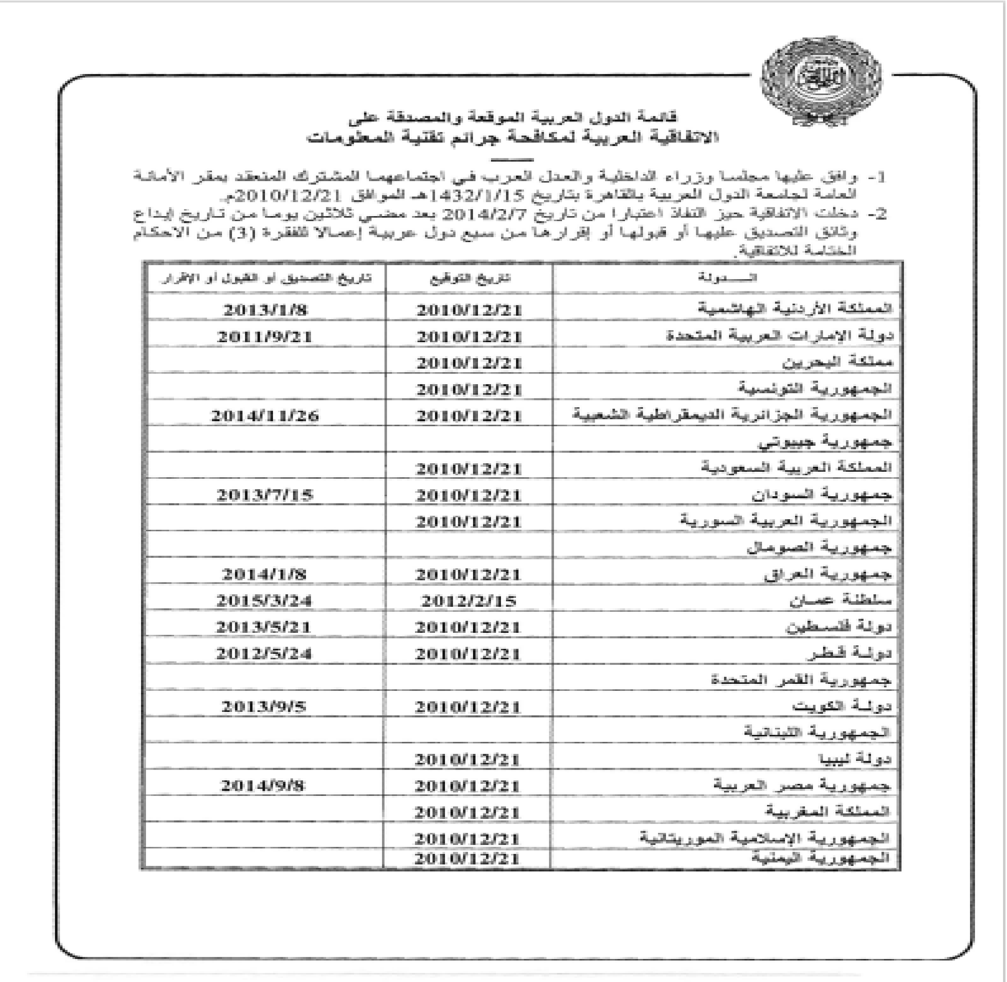
The lack of a universally accepted definition of cybersecurity, the overlap between information security and cybersecurity, and the similar ambiguities in the titles of leadership roles typically associated with cybersecurity in organizational contexts have caused confusion within the United Nations system. (jiu_rep_2021_3_arabic.pdf (unjiu.org), 2021)

Global Cybersecurity Policies and Practices

As examples of cybersecurity policies from non-Arab countries, consider the following:

- The UK's 2011 strategy classified cybersecurity as a national security priority by establishing a Cyber Incident Response Center and a National Cyber Crime Unit, creating partnerships with institutions, supporting the software and hardware industry for cybersecurity, and collaborating with other countries to identify and manage cyber risks. The National Cyber Security Strategy 2011 made significant improvements in the UK's cybersecurity. It achieved important results by looking to the market to promote safe online behaviors. However, this approach did not achieve the scale and pace of change required to stay ahead of rapidly evolving threats. Consequently, an updated version of the strategy was issued for 2016 to 2021.

The 2021 vision was for the UK to be secure from cyber threats and resilient in the face of them, thriving and confident in the digital world. To achieve this vision, the strategy aimed to accomplish the following goals: defense, deterrence, and development. The strategy covered the entire UK. The UK government sought to ensure the implementation of the strategy across the country and will make significant improvements to national information security in the future. This ambitious development program will focus on four main areas: enablers and incentives, expanded intelligence work and law enforcement focus on threats, and technology development and usage. (GOV.UK (www.gov.uk), 2016)



قائمة الدول العربية الموقعة والمصدقة على
الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

1- وافق عليها مجلسا وزراء الداخلية والعدل العرب في اجتماعهما المشترك المنعقد بمقر الأمانة العامة لجامعة الدول العربية بالقاهرة بتاريخ 1432/1/15هـ الموافق 2010/12/21م.

2- دخلت الاتفاقية حيز النفاذ اعتبارا من تاريخ 2014/2/7 بعد مضي ثلاثين يوما من تاريخ إيداع وثائق التصديق عليها أو قبولها أو إقرارها من سبع دول عربية إعمالا للفقرة (3) من الاحكام الختامية للاتفاقية.

تاريخ التصديق او القبول او الإقرار	تاريخ التوقيع	الـــدولة
2013/1/8	2010/12/21	المملكة الأردنية الهاشمية
2011/9/21	2010/12/21	دولة الإمارات العربية المتحدة
	2010/12/21	مملكة البحرين
	2010/12/21	الجمهورية التونسية
2014/11/26	2010/12/21	الجمهورية الجزائرية الديمقراطية الشعبية
		جمهورية جيبوتي
	2010/12/21	المملكة العربية السعودية
2013/7/15	2010/12/21	جمهورية السودان
	2010/12/21	الجمهورية العربية السورية
		جمهورية الصومال
2014/1/8	2010/12/21	جمهورية العراق
2015/3/24	2012/2/15	سلطنة عمان
2013/5/21	2010/12/21	دولة فلسطين
2012/5/24	2010/12/21	دولة قطر
		جمهورية القمر المتحدة
2013/9/5	2010/12/21	دولة الكويت
		الجمهورية اللبنانية
	2010/12/21	دولة ليبيا
2014/9/8	2010/12/21	جمهورية مصر العربية
	2010/12/21	المملكة المغربية
	2010/12/21	الجمهورية الإسلامية الموريتانية
	2010/12/21	الجمهورية اليمنية

Figure 4: The State of Palestine signing the Arab Convention on Combating Information Technology Crimes. (Ratification of the Arab Convention on Combating Information Technology Crimes.pdf (lasportal.org), 2010)

•	Regarding the Russian experience, improvements have been made to the Russian cybersecurity strategy by integrating cybersecurity into the new National Security Strategy for 2021, replacing the previous 2015 strategy. Key aspects concerning information security in the new strategy include:

o	The rapid development of information and communication technologies increases the likelihood of risks to the security of citizens, society, and the state.

o	The expanded use of information and communication technologies to interfere in the affairs of states and undermine their sovereignty and territorial integrity poses a threat to international security and peace.

o	An increase in attacks on Russian information resources, most of which are carried out from abroad.

o	Russian initiatives aimed at ensuring international information security face opposition from foreign countries seeking dominance in the global information space.

o Foreign intelligence agencies are intensifying their activities to carry out operations in Russia's information domain.

o Russia faces disinformation and disruptive campaigns on the internet, primarily targeting the youth (including false news about the risk of terrorist attacks, calls for suicide, dissemination of extremist materials, incitement to commit illegal acts, and drug promotion).

o Major international companies seek to establish monopolies on the internet and control all information resources by imposing illegal censorship and closing alternative information resources.

o Internet users face attempts to impose distorted views on historical facts and developments in Russia and the world for political reasons.

o The use of foreign information and communication technologies in Russia increases the risk of foreign attempts to influence the country’s information resources.

o The goal of ensuring Russia’s information security is to strengthen the country’s sovereignty in the information domain. ("Cybersecurity" as a key aspect of the new Russian National Security Strategy - RT Arabic, 2021) The original strategy text is available at (pravo.gov.ru, 2021).

o The American Experience: The United States is among the first countries to address cybersecurity as a strategic mission to counter the growing threat to an economy increasingly reliant on information and communication technologies. This prompted the U.S. presidential administration to work on providing cybersecurity defenses and redefining the mission of ensuring the security of critical infrastructure. An integrated approach was formulated in 2003 under a comprehensive strategy known as the "National Strategy to Protect the Cybersecurity Space," which distributed responsibility for ensuring cybersecurity among federal agencies, with the Department of Homeland Security being the coordinating authority. It relied on four pillars: protecting the American people, homeland, and way of life; enhancing American prosperity; preserving peace through strength; and advancing American influence.

The U.S. Department of Defense and law enforcement agencies developed threat and attack detection systems to ensure timely and effective responses, while the Department of State worked on international cooperation on all cybersecurity issues. It emphasized the need for a cooperative international environment among countries sharing a common vision on issues like technical standards, legal standards regarding territorial jurisdiction, sovereign responsibility, and the use of force. In 2008, a new transitional phase in cybersecurity development began, aimed at addressing inherent cybersecurity problems with a slightly adjusted and moderated implementation approach. (annabaa.org, 2018) The original strategy text can be found at 01_letter-toc.qxd (itu.int, 2003).

Subsequent policy reviews in 2009 and 2014 added improvements to the original strategy, focusing on reliable and resilient information and communication infrastructure (itu.int, 2009). The 2015 Cybersecurity Strategy introduced clear enhancements and new measures (web.pdf (itu.int, 2015)). The 2018 strategy highlighted the role of the Department of Defense in mitigating the serious and growing threat posed by harmful cyber actors to U.S. national security. "The Department of Defense is prepared, as part of the whole-of-government approach outlined in the National Cyber Strategy, to preserve peace through strength by identifying, countering, disrupting, and deterring destabilizing behavior in cyberspace that conflicts with the United States. The National Cyber Strategy will enhance an open and secure internet by encouraging other nations to promote internet freedom and strengthening the multi-stakeholder model of internet governance. It will also bolster open, interoperable, reliable, and secure communications infrastructure while opening foreign markets to U.S. expertise and building international cybersecurity capabilities." (jcs.mil, 2018)

In 2018, the Department of Defense adopted the "Defense Forward" strategy, a proactive offensive approach. This strategy was considered successful, preventing interference in the 2018 and 2020 congressional elections, although it failed to detect some breaches, which most intelligence estimates attribute to Russia. The strategy noted that the era of the internet has created new opportunities and challenges for successive U.S. governments, making access to verified information a vital interest for the United States (aljazeera.net, 2020). The Pentagon’s cybersecurity strategy focuses on five key areas:

- Ensuring U.S. cybersecurity forces can perform their missions in a hazardous cyberspace environment.
- Enhancing the capabilities of cybersecurity forces to conduct operations that strengthen U.S. military advantages.
- Defending critical U.S. infrastructure from any cyber-attacks.
- Securing information, systems, and networks of the Pentagon against any cyber-attacks.
- Expanding cybersecurity cooperation with partners in both the private sector and internationally.

The strategy emphasizes the high cost to U.S. adversaries of engaging in malicious or harmful cyber espionage activities. (Summary of the 2018 National Defense Strategy, 2018)

Regional Challenges in Cybersecurity

In addition to local challenges, regional challenges have emerged in this evolving and dynamic field based on regional events. These challenges include: the widespread adoption of information and communication technology, the dependence of most human activities on technology, the availability of advanced devices that enable criminals to commit their crimes, the weakness of internet monitoring mechanisms, and in the Arab region specifically, key strategic challenges include: weak regulatory and legal frameworks, difficulties in warning users in a timely manner about potential cybersecurity threats and incidents, low awareness of cybersecurity risks, and a lack of statistics and studies on cybercrime. (Cybersecurity and Combatting Cybercrime in the Arab Region: Policy Recommendations - unescwa.org, 2015).

4. Conclusions and Summary

Developing a comprehensive national cybersecurity strategy for Palestine requires the concerted efforts of government, private sector, and civil society, with a clear set of principles and vision. The strategy should be holistic and tailored to the country's conditions and priorities. As emphasized by the International Telecommunication Union in its guide on strategic cybersecurity planning, the strategy should promote economic and social prosperity and sustainability, leveraging information and communication technologies for sustainable development in Palestine. It must undoubtedly adhere to fundamental human rights and be consistent with them, allowing for effective management to avoid cybersecurity risks and issues. Additionally, the strategy should utilize available tools and policies to achieve its goals, considering the unique conditions of the country under occupation. The strategy should be established at the highest level of government to play a crucial role in defining relevant responsibilities and roles and allocating adequate human and financial resources. It should help build a digital environment that citizens and organizations can trust. (The Guide - NCS guide, 2020)

Guide to Developing a National Cybersecurity Strategy:

Based on the study of experiences from Arab, regional, and international countries, a guide for developing a national cybersecurity strategy can be established, drawing on the guidance provided in the International Telecommunication Union's guide (The Guide - NCS guide, 2020). The objective is to "provide a useful, flexible, and easy-to-use framework for defining the country's social-economic context, current security posture, and to assist policymakers in crafting a strategy that takes into account the country's specific situation, cultural and societal values, and to encourage achieving security, resilience, and development of connected communities empowered by information and communication technologies."

The guide indicates that "developing and implementing a national cybersecurity strategy can help a country improve the security of its digital infrastructure and ultimately contribute to achieving its broader social and economic aspirations." Based on existing research in this field, the guide encourages stakeholders to consider a national cybersecurity strategy as follows:

- It should include the vision, objectives, principles, and priorities that guide the country in handling cybersecurity.
- It should define the stakeholders, their roles, and responsibilities.
- It should describe the steps, programs, and initiatives that the country will undertake to protect its national electronic infrastructure while increasing its security and resilience.

See Figure 5 (The Guide - NCS guide, 2020).

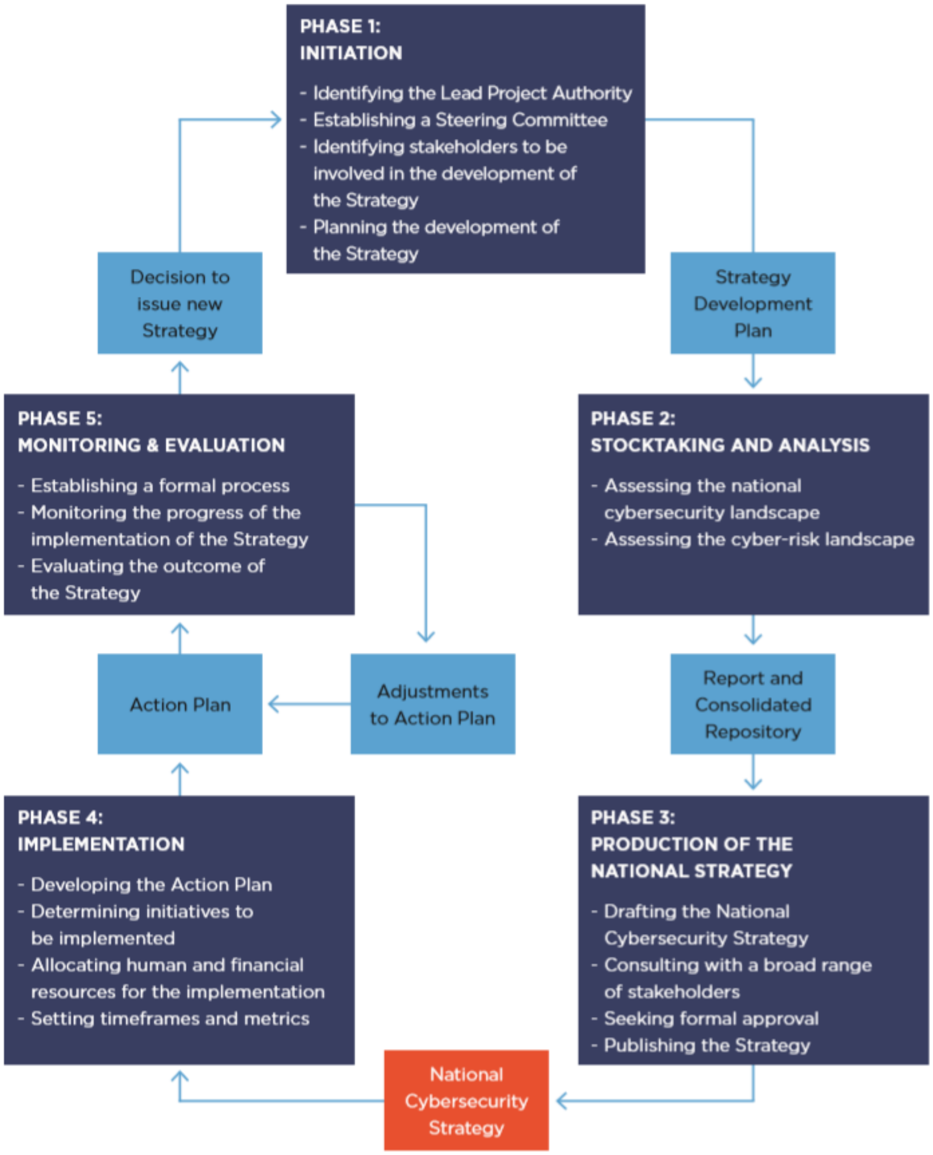

PHASE 1:
INITIATION
- Identifying the Lead Project Authority
- Establishing a Steering Committee
- Identifying stakeholders to be involved in the development of the Strategy
- Planning the development of the Strategy
Decision to issue new Strategy
Strategy Development Plan
PHASE 5:
MONITORING & EVALUATION
- Establishing a formal process
- Monitoring the progress of the implementation of the Strategy
- Evaluating the outcome of the Strategy
PHASE 2:
STOCKTAKING AND ANALYSIS
- Assessing the national cybersecurity landscape
- Assessing the cyber-risk landscape
Action Plan
Adjustments to Action Plan
Report and Consolidated Repository
PHASE 4:
IMPLEMENTATION
- Developing the Action Plan
- Determining initiatives to be implemented
- Allocating human and financial resources for the implementation
- Setting timeframes and metrics
PHASE 3:
PRODUCTION OF THE NATIONAL STRATEGY
- Drafting the National Cybersecurity Strategy
- Consulting with a broad range of stakeholders
- Seeking formal approval
- Publishing the Strategy
National Cybersecurity Strategy

Figure 5: Steps to formulate a national cybersecurity strategy.

5. The Recommendations

Countries in the region face severe weaknesses in crisis response and management capabilities and in adopting a national strategy for digital resilience. To address these obstacles and overcome the previously mentioned challenges, the following recommendations are proposed:

1. Information Sharing: Activate provisions related to information exchange and technical assistance, which are general principles adopted by many international instruments.
2. Exchange of Expertise and Technical Assistance: Conduct training courses and consultative meetings in areas covered by criminal policy for combating crime in

general. Benefit from the experiences of some Arab countries, learn about their legislative environments, and understand the technical mechanisms and human resources deployed for cybersecurity.

3. Adopt Successful Regional Experiences: Transfer successful Arab and European experiences in adopting national cybersecurity policies and relevant legislation, such as the General Data Protection Regulation (GDPR). Consider adopting similar regulations in the region.

4. Establish an Alliance: Create a coalition that brings together European Union countries and Arab states around cybersecurity capabilities. This alliance should include Computer Emergency Response Teams (CERTs) to facilitate training, capacity building, and information exchange.

5. Develop Palestinian Cybersecurity Legislation: Update Palestinian cybersecurity legislation in line with technological advancements to build a knowledge-based society. Close all potential security and threat gaps, facilitate transactions across all sectors, promote internal and external integration, and enhance actual cooperation to address risks and reduce cybercrime.

6. Join International Agreements: Accede to international agreements on the protection of information systems, such as the Budapest Convention, to encourage coordination and cooperation with experts and institutions in the field of cybersecurity at both regional and international levels. These recommendations aim to improve regional cybersecurity resilience, facilitate effective responses to cyber threats, and enhance collaboration and legislative frameworks to safeguard information systems and digital infrastructures.

References

1. Sari Ghadban Ghaidan and Muhammad Munther Jalal Al-Rubaie: Cybersecurity and International Confrontation Policies, Journal of Strategic and Military Studies, issued by the Arab Democratic Center, Volume 2, Issue 9, December 2020.

2. Sheikha Hassani Al-Zahrain: International Cooperation in Confronting Cyber Attacks, Sharjah University Journal, Volume 17, Issue 1, June 2020.

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

4. Dr. Musa: Cybersecurity is a national security issue (mtit.gov.ps), 2018, https://www.mtit.gov.ps/index.php/c_home/showNew/2118

5. Cabinet Resolution No. (16) of 2015 on the internal regulations of the Palestinian Computer Emergency Response Team - Qanon website (qanon.ps), 2015, http://qanon.ps/news.php?action=view&id=22749

6. It is no longer a secret: Palestine needs Cyber Hygiene - Community Media Center (cmcgaza.ps), 2022, https://cmcgaza.ps/ar/?p=5010

7. The Palestinian Strategy for Cybersecurity, Cyber Unemployment and the Employment Path (maannews.net), 2022, https://www.maannews.net/articles/2064517.html

8. Definition of Cybersecurity Safety And its checklist (kaspersky.com), 2021, https://me.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits

9. The Cabinet decides to establish the National Cybersecurity Authority and assigns a government team to prepare for it | PNN, 2022, https://pnn.ps/news/666105

10. Plenipotentiary Conferences (itu.int), 2018, https://www.itu.int/en/history/Pages/PlenipotentiaryConferences.aspx?conf=4.444#:~:text=29%20October%20to%2016%20November%202018%20%2D%20Dubai%2C%20United%20Arab%20Emirates&text=ITU's%2020th%20Plenipotentiary%20Conference%20(PP,2300%20participants%20from%20180%20countries

11. Final Documents of the Plenipotentiary Conference (Dubai, 2018) (itu.int), 2018, https://search.itu.int/history/HistoryDigitalCollectionDocLibrary/4.444.43.ar.400.pdf

12. Arabic_GOAT.pdf (cybilportal.org), 2021, https://cybilportal.org/wp-content/uploads/2021/12/Arabic_GOAT.pdf

13. 512525A.pdf (itu.int), 2022, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/512525A.pdf

14. International Telecommunication Union (ITU), World Bank, Commonwealth Secretariat (ComSec), Commonwealth Telecommunications Organization (CTO), and NATO Cooperative Centre of Excellence for Cyber Defence (COE CCD NATO) 2020. A Guide to Developing a National Cybersecurity Strategy Cyber - A strategic commitment to cybersecurity. The Guide - NCS guide, 2020, https://ncsguide.org/the-guide/

15. jiu_rep_2021_3_arabic.pdf (unjiu.org), 2021, https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_arabic.pdf

16. Cybersecurity and Combating Cybercrime in the Arab Region Policy Recommendations (unescwa.org), 2015, https://archive.unescwa.org/sites/www.unescwa.org/files/publications/files/policy-recommendations-cybersafety-arab-region-arabic.pdf

17. America and the Cyber Strategy (annabaa.org), 2018, https://annabaa.org/arabic/informatics/17712

18. How the Strategy Failed “Defending Forward” in Protecting America from Cyber Attacks? | Politics News | Al Jazeera Net (aljazeera.net), 2020, https://www.aljazeera.net/politics/2020/12/19/%D9%83%D9%8A%D9%81-

%D9%81%D8%B4%D9%84%D8%AA-%D8%A5%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A9-%D8%A7%D9%84%D8%AF%D9%81%D8%A7%D8%B9-%D9%84%D9%84%D8%A3%D9%85%D8%A7%D9%85-%D9%81%D9%8A

19. “Cybersecurity” is among the most prominent items of the strategy Russia's New National Security - RT Arabic, 2021, https://arabic.rt.com/russia/1248067-%D8%A7%D8%B3%D8%AA%D8%B1%D8%A7%D8%AA%D9%8A%D8%AC%D9%8A%D8%A9-%D8%A3%D9%85%D9%86-%D9%82%D9%88%D9%85%D9%8A-%D8%B1%D9%88%D8%B3%D9%8A%D8%A9-%D8%A3%D9%85%D9%86-%D9%85%D8%B9%D9%84%D9%88%D9%85%D8%A7%D8%AA/#

20. ARCC-AR-LAYOUT(N)-A-1.pdf, 2021, https://arcc.om/files/ARCC-AR-LAYOUT(N)-A-1.pdf

21. Arab Regional Cybersecurity Center (arcc.om), 2022, https://arcc.om/

22. What is Cyber Hygiene and Why is It Important? (techtarget.com), 2022, https://www.techtarget.com/searchsecurity/definition/cyber-hygiene

23. Cyber Hygiene: Definition & Best Practices | Okta, 2022, https://www.okta.com/identity-101/cyber-hygiene/

24. Decree of the President of the Russian Federation dated 02.07.2021 No. 400 · Official publication of legal acts · Official Internet portal of legal inf. (pravo.gov.ru) 2021, publication.pravo.gov.ru/Document/View/0001202107030001?index=1&rangeSize=1

25. National Cyber Security Strategy 2016 to 2021 - GOV.UK (www.gov.uk), 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

26. Summary of the 2018 National Defense Strategy, 2018, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf

27. White House Releases First National Cyber Strategy in 15 Years > Joint Chiefs of Staff > News Display (jcs.mil), 2018, https://www.jcs.mil/Media/News/News-Display/Article/1643010/white-house-releases-first-national-cyber-strategy-in-15-years/

28. UnitedStates_2015_Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (itu.int), 2015, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/UnitedStates_2015_Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

29. Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (itu.int), 2009, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/UnitedStates_2009_Cyberspace_Policy_Review_final_0.pdf

30. 01_letter-toc.qxd (itu.int), 2003, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/UnitedStates_2003_cyberspace_strategy.pdf

31. ITU Publications, 2021, https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E.

32. National Cybersecurity Strategies Repository (itu.int), 2022, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

33. Chart: A Minute on the Internet in 2021 | Statista, 2021, https://www.statista.com/chart/25443/estimated-amount-of-data-created-on-the-internet-in-one-minute/

34.https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf, 2022

35. Full list (coe.int), 2001, https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185