ARAB
CYBERSECURITY
VISION

# THE ARAB VISION FOR CYBERSECURITY

## Reality - Challenges - Opportunities

## ARAB LEAGUE SECRETARY-GENERAL

The subject of data security has recently witnessed important developments at the international level... The United Nations has established an open-ended committee to elaborate a comprehensive international convention against the criminal use of technology... It is a committee that will soon begin its work... As Arabs, we should actively participate in its work to protect and .defend our rights

In the same context, at the previous session of the High Coordination Committee, we had set up a working group to develop a unified Arab framework to counter cyber piracy and protection of networks... We also called .. for the organization of an Arab forum to discuss Cybersecurity challenges... and I'm looking forward for it to be held as soon as possible, and I hope that all Member States and institutions of joint Arab action will .participate actively on it

**Extract from Mr. Ahmed Abu Gheit Speech**
**Arab League Secretary-General**
**(Opening Ceremony works of the Session (51**
**of the High Coordination Committee for Joint Arab Action -**
**New Alamein City: 8/7/2021**

## GENERAL DIRECTOR OF THE ARAB ICT ORGANIZATION -AICTO

For years, the world has been living on the impact of the digital revolution, known as the Fourth Industrial Revolution, which has opened the door to the infinite possibilities of access to knowledge and the provision of services through many technological trends that evolve day after day: artificial intelligence, robotics, 3D ,Internet of Things, self-driving vehicles printing, nanotechnology, biotechnology, satellite navigation technology, Blockchain, .etc

and the spread of 2020 With the onset of the Corona pandemic at the global level, the leading role of technology in our lives has strengthened and has become the vital factor, almost the only one, for decoupling people and sustaining many economic sectors: education, employment, transportation, health, etc. Thus, the transition to digital solutions at all levels has become necessary and not an option to deal with this health crisis and reduce its negative .effects

Our Arab States were not immune from these global developments and changes. They were obliged to impose preventive measures, sometimes strict, and most Arab States were obliged to harness all their potential to curb the spread of the crisis. We have seen a major transition to digital services and solutions in many States, both ready and not ready, which .has compounded cyber threats and risks

Today, after our experience with the Corona pandemic, we must acknowledge that we are living in a rapidly changing world that can be described as VUCA World Volatile, Uncertain, Complex and Ambiguous. In this world, the old rules no longer apply. In order to keep up with the pace, the Arab States must be able to predict the future and adapt to variables at the same pace, with flexibility, particularly in the design and implementation of policies, especially in the technological and digital .sectors

At this point, we cannot address the issue of digital economy or the transition to digital societies without considering that Cybersecurity is one of the key elements supporting the successful building of a strong .digital economy within any State

In this context, and aware that addressing the ever-increasing cyber risks is necessary to join efforts at the Arab and regional levels to find comprehensive solutions that will serve all, the Arab Organization for Communication and Information Technologies (AICT), in January 20 of 56 accordance with resolution of the Arab Development Summit, has 2019 taken the initiative to formulate a "Unified Arab Vision for Cybersecurity". This took place within the framework of our contribution to the promotion of joint Arab action and assistance to Arab States to work in a complementary and participatory manner in a way that ensures the prosperity and advancement of our Arab .States in the digital area

We thank the League of Arab States for its support in this initiative. We hope that this «Unified Arab Vision for Cybersecurity» will serve as a starting point for joint Arab Cybersecurity strategies and initiatives, especially that the region has so much human potential in this area as well as successful .experiences at the global level

**Let›s work together for a secure Arab» «digital society**
**Engineer/Mohamed Ben Amor**
**General Director**
**of the Arab ICT Organization -AICTO**

## MINISTER OF COMMUNICATION TECHNOLOGIES REPUBLIC OF TUNISIA

In recent years, the world has witnessed an intense development in the use of digital applications and communication technologies by different groups and in all areas. These new technologies make it possible, on the one hand, to facilitate and simplify the life of citizens and to contribute to the achievement of the economic and social development, on the other hand. However, they pose important challenges in terms of information safety and the protection of cyberspace from internal and external risks and threats targeting the .national security

In order to keep pace with these rapid technological developments, the Ministry of Communication Technologies has made strengthening Cybersecurity and enhancing digital sovereignty as one of the pillars of its strategy for action to meet the challenges of digital transformation, the need to open up to information systems and applications, and to cope with risks the National ,2019 from the volume of exchanged data across networks. In .Cybersecurity Strategy was endorsed by the National Security Council

The Ministry and its various structures are keen to continue their efforts to foster a culture of Cybersecurity and call on the various actors to protect national cyberspace and prevent and withstand cyber risks by building on .national capabilities and strengthening digital trust

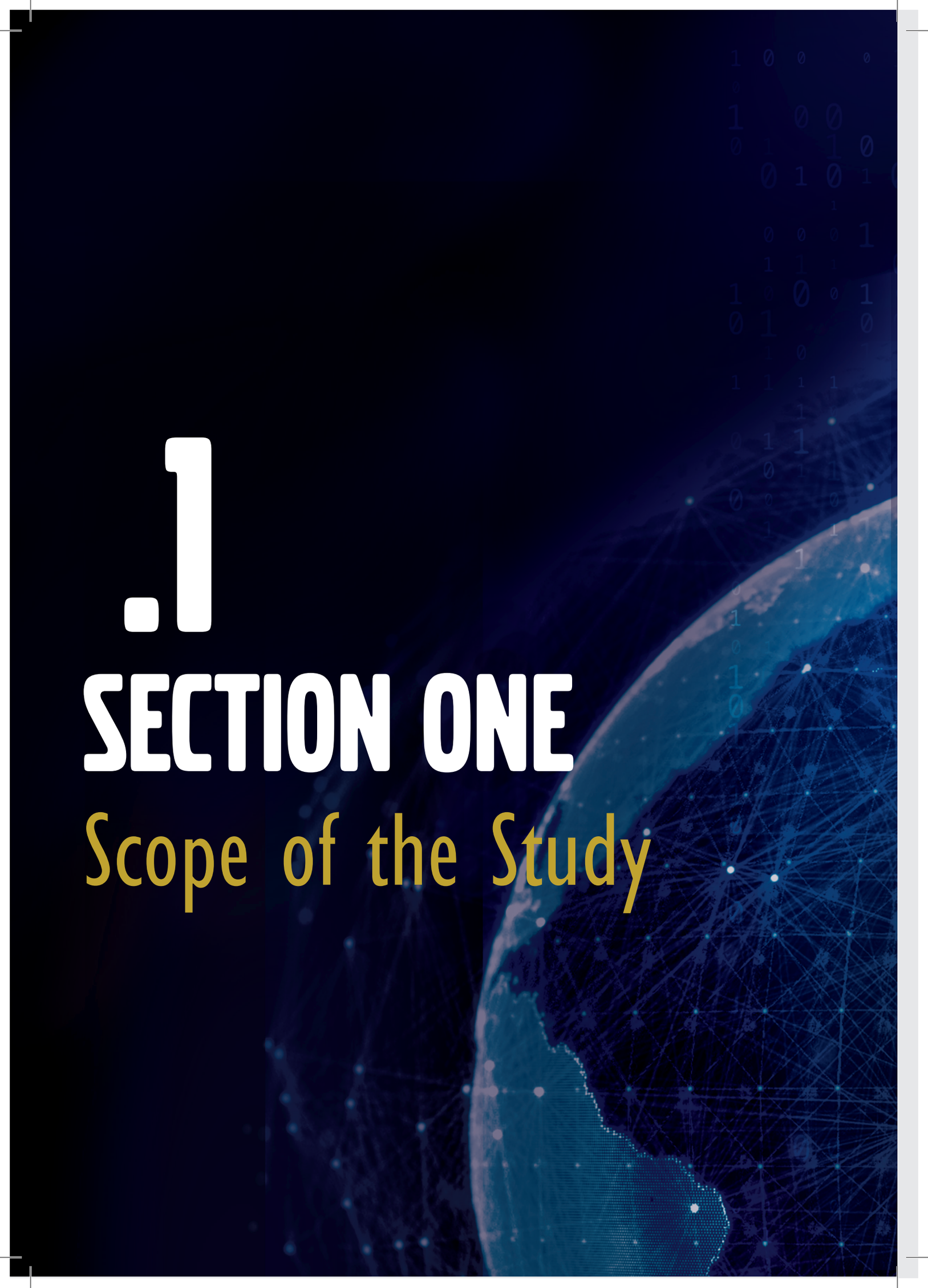
**Dr. Nizar Ben Neji**
**Minister of Communication Technologies**
**Republic of Tunisia**

# TABLE OF CONTENT

# EXECUTIVE SUMMARY

By considering the economic, social and human development indicators among the Arab States, it becomes clear that there is an imbalance between them, as the ranking of some States rises to a level approaching the developed States, while other States face difficulties with development due to many variables, conflicts and other handicaps that affect the region and its surroundings. The Covid-19 wave, the largest health crisis facing the entire world, has deepened this imbalance. This imbalance also includes the willingness and readiness of Arab States to deal with the issue of cybersecurity, which has become a national security issue with the same importance as other critical strategic sectors such as defense and public security... The effort exerted in recent years by the Arab States in building capacities in the field of cybersecurity had an outstanding effect in the evolution of the ranking of many Arab States as for the international specialized indicators, where some of them have achieved exceptional qualitative leaps, while indicators of other States have stabilized. With all these initiatives, there remains an urgent need for concerted efforts within a regional framework to further support the Arab capabilities, such as the comparative experiences. Within the framework of this document, we present the most important conclusions we have reached regarding the current situation in the Arab States and the nature of the risks to which they are exposed. This document also presents a proposal for a common Arab strategy for cybersecurity and, finally, recommendations on the issue of cybersecurity governance in the Arab region and some initiatives that could be implemented.

The different and differentiated situations of the Arab States with regard to the adoption of a national strategy for cybersecurity and related legislations have not prevented the emergence of a number of initiatives for the joint Arab action and in various regulatory and institutional frameworks that would support and contribute to the implementation of the outcomes of an Arab vision for cybersecurity, in particular its action plan.



# .1 SECTION ONE

## Scope of the Study

## 1.1 GENERAL INDICATORS

Demographic data in the Arab region has witnessed an important development in recent decades. The population today is about 423 million people, compared to 222.7 million in 1990. Today, the population of the Arab region represents 5.6% of the world's population, distributed over 22 States covering the tenth of the land area (14 million km²). The Arab region is characterized by a high percentage of young people, as the 10-24 age group constitutes about a quarter of the region's total population.

With reference to international indicators, it is clear that the economic, social and human development levels are unbalanced among the Arab States. Some States are at a level close to the developed States, while others face difficulties with development because of economic, social and economic infrastructure variables, conflicts and other constraints affecting the region and its surroundings. The Covid-19 wave, the major health crisis facing the entire world, had deepened this imbalance, especially since some States were ready to employ digital solutions to accommodate profound changes in working and production methods and remote service delivery, while others were unable to achieve a smooth and flexible transition from face to face services to remote services. The gap between the States of the region was exacerbated by the differentiated development in infrastructure, competencies, research and development systems, as well as legislative systems.

In the midst of rapid digital developments in the world's economy, the States of the Arab region have begun to shift from the traditional to the digital economy. Some States have made significant progress in digitizing a number of different areas and sectors. A study published by the Arab Monetary Fund in 2020 showed that the digital economy, for example, has contributed to reducing the cost of delivering government services by up to 88 % in some States, while others are still very slowly engaged in the digital transformations. The digital divide is expected to play a role in widening the economic gap between the States of the region.

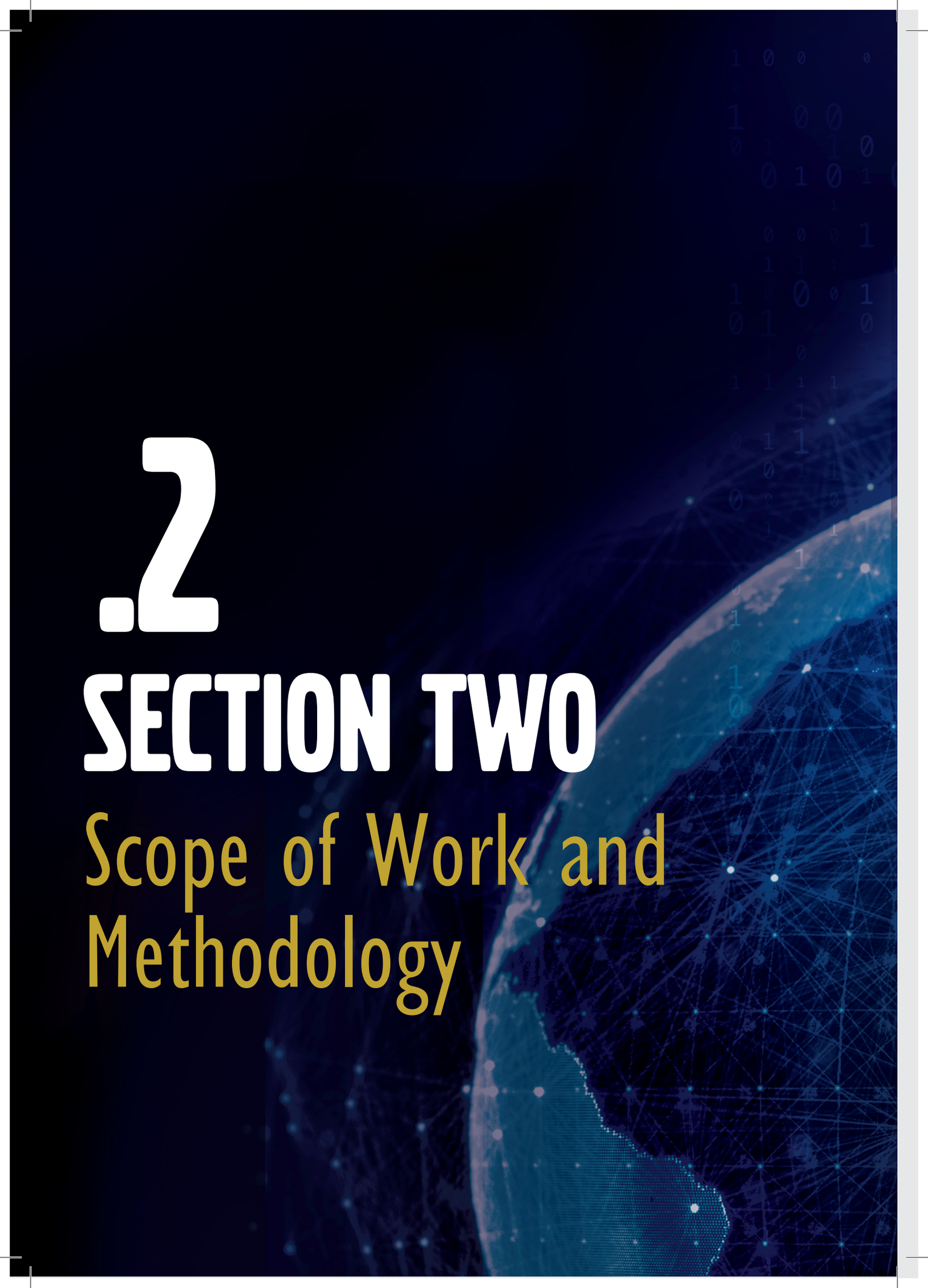
In the light of the above, Cybersecurity is one of the strategic priorities for the States in the Arab region. Since the opening up of cyberspaces to their surroundings has been inevitable, it opens up enormous challenges. Cybercrime has become dependent of the latest technologies (artificial intelligence, Internet of things...) to avoid being tracked down and to create as much damage as possible. The Arab region is considered as fragile in this regard considering the interest of young people, who constitute the majority of the population, by cyberattacks and the inability of electronic systems to keep pace with the quantitative and qualitative evolution of such attacks.

In this regard, this document proposes a strategic vision to reduce cybersecurity risks for the States of the Arab region.

## 1.2 SPECIFIC SCOPE OF THE STUDY

The preparation of this study is part of the efforts of the Arab Organization for Communication and Information Technologies and its partners to implement the relevant resolutions aimed at raising the capacity of the Arab region in the communication technology sector, in particular in implementation of the decision of the Fourth Ordinary Session of the Economic and Social Development Summit, held in Beirut, Lebanon, on 20 June 2019, Decision No. 56 DA (4) - C3 - 20/01/2019 - (Point 3), which states: «To assign the General Secretariat, in coordination with the relevant ministerial councils and the Arab Organization for Communication and Information Technologies and Expertise of the Arab States, the task to study the development of a common Arab vision in the field of technology, the digital economy and cybersecurity.»

In this context, the Group of Arab Experts on Cybersecurity from the Arab Region was established and tasked to prepare this study, with a framework and follow-up by the Arab Organization for Communication and Information Technologies.



# .2 SECTION TWO

## Scope of Work and Methodology

## 2.1. SCOPE OF WORK

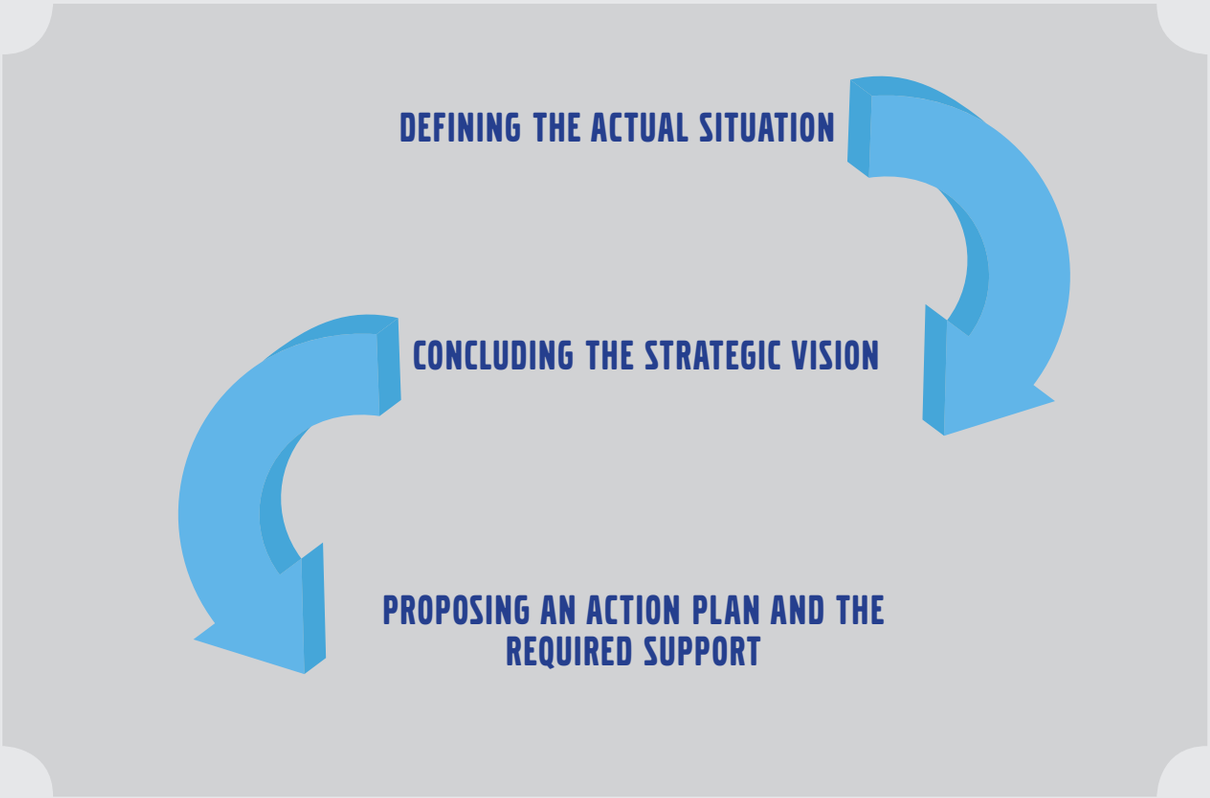
There is no doubt that the Arab Organization for Communication and Information Technologies is one of the players in the field of cybersecurity at the Arab level. In view of its concern to provide support to the Arab States in order to achieve the objectives of their establishment, the organization proposes this Arab vision of cybersecurity aimed at providing a regional participatory environment to address the challenges associated with cyberspace safety and security.

The group of expert was assigned to prepare the study sought to define a general vision for the implementation, operation and improvement of cybersecurity management systems in order to add value through the completeness, comprehensiveness, accuracy, validity and reliability of the data they provide. Thus, to determine and identify the various risks and threats to information and communication systems and to develop ways to protect the data contained therein. The proposed outputs within this report will also enable to establish Indexes for the following benefits:

- ESTABLISHMENT AND APPLICATION OF BEST PRACTICES FOR THE MANAGEMENT OF INFORMATION SECURITY SYSTEMS AND SECURITY CONTROLS
- FORMULATION OF AN ARAB INTEGRATION MECHANISM IN HUMAN RESOURCES, SOLUTIONS AND APPLICATIONS
- PROPOSING WAYS TO DEVELOP CYBERSECURITY-BASED EMPOWERMENT TOOLS IN DIGITAL TRANSFORMATION
- PROVIDING MEANS OF MONITORING AND CONTROLLING INFORMATION SECURITY, AND MINIMIZING THE RISKS TO INFORMATION MANAGEMENT BUSINESSES
- COMPREHENSIVE HANDLING OF THE DEVELOPMENT OF THE ORGANIZATIONAL STRUCTURE OF INFORMATION SECURITY SYSTEMS IN THE APPLICATION OF BEST PRACTICES, POLICIES, ACTION PLANS, RESPONSIBILITIES, PROCEDURES AND PROCESSES
- IMPROVEMENT OF CAPACITIES TO DEAL WITH AND RECOVER MORE RAPIDLY FROM SECURITY INCIDENTS AND TO CONTINUE BUSINESS DURING CRISIS SITUATIONS
- RAISING AWARENESS AMONG STAFF ON THE CONCEPT OF INFORMATION SECURITY MANAGEMENT
- INCREASING THE EFFECTIVENESS AND EFFICIENCY OF THE INFORMATION SECURITY AND MANAGEMENT PROCESS, SAVING TIME AND RESOURCES THROUGH THE ACTIVATION OF PROCESS ENGINEERING

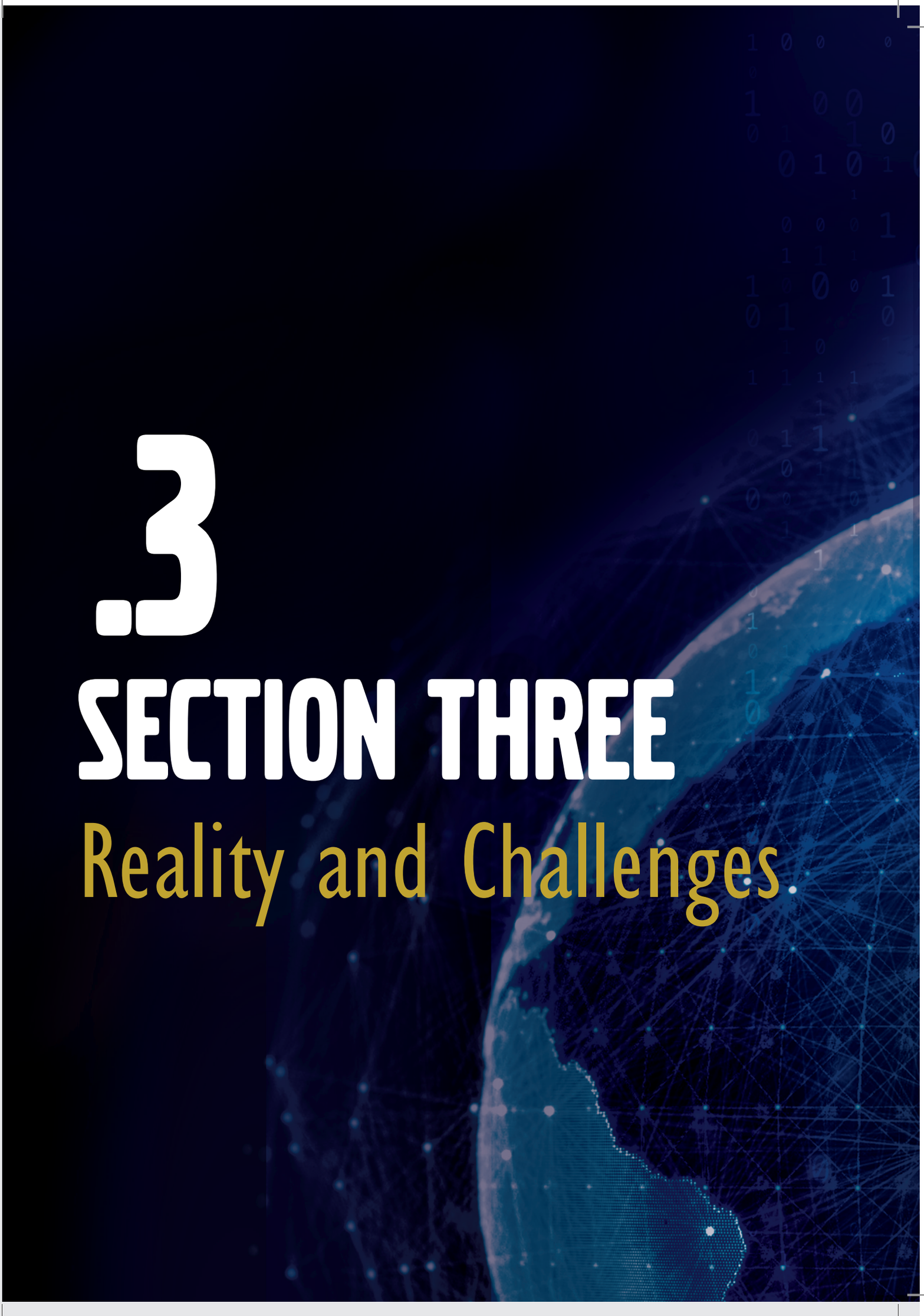
## 2.2. WORKING METHODOLOGY

The group of expert adopted a methodology based on three main stages:




The group of expert proceeds to define the current situation based on:

- REVIEW OF REGIONAL AND INTERNATIONAL COMPARATIVE STUDIES
- DEFINING, COLLECTION AND ANALYSIS OF OFFICIAL PUBLICATIONS AND DATA FOR ARAB STATES, REVIEWING AND UPDATING THEM UNTIL THE DATE OF SUBMISSION OF THE VISION ON OCTOBER 21, 2021 CORRESPONDING TO SAFAR 09, 1443 H
- INTERNATIONAL TELECOMMUNICATIONS UNION INDICATORS
- STANDARD FRAMEWORKS AND INDEXES



# .3
# SECTION THREE
## Reality and Challenges

## 3.1. THE IMPORTANCE OF THE LEGAL FRAMEWORK IN THE

Arab Cybersecurity Vision

Establishing a legislative, regulatory and institutional legal framework for cybersecurity is one of the most important conditions for the success of any vision or policy that ensures the security and safety of cybersecurity from all cyber risks and offences committed in cybersecurity. This legal framework includes strategic plans, legal texts and procedures relating to the legislative and regulatory framework, as well as the institutional framework that seeks to achieve the above-mentioned objective.

The legal framework for cybersecurity is translated into a number of strategic plans, programs and laws, either that revise and supplement the laws in force or into new laws, as well as the adoption of regulations and ordinal provisions to give effect to these legislative texts. This legal framework is also reflected in the development of procedures, regulatory mechanisms and institutional frameworks designed to achieve the intention of the public authorities for the purpose, as well as in the establishment of mechanisms for legal cooperation, especially judicial cooperation between States, as national solutions alone are ineffective and inefficient in addressing the cyberspace risks and offences.

We can also define the areas of cybersecurity legislation to the following purposes and axes: Digital trust services, information systems security services, sensitive infrastructure security services, countering cybercrime, and personal data protection.

The importance of the legal framework in achieving cybersecurity compared to other mechanisms and initiatives in this study is its contribution to the following objectives:

- Developing a strategic plan to assess the current situation of risk and identify objectives, programs and mechanisms to secure cyberspace.
- Developing legal rules for the identification of cybercrime and procedures in dealing with it by the judicial system.
- Developing legal rules compatible with technological developments in the digital space and with emerging threats to digital space.
- Enabling cybercrime tracking bodies to conduct the necessary researches and investigations
- Establishing legislative texts and regulations guaranteeing the rights and freedoms of individuals on Internet during the investigation of cybercrimes and of their personal data and privacy.
- Establishing the institutional framework to address the risks and cybercrimes and taking the necessary precautions to safeguard cyberspace security by establishing and regulating the functioning of a regional-national cybersecurity body and the other involved actors.
- Establishing the legislative and provisions for various initiatives to address the risks and cybercrimes and to take the necessary preventive measures to safeguard the security of national cyberspace.
- Establishing the frameworks, procedures and mechanisms for legal, especially judicial, cooperation between States concerned with cybercrime.

## 3.2. MECHANISMS FOR JOINT ARAB ACTION IN THE AREA OF CYBERSECURITY

The different situations and divergences of the Arab States with regard to the adoption of a national strategy for cybersecurity and related legislations have not prevented the emergence of a number of initiatives at the level of joint Arab action and in various regulatory and institutional frameworks that would support and contribute to the implementation of the outcomes of an Arab vision for cybersecurity, in particular its action plan.

The first and foremost of these initiatives was the ratification by the League of Arab States of the Arab Convention for Countering Information Technology Offences of 21 December 2010, ratified by a number of Arab member States. This Convention entered into force on 06 April 2014, 30 days after the deposit of the instruments of ratification, approval and/or acceptance by seven Arab States - Annex 1.

This Convention aims to counter offences that adopt information technologies as information technology offences and to establish a framework for the investigation and prosecution of such offences. The following acts were identified in the list of technical offences:

- Illicit access to, presence in or contact with part or all of the information technology, or the perpetuation thereof.
- The deliberate unlawful interception of the movement of data by any technical means, and the disruption of transmission or reception of information technology data.
- Offence Against the Integrity of Data - Deliberate unlawful destruction, obliteration, obstruction, modification or concealment of information technology data.
- Misuse of Information Technology Means - The production, sale, purchase, import, distribution

or provision of any tools or programs designed or adapted for the purpose of committing technological offences or the information system password, access code or similar information

- Forgery - The use of information technology • Fraud to illicitly realize interests and benefits to the perpetrator or a third party
- Pornography - The production, display, distribution, provision, publication, purchase, sale, import of pornographic material or material that constitutes outrage of modesty through information technology.
- Offences Related to Pornography - Gambling and sexual exploitation.
- Offence against privacy by means of information technology
- Terrorism - Dissemination and advocacy of the ideas and principles of terrorist groups, financing of and training for terrorist operations, dissemination of methods to make explosives, spreading religious fanaticism and dissention and attacking religions and beliefs.
- Organized crimes - Undertake money-laundering operations, request assistance or disseminate money-laundering methods, advocate the use of and traffic in drugs, traffic in persons, in human organs and (illicit) traffic in arms.
- Offenses Related to Copyright
- Illicit use of electronic tools
- Attempt at and participation in the commission of offences

Joint Arab legislative initiatives have subsequently taken the form of indicative laws, either in the area of cybersecurity as a whole or in the area of combating cybercrime or in certain other specific areas, such as the Arab Indicative Act on Information Technology Offences, the Indicative Act on Proof of Modern Techniques and the Indicative Act on Electronic Business Transactions and others. It was developed within the framework of the works of the Arab Centre for Legal and Judicial Research of the League of Arab States , which operates under the auspices of the Council of Arab Ministers of Justice.

These joint Arab initiatives have taken the form of an Arab Convention Project. In this regard, we should mention the preparation by the Arab Centre for Legal and Judicial Research of the Arab Convention Project for the Protection of Cyberspace in 2018, which was ratified by the Council of Arab Ministers of Justice of the League of Arab States.

It is useful to mention the recent initiative in the framework of the works of the Joint Arab Action High Coordinating Committee - Session 50-March 2021 - presented by the Arab Academy of Sciences, Technology and Maritime Transport and the Arab Organization for Communication and Information Technologies, which could serve as the reference framework for countering electronic piracy and protecting the networks of joint Arab action institutions and organizations.

## 3.3. REGULATORY CYBERSECURITY STRUCTURES

At the outset, it is necessary to emphasize that, in the context of monitoring the realities of the legislative and institutional framework of the Arab States in cybersecurity, and taking into account the time factor that did not enable the group of experts to carry out a complete and accurate inventory of this reality through, for example, a questionnaire in which all Arab States participate, the group has adopted a qualitative and non-quantitative approach based on the most important available and the most prominent studies and data. It has identified some examples from the Arab States without considering them in a comprehensive and complete manner, as we are developing a general cybersecurity Arab vision, while stressing the necessity and importance of a more comprehensive study of the realities of this legislative and institutional framework.

### 3.3.1. THE REALITY OF CYBERSECURITY NATIONAL STRUCTURES

Most Arab States have not created a national cybersecurity body, except for some States that have established such bodies with different designations: such as Saudi Arabia, Libya, United Arab Emirates, Jordan, Oman, Morocco, Qatar, Bahrain, etc.

In some other Arab States, however, we note the creation of several councils and bodies that play an important role in defining the cybersecurity national strategic vision and in developing practical programs to achieve it, sometimes in the form of councils and sometimes in the form of administrative bodies under the Presidency of the Republic or the Ministry responsible for security, national defense or justice, as is the case in Egypt (the Supreme Council for Cybersecurity), and Algeria (National Authority for the Prevention of Offences Related to Information and Communication Technologies). In Kuwait, the General Authority for Communications and Information Technology has jurisdiction over cybersecurity functions and responsibilities, among others.

In the area of protection of personal data, we note that some Arab States have established national bodies to monitor personal data, including the following: Tunisia, United Arab Emirates, Morocco, Egypt and Jordan. However, it is useful to emphasize that these bodies are not subject to the same legal regime and do not enjoy the same authorities and privileges. It should be noted that some Arab States have entrusted the task of monitoring personal data to some Ministries' Departments, as in the case of the State of Qatar, where the legislator made the legal department of the Ministry of Communications the competent authority in this area and subsequently, pursuant to Sovereign Decree No. 1 of 2021, the authority of cybersecurity and personal data protection were transferred to the National Cybersecurity Agency. In Jordan, a 2020 Bill Project has been published to protect personal data, including the creation of the Personal Data Protection Board.

As for electronic exchanges, some Arab States have introduced an Electronic Exchange and Digital Certification Control Body in charge with the organization and management of the national digital trust infrastructure (public key infrastructure), such as regulating the operation of digital trust services, monitoring the provision of such services and indicating the system of responsibility of service providers, like: Tunisia (The National Electronic Certification Agency), Saudi Arabia (The National Digital Certification Centre), Oman (The National Electronic Certification Centre), Egypt (The Information Technology Industry Development Authority) and Algeria (The National Electronic Certification Authority). Jordan tends to create such bodies...

Other Arab States have also pursued different institutional formulas. In the United Arab Emirates, for example, the Federal Identity and Nationality Authority provides the digital signature service and other digital trust services. In Morocco, the National Telecommunications Regulatory Agency functions as an oversight body for electronic exchanges and digital certification.

### 3.3.2. THE CURRENT READINESS OF THE ARAB REGION IN THE AREA OF LEGISLATION

Some Arab States have adopted a specific law on cybersecurity that contains the various dimensions of the latter, as enshrined in the best legislations in the world: a physical legal regime for cybercrime, a procedural legal system for its tracing, a special regulatory and oversight body, a legal regime for international cooperation and a framework for internal cooperation between the cybersecurity system components. Among the Arab States that have adopted such legislation, Jordan (Cybersecurity Act No. 16 of 2019) and Morocco (Cybersecurity Act No. 05.20) may be mentioned.

In contrast, some Arab States have only adopted special laws to counter media and communication offences or, rather, cybercrimes, as is the case with: Saudi Arabia, United Arab Emirates, Sudan, Lebanon, Yemen, Kuwait, Egypt and Bahrain. Some other Arab States have made amendments to their penal laws, as is the case with Oman and Tunisia. Other Arab States also included provisions on countering cybercrime in their general law on cybersecurity, such as Jordan and Morocco. It may also be noted that some States, such as Algeria, have ratified laws on procedures for tracking cybercrime (Act No. 2009-4 of 5 October 2009 on rules of procedures for the prevention of

offences related to information and communication technologies).

With regard to legislations on electronic transactions, most Arab States have developed such legislations, like Bahrain, Egypt, Jordan, Morocco, Saudi Arabia, Saudi Arabia, Tunisia, Kuwait, and others. It is notable that most of these texts are also related to electronic commerce.

On another level, many Arab States have ratified a law on the protection of personal data, such as United Arab Emirates, Qatar, Tunisia, Morocco, Lebanon, Bahrain, Egypt and others. Some other States had initiated the preparation of a law project on the protection of personal data that they had not yet ratified, such as Jordan and Comoros Islands. It should be noted, however, that some other Arab States have allocated some provisions of their law on trade and electronic commerce to the legal system of personal data, as is the case with Kuwait and the Sultanate of Oman. In Saudi Arabia, a system for the protection of personal data was ratified on 15 September 2021 and will enter into force within six months of its publication.

### 3.3.3. INITIATIVES OF ARAB STATES TO DEVELOP NATIONAL CYBERSECURITY STRATEGIES AND PLANS

Despite its importance in ensuring national cybersecurity, the adoption of a national cybersecurity strategy was not a common denominator among all Arab States. Having been adopted by some Arab States, such as Saudi Arabia, Oman, Egypt, Emirates, Jordan, Iraq, Lebanon, Tunisia, Morocco, Kuwait, Comoros Islands and others, we note that some other Arab States are still considering and discussing their national strategies for the purpose, such as Algeria and Mauritania. Other States have not yet begun to prepare such a national strategy, like Djibouti. In addition, several Arab States have addressed cybersecurity in their communications and information technology strategies in general, such as Libya, and have not yet ratified them.

With regard to the content of most of the Arab national strategies in force, we note that the methodology for their preparation, development and implementation is close, with almost the same elements: initiation, definition, analysis, development of the national cybersecurity strategy, implementation, monitoring and evaluation. Their content is also convergent as they contain the following axes: Identifying risks and challenges to cybersecurity, defining strategic priorities and critical target sectors, setting national and sectoral strategic objectives, developing implementation mechanisms and programs to achieve these goals and establishing mechanisms for their evaluation. Among the important areas of the national strategy: legislative and regulatory framework, cybersecurity technology framework, cybersecurity culture, capacity building, compliance, implementation and preparedness of cybersecurity incidents and international cooperation...

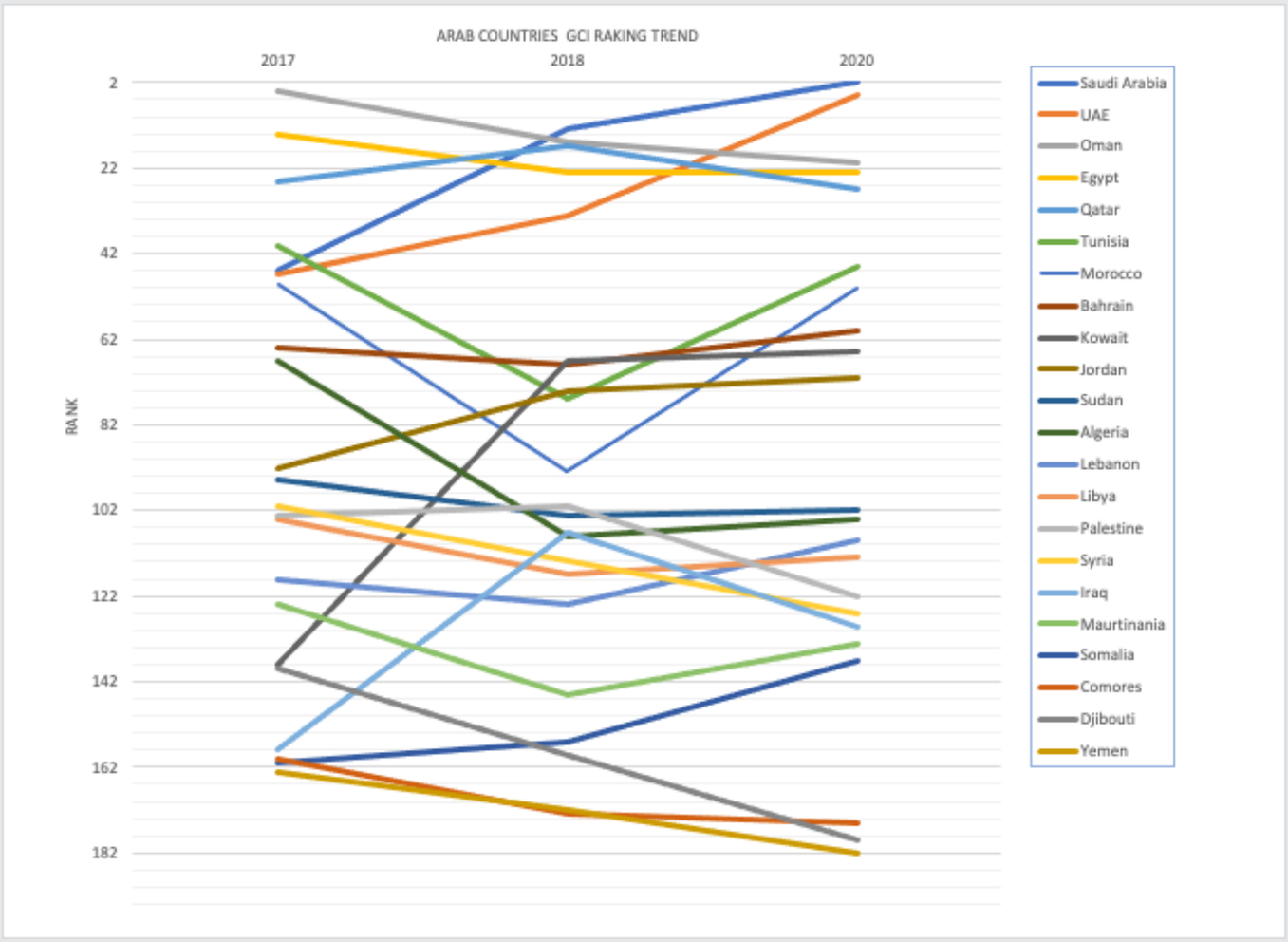
Thus, most of these adopted strategies by some Arab States are fully compatible with international best practices in this area, for example in the "Guide to a National Cybersecurity Strategy: A Strategic Commitment to Cybersecurity" by the International Telecommunication Union (ITU) or the Guidelines on Internet Infrastructure Security in the Arab States of the Internet Society Foundation (ISOC).

## 3.4. DEVELOPMENT OF THE ARAB STATES› INDEX

The effort made in recent years by Arab States in cybersecurity capacity build has had a distinct impact, as the ranking of many Arab States in the International Telecommunication Union (ITU) specialized Index has evolved. In this area, Saudi Arabia has jumped in three years from the 46th rank to the 2nd rank in the world in 2020.

This distinction was achieved in particular by establishing a national cybersecurity Centre, by adopting a wide range of policies and performance indicators for cybersecurity, and by continuously monitoring the cybersecurity situation. Saudi Arabia has also relied on global standards in the areas of data classification, cloud computing, data protection, etc. That is in addition to adopting applicable laws that are being applied. The Kingdom has also developed series of programs and initiatives to train in various subjects in cybersecurity for a very large number of employees and workers in this area. This development is the result of the Kingdom›s efforts to implement reforms in the business environment and government programs as part of its implementation of the Saudi's Strategic Vision 2030, which is primarily designed to enhance its effectiveness and increase its competitiveness. In addition to Saudi Arabia, the indicators for the United Arab Emirates, Morocco, Bahrain and Kuwait have evolved. However, the indicators of other Arab States were relatively stable.

This ITU Index aims to measure the level of commitment of each ITU Member State to the five main areas of cybersecurity: legal, technical, organizational, capacity building and cooperation levels. This Index aims to assist States in identifying areas of development and catalyzing actions to improve their ranks in the relevant world cybersecurity index, increase the level of cybersecurity worldwide, help identify and promote best practices and promote the building of a global cybersecurity culture.




*hart - Evolution of ITU Index from 2017 - 2020*

## 3.5. RISKS ANALYSIS FOR ARAB STATES

### 3.5.1. RISK ASSESSMENT

The main risks to cybersecurity in the Arab region, particularly at the legal and institutional levels, are centered on the following points:

- The failure of many Arab States to adopt cybersecurity legislation;
- The dispersal of cybersecurity legislations and cybersecurity offences between several laws, and the absence of a unified law whose provisions are easily referenced.
- Multiple cybersecurity structures have created difficulties in identifying and coordinating areas of intervention.
- Some cybersecurity legislations are inadequate for the privacy and challenges of digital space
- Inappropriate legislation that constitutes the legal environment for cybersecurity (such as the Electronic Communications Act...) with the specificities and challenges of digital space.
- Many cybersecurity laws remain inapplicable because of the absence of the needed provisions to achieve them.
- Most States lack legislations to process and protect data of a personal nature.
- The absence of a common regulatory and legal issue of digital space reference among the Arab States.
- Significant lack of implementing regulations, procedural decisions and regulatory instruments for the application of laws.
- Most Arab States lack a procedural law governing the investigation and collection of electronic evidence because of the privacy of these procedures in connection with digital space.
- Difficulties in applying traditional penal codes in digital space.
- Adoption of some States of special regulations and provisions in the area of tracing cybercrime because of the slow legislative process, even though the scope of such orders and decisions is the authority of the legislator.
- The difficulties of accepting digital evidences in both civil and criminal courts in the absence of legal recognition in some States in terms of validity and evidentiary value.
- The failure of traditional means of

international judicial cooperation to effectively address cybercrimes.

- Weak human and material potential in some Arab States to deal with cybercrime
- Absence of special teams of law enforcement officers to deal with cybercrimes.
- Difficulties in resolving the question of jurisdiction for transnational cybercrimes.
- The lack of awareness-raising programs for citizens and the lack of involvement of civil society in these dynamics.
- Focus on the central role of the State in most Arab States in implementing cybersecurity initiatives, including the computer's security response teams.
- The lack of computer's security response teams of the legal basis for their activity, financial resources, equipment, human resources, skills and empowerment.

### 3.5.2. REGIONAL CHALLENGES

There are many challenges to security, stability and prosperity in the region, especially with the growing reliance on technology and the rapid transmission of information. Cybersecurity concept is one of the most important challenges at the strategic level because of its national and international impact. These challenges have evolved because of the backdrop of the world extraordinary and unprecedented global health crisis since the beginning of the spread of the COVID19- virus, which has significantly increased the number of targeted attacks on various components of cyber spaces. The sudden changes in the methods and approaches of remote service delivery have been the most important contributing factors to the frequency of cyber-attacks and the increased risks to cybersecurity.

In this context, States should take sustained and sophisticated measures to be prepared to face the risks of cyber threats to their infrastructure within their digital information space and associated activities on the World Wide Web. This requires strengthening and reinforcing the components of their electronic arsenal by building on their national strengths and by engaging with the private sector to avoid the consequences of damaging their strategic interests and the foundations of their national security.

Digital space is reshaping politics, economy and societies around the world. Many of these communities and companies rely on the continuous operation of digital machines to deliver important services such as hospitals, funding, communications and other military and civilian purposes. As a result, internet users face many challenges, which require a security response at the highest level to meet those challenges and risks and minimize the resulting damages.

With regard to the protection of digital space from threats of cybercrime, cyberterrorism and cyberattacks by States or non-State actors, it is a matter of protecting networks and information systems from attacks that could endanger devices, programs or information, especially since such attacks may lead to the diversion of private information, as well as damage or create chaos to destabilize and push for increased disorder at various levels: politically, security, economically and militarily.

Despite the new opportunities created by digital innovation, which have contributed significantly to advancing technological development, there are significant security challenges, the greatest of which is information security as well as risk management, organization, infrastructure management and disaster recovery.

In view of what has been said, it is necessary to look at the concept of digital space, the campaigns of sabotage, espionage, disruption or destruction and their strategic impact on national security.

In this context, disruption or destruction is defined as malicious and deliberate action that disrupts routine tasks, features and electronic capabilities, including damage or destruction of information and equipment.

Cyber espionage is the process of obtaining information and secrets without the permission of the owner, to gain advantage over individuals, competitors, groups and governments. Cyber espionage is carried out through the exploitation of proxy servers through harmful software, viruses, worms, Trojan horses, and spy programs.

Sabotage is defined as activities aimed at influencing the domestic policies of the target States. It is a kind of new war without a weapon. Cyber sabotage undermines the power and authority of the political system or State institutions and aims to achieve strategic impact without the use of force.

The Internet then served as a suitable platform for more terrorist and aggressive acts than ever before, as well as for the rapid development and acquisition of modern technologies by terrorist groups. These terrorist groups deal with each other in ways that were not available in the past, using modern means

of communication, especially the internet, to ensure communication and coordination in order to exercise their activities, spread their ideas and attract young people.
Electronic risks have become part of the daily life and the more digitized services and governments become, the more vulnerable they become to infection and attacks. Thus, specialized national security agencies are increasingly involved in identifying and addressing the strategic implications of cybersecurity issues within their strategies that link digital technology to State policy in terms of organization and governance.

Offensive Cyber Operations have become one of the most important forms of inter-States warfare, not only large and technologically advanced States, but also many States in the world that have been able to acquire these tools because of their relative ease of access and the relatively low cost of acquiring them comparing to the tools of normal warfare. In the past 10 years, the world has witnessed a tremendous development in the capacity of various States to cause serious damage to other States because of these cyber-intrusions. This may extend through a long history of intrusions, some of which have been identified and others have yet to be confirmed.
Many major States have expressed their concerns about this type of attacks, which target not only the confidentiality of their data, but has also been able to undermine critical infrastructure services in many States. The world›s major States have been attacked by critical infrastructure systems, industrial control systems, government electronic services, desalination plants, power plants, airport air traffic management systems, and through health management systems. These attacks have reached all sectors and all over the world, no matter how high the defense technical potential of each State is. The key rule in information security remains that «there is no %100 security system», which makes everyone targeted and put everyone in the threat circle.
It should be noted that in September 2018, the United States announced the National Cyber Security Strategy to counter its risks. The UK has also announced the creation a strong cyber unit in collaboration between the GCHQ and the British Ministry of Defense with an estimated strength of 2000 hackers. In October 2018, the NATO leadership announced the establishment of the CCDCOE - Cooperative Cyber Defense Centre of Excellence.
It involves 25 States for establishing a Centre at the highest level of technical equipment and human skills to monitor and counter cyber-attacks on any of the NATO member States in an effort to prevent or minimize their effects. The NATO has examined military strikes against any State found to be involved in cyber-attacks against any Member State and it is planned that this Centre will be fully operational by 2023.
Germany and France preceded the United States of America as well as the United Kingdom in announcing the establishment of cyber armies of a declared strength of 13500 hackers. The German Ministry of defense identified this entity as one of the main units in the German Ministry of defense, as did the Air, Land and Sea Forces. Finally yet importantly, France has also announced the establishment of units of cyber armies to counter the France's risks of such attacks.

### 3.5.3. SOME RECENT EXAMPLES OF HACKS

The following are some recent examples of intrusions that have had a huge impact on the national security of States and the protection of their sensitive data or the disruption of critical infrastructure services:

### 3.5.3.1. THE GREAT HACK

This Hack is called the Great Hack because of the level of complexity associated with it, the implementation mechanism, as well as its implications. Undisputed, it is one of the most important and powerful hacks of recent years, with one of the largest companies involved in the production of management programs hacked into networks and organized information, the Solar Windows Company, which owns thousands of customers worldwide, particularly in the United States of America. After hacking into this company, hackers were able to exploit its client software to hack into these clients, making it multi-phased, not only hacking into the software company, but also using it as means of hacking into its customers. In order to identify the damage caused by this hack, it is enough to know that clients of this company include the United States Treasury Department, the United States Department of Defense and Microsoft. After the discovery of this hack, Solar Windows announced that 18000 of its clients had been hacked; including Microsoft, which later announced that 30,000 of its cloud-computing customers had been hacked. It may not be exaggerated to say that the scale of the real damage caused by such a hack is too great for anyone to account for. The U.S. Intelligence Agency reports that the culprit behind these attacks is foreign intelligence, which led the current U.S. President to impose a $1 billion penalties for Russian companies he said they were involved in.

### 3.5.3.2.THE SCANDAL OF LEAKING THE DATA OF MILLIONS OF AMERICAN CITIZENS THROUGH SOCIAL NETWORKS APP AND INFLUENCING AMERICAN PUBLIC OPINION

In a first in history, a company specializing in campaign management (Cambridge Analytica), one of the companies involved in the campaign management of the former President of the United States, obtained the data of more than 80 million U.S. citizens. This analytical data has made it possible to identify who is in his favor and who is in favor of his competitor. The study of demographic data and the analysis of the trends of the owners of these political accounts through the analysis of their behavior on social media networks has made it possible to carry out propaganda campaigns and to direct content that will improve the mental image of the users of these accounts of a candidate and show the disadvantages of the other candidate, especially after another cyber scandal involving the hacking of his e-mail and the disclosure of highly critical secrets related to an earlier period.

### 3.5.3.3 KIEV-UKRAINE MAIN CONTROL CENTRE HACK

In 2016, the special electronic system of Kiev›s main control station in Ukraine, followed by more than 60 substations, was hacked into the accounts of the station›s management staff and then tapped into their passwords for remote access to control the substations and access to total power outages. This disruption for long hours has caused many damages to all sectors, whether military or civilian, including but not limited to: Hospitals and e-government services, as well as severe impacts on banking services. It may be also necessary to mention that this has been repeated several times in different forms and objectives.

### 3.5.3.4.«CRYPTO AG" SCANDAL

Crypto AG is one of the largest and best-known companies in the production of encryption equipment and tools for highly classified correspondence at the level of Heads of States and diplomatic bodies around the world. For decades, the company has been trusted by dozens of States around the world and has sold its equipment in over 120 States around the world. In February 2020, «The Washington Post» published a shocking report, announcing that the company had been secretly acquired by a developed State. With sophisticated technology, it was able to acquire the encryption keys used by this equipment, which enabled it to monitor and follow up on all the correspondence made through the company›s equipment worldwide.

### 3.5.3.5.THE UK «NATIONAL HEALTH SERVICE" HACK

In May 2017, the UK National Health Service was targeted with ransom viruses. Key servers, databases and applications of the health system were encrypted. This paralyzed the entire electronic system. As a result, all health services were disrupted in a wide range of the United Kingdom. This has had a serious impact on the health services of hospitals and health-care centres, posing a serious threat to the lives of citizens present or attending hospitals. From the above, the extent of the severe damage that cyber-attacks can cause and their effects on the national security of States is clearly demonstrated. For the Arab region, there is an urgent need today to formulate

an integrated Arab cybersecurity strategy in order to strengthen joint Arab cooperation in this important area, exchange Arab experience and build capacity, as well as to intensify coordination in monitoring and responding to risks towards a secure Arab cybersecurity space. Such space that will enable many States to realize their future vision towards supporting the digital economy and implementing the digital transformation mechanisms, providing smart digital services and further expanding the systems of the Fourth Industrial Revolution. In addition to securing the implementation of intelligent city projects in many Arab capitals, which ultimately leads to the maintenance of Arab national security and the provision of greater welfare to the Arab citizen.

## 3.5.4. CHALLENGES OF SECURING MOBILE NETWORKS

### 3.5.4.1. CHALLENGES

Fourth and Fifth-generation networks face security challenges and opportunities stemming from the new services they provide as well as the nature of the infrastructure and technologies they exploit , as well as the normal requirements for protecting the privacy and data of the last user. All stakeholders need to understand the requirements of diverse scenarios to establish the networks, the infrastructure and the services to be provided, in particular better definition of insurance standards and techniques to address the associated risks.

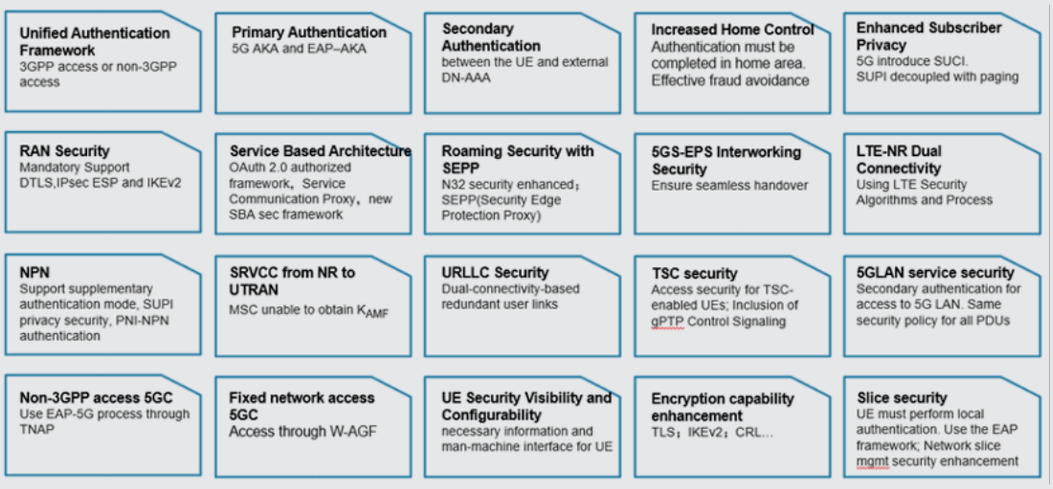
### 3.5.4.2.TECHNOLOGY INSURANCE FEATURES

The independent fifth-generation network provides more security and safety features to meet potential security challenges in the life cycle of future networks, such as air interface security, enhanced user privacy data protection, enhanced roaming security, improved encryption algorithms, etc.

Non-independent fifth-generation and fourth-generation networks share the same safety mechanisms and operate in accordance with standards and practice to continuously improve their security levels. Therefore, they are securer networks than other generations, especially through their realization of all means of security reference in all their components.

### 3.5.4.3. MOBILE NETWORK SECURITY MEASUREMENT STANDARDS

Within the framework of fifth-generation networks, GSMA and 3GPP , leading standard-setting organizations in the telecommunications industry, jointly defined the Network Equipment Security




*Key components in securing fifth-generation networks*

Assurance Scheme (NESAS ) and developed the Security Assurance Specification (SCAS) for the evaluation and security audit of mobile network equipment. The NESAS/SCAS specification provides a basic framework and a unified approach to establishing and verifying that networks meet all security and safety requirements.

The Operators Association has launched a special platform for sharing knowledge on fifth generation network security . This platform aims to support stakeholders in identifying, planning and mitigating risks; it is a comprehensive knowledge database to scan the various threats to fifth-generation networks and to propose security controls and solutions.

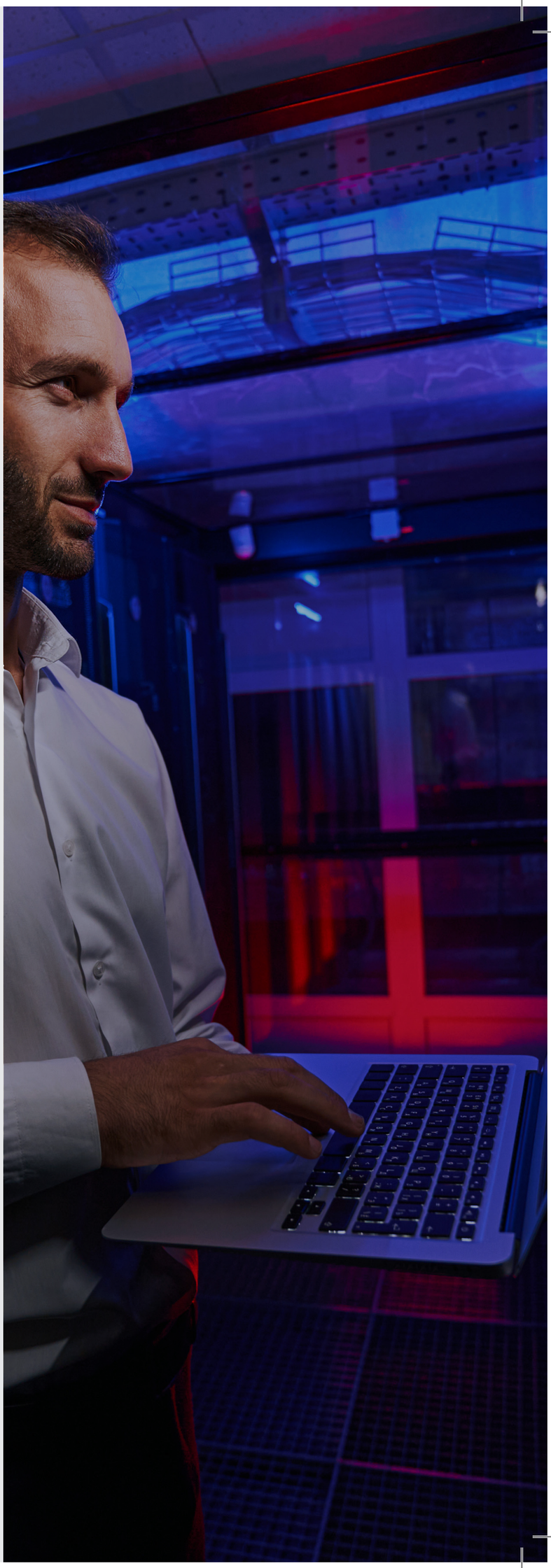
### 3.5.4.4. BUILDING TRUST BY PARTNERSHIP

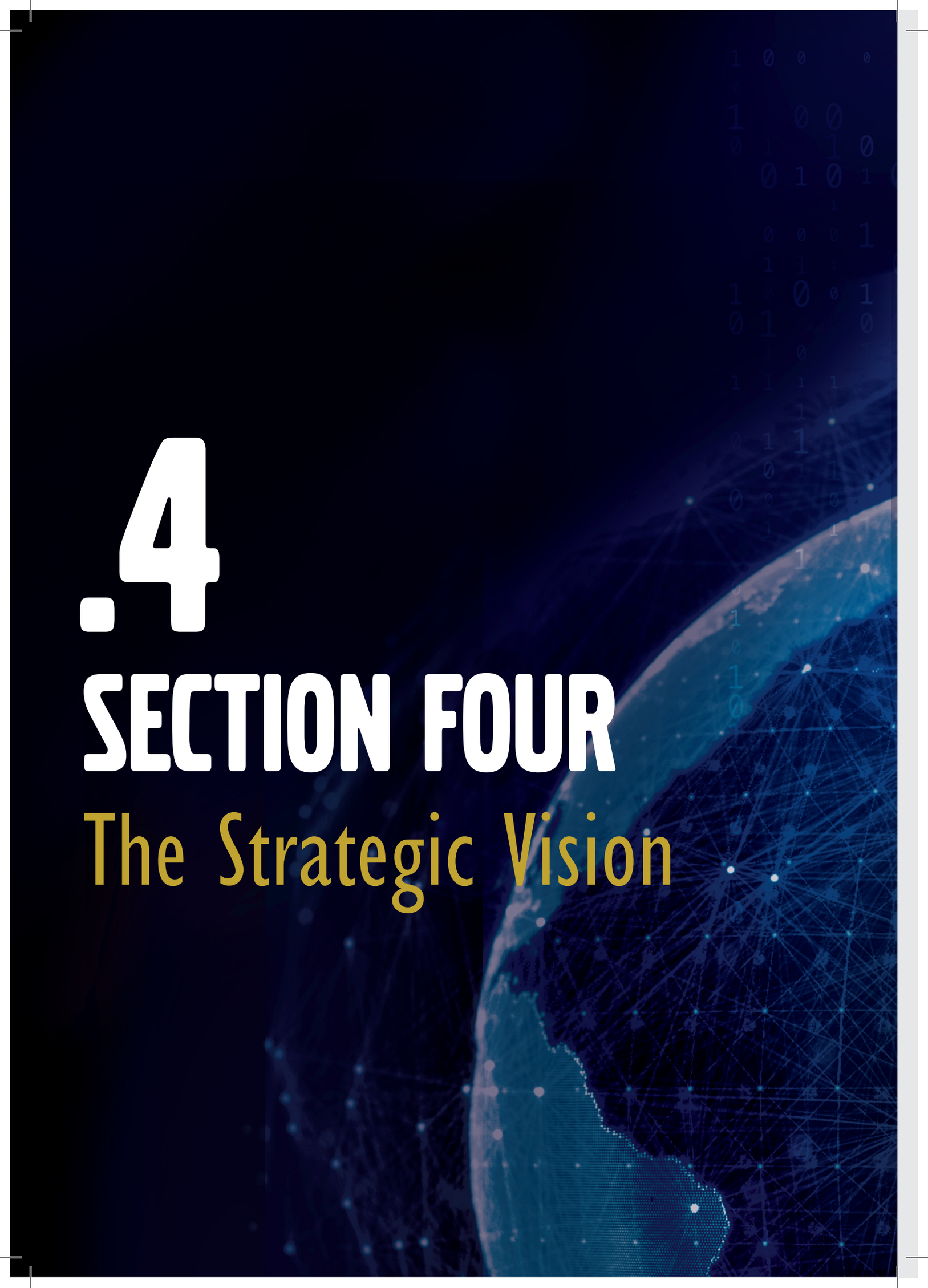
Today, the fifth-generation networks are real and this generation›s life cycle will last for some time. Building on successful experiences of fourth-generation security, the security risks of fifth-generation networks can be controlled through the joint efforts of all stakeholders.

In order to build a credible system, there is a need to work within harmonized responsibilities and common standards with a clear regulatory framework. In order to control the risks of the fifth generation life cycle, there is a need to continuously promote security solutions through technological innovation and building secure systems and networks based on appropriate standards and in collaboration among all stakeholders:

- Networks Manufacturers: Manufacturers shall contribute seriously to the development and improvement of secure network standards and shall comply with standards, integrate insurance techniques to build a secure network, together with customers and other stakeholders. Manufacturers shall mobilize capabilities to support operators to ensure the safe and flexible operation of the network.
- Operators: Operators are responsible for the continuous flexible safety of their own networks. Operators can prevent external attacks by creating firewalls and safety gates. With regard to internal threats, operators can establish appropriate and effective procedures for the management, control and scrutiny of all partners to ensure that all components of their network are secure.
- Industrial and governmental regulatory bodies: All these bodies need to work together according to Indexes under shared responsibility. With regard to technologies and fifth-generation orientations, there is a need to develop an ongoing context for the safety of fifth-generation networks in the light of risks related to multiple service scenarios (such as Slicing - MEC, mMTC, etc.). As for insurance security, there is a need to consolidate cybersecurity requirements and ensure that these standards are applicable and verifiable for all operators and manufacturers by focusing on risk identification and response.

In the age of fifth generation and artificial intelligence, all stakeholders shall collaborate to set Indexes for network safety and to develop audit, risk identification and response systems, while working to innovate and develop new solutions for flexible security.





# .4
# SECTION FOUR
## The Strategic Vision

## 4.1. STATEMENT OF THE STRATEGIC VISION

Towards a safe, integrated Arab society integrated into the global digital economy and self-sufficient solutions and expertise supporting digital confidence and protector of Arab cyberspace

- Safe Arab Society: By strengthening the sense of safety of all members of the Arab community and providing the objective conditions and requirements of cybersecurity;
- Comprehensive: Inclusive and dependent on interaction of all stakeholders.
- Integrated into the global digital economy: By formulating the necessary regulatory and technical safety measures against potential harms in the light of adopted international standards and best practices and clear guidelines through which companies and economic actors can safely develop new and innovative digital products and services to be part of the digital economy.
- Self-sufficient solutions provider: Through the development of incentive strategies for solutions developers in the Arab region to produce tools and programs for homemade IT safety;
- Digital trust supporting expertise: Through the development of qualified educational and training programs for Arab cadres and officers in all areas supporting digital trust;
- Arab cyberspace/digital protector: The ultimate strategic objective is to protect Arab regional and national cyberspace.

## 4.2. QUALITATIVE OBJECTIVES OF THE VISION

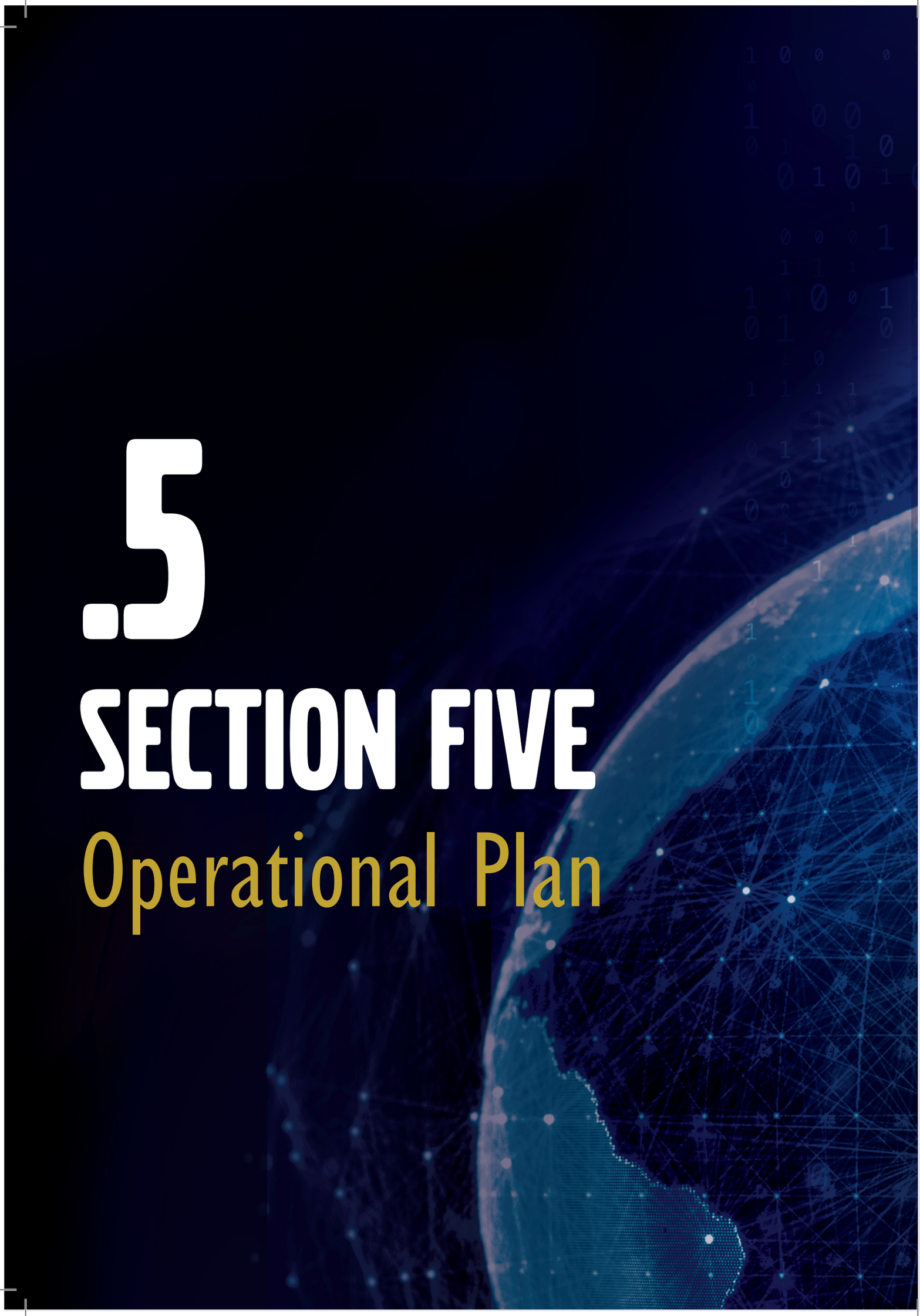
With regard to the serious challenges and risks facing the Arab region that have been intensified by the «extraordinary» global health crisis of 2020, this vision aims at:

- Creating participatory mechanisms by taking advantage of the region›s cybersecurity market
- Developing the capacity of cybersecurity specialists, encouraging professionals and students to get involved, building capacity and developing an integrated cybersecurity training system.
- Increase community awareness of cybersecurity and Internet-related risks, promoting safe digital practices and encouraging institutions to spread cyber awareness effectively.
- Organizing competitions that support cybersecurity excellence through Arab award programs, encouraging institutions to launch cybersecurity programs, inspiring entrepreneurs to innovate in the field, supporting creative research in academic institutions and encouraging students to be involved in cybersecurity;
- Regulating the cybersecurity incident detection and reporting mechanism.
- Establishing a standardized methodology for assessing the degree of gravity of cyber incidents to provide appropriate support.
- Building Arab capacities at a global level to respond to all types of cyber accidents
- Designing a comprehensive legal and regulatory framework for cybersecurity to address all types of cybercrimes, building a regulatory framework to protect current and emerging technologies, and developing supportive systems to empower small and medium-sized enterprises and protect them from cyber threats

## 4.3. MECHANISMS AND COMPONENTS OF THE VISION DEVELOPMENT

By defining the realities and challenges of cybersecurity in the Arab States, we can consider some achievements that could form the basis of the strategic vision:

- The trend of many Arab States towards adopting a national cybersecurity strategy
- The trend of many Arab States towards the adoption of general cybersecurity legislation
- The importance of Arab initiatives in bringing Arab national legislation closer together and developing joint action in the area of cybersecurity
- Most Arab States rely on the best legislative practices of the world to develop either the strategy or the national cybersecurity legislations.
- Value the role of initiatives of global international and Arab organizations in developing effective national strategies and legislations.



# 5 SECTION FIVE

## Operational Plan

## 5.1. OUTLINES OF THE OPERATIONAL PLAN

### 5.1.1. DEVELOPMENT AND IMPLEMENTATION OF A NATIONAL CYBERSECURITY STRATEGY

The Arab States lack National cybersecurity strategy, which reflects the lack of a clear or far-reaching view of cyber risks and the strategic objectives to be achieved. The development of a strategy for cybersecurity is the first step towards achieving a secure digital space for any institution or State. Undoubtedly, the path of this strategy begins after each State has defined its own vision and message regarding the management of the cybersecurity and the impact of its risks. One of the most important and best global references in this regard is the International Telecommunication Union "GUIDE TO DEVELOPING A NATIONAL CYBERSECURITY STRATEGY ."

Once the vision and the message had been defined, the analysis of the gap between the gap and the desired situation should begin to be completed, and the strategy should then be developed to serve as the road map towards moving to the desired situation. The cybersecurity strategy must be implemented within a framework of institutional governance that ensures that risks are reduced and resources are well exploited, that initiatives and projects are in line with the objectives to deliver expected outputs, and those Indexes for measuring performance are developed at all stages.

A global cybersecurity framework is also strongly recommended, representing the best global practices for managing this important topic. One of the best known models is the Cybersecurity Framework NIST , which operates on five parallel hubs in order to have full cybersecurity capabilities, which are:

1- Identify the digital assets and the associatedrisks
2- Protect and Secure
3- Detect cybersecurity events
4- Respond to cybersecurity incidents
5- Recover from cybersecurity incidents

It should be noted that the Framework is a general framework that can be used anywhere and in any of the different business sectors. It is not linked to specific technology, but is compatible and integrated with a very large number of the most popular global standards and frameworks associated with cybersecurity. The implementation of this framework shall be linked to the existence of several mechanisms, including, but not limited to:

- Mechanism for determining the critical digital assets of an enterprise
- Mechanism for risk assessment
- Mechanism for assessing impact on businesses
- Mechanism to support the principle of continuous improvement

### 5.1.2. SUPPORTING RESEARCH AND DEVELOPMENT

One of the most important factors and axes supporting tangible success in possessing cyber capabilities, whether in defense or cyberattack, is research and development. The level of success in achieving the required capabilities is linked to the volume of expenditure and logistical support available to research and development operators, whose branches and disciplines are very numerous, for example (cloud computing • mobile phones systems - systems and virtual applications - embedded systems and Internet of Things applications).

In that regard, it is important to highlight the opportunities for the required partnership between the private and the governmental sector. This could promote investment in that area, with a view to achieving many objectives, not only supporting research and development, but also creating opportunities for the development of solutions and applications or processes that support cybersecurity and enrich the technology market in the Arab States.

### 5.1.3. TRAINING AND AWARENESS-RAISING

Any successful system is based on three main axes (individuals - regulations, policies and laws - technology). In the area of cybersecurity, human resources are among the most important and almost all-important components of the system. Whatever the ability of institutions and States to possess highly sophisticated techniques, the best possible performance of such techniques will continue to depend on the capacity to operate and manage them. Therein lies the critical importance of cadre development and human capacity building. It should be noted that the world is experiencing a significant shortage of trained and qualified personnel to secure thousands of technologies in the business sectors, such as: Education, health, e-government services and banking services of various kinds, regulated by industrial control and critical infrastructure management networks, which may be the most hazardous of all, since tampering with the settings of such networks or illegal communication with them

may lead to complete paralysis of institutions and even States.

In this regard, there are well-known models and global frameworks that can be relied upon or even adopted as they are for a vision of preparing specialists in various areas of cybersecurity. The most famous model is the National Initiative for Cybersecurity Education (NICE) developed by the American National Institute of Standards and Technology (NIST). This framework defines a number of workers in cybersecurity and sets out for each function a type of job description in addition to the capabilities and skills required for the job. Thus, enabling to develop specialized training programs for the preparation of specialists from various cybersecurity branches, such as a clear path to developing the capabilities of workers in this field from the earliest to the most advanced levels. Perhaps the best Arab initiatives in this context is the Saudi Arabia›s so-called: The "Saudi initiative for cybersecurity cadres (swords).»

While we are talking about the human factor as one of the most important factors supporting the success of the cybersecurity system, it does not stand within the limits of specialists and cybersecurity officials, but rather extends to every individual in the institution. It is very likely that an enterprise will be fully targeted by any employee or affiliate, or even by any individual who has dealt with it, such as suppliers, clients, partners and any other institution associated with the target to be breached. Hence cybersecurity awareness as a critical factor, as we always stand that the weakest link in the information security chain is the human factor.

All global standards dealing with information security require awareness-raising programs for staff or users of technological systems in general, including but not limited to:

- PCI – Payment Card Industry Standard
- GDPR – General Data Protection Regulation
- ISO 27001 International Standard for Information Security

### 5.1.4. SECURITY STANDARDS

The adoption of specific cybersecurity standards as a minimum for technological security controls is important. Many States in the world have developed binding standards and controls to achieve a minimum level of cybersecurity objectives, which would be enhanced but cannot be removed without them. One of the most famous global models in this regard is that of the United States of America.

- FIPS Federal Information Processing Standards
- CC Common Criteria
- NIST 53-800 r5 (Security and Privacy Controls for Information Systems

There are also many global models that represent public standards that are not linked to a State, but can be used as public references and accepted by all the world›s specialists:

- CIS Controls - Top Critical Controls
- ISO 27001 International Standard for Information Security

Some Arab examples on this context are the United Arab Emirates, the Kingdom of Saudi Arabia and Qatar, where they have binding regulations over the various business sectors in order to achieve a minimum level of State-level cybersecurity. They are also established to develop more specialized regulations in each business sector, or more robust ones, in accordance with actual security requirements.

### 5.1.5. INTERNATIONAL COOPERATION (JOINT ARAB COOPERATION)

The exchange of expertise and technical information related to the analysis of cyber-hacking mechanisms and the attempt to determine its source and objectives is an important and potentially useful outcome of joint Arab cooperation. Access to information and the timing of access to information are crucial in detecting or predicting cyber accidents. They may also be prevented or their effects to be reduced. The idea of cooperation and exchange of information is not new, and perhaps one of the strongest examples is the North Atlantic Treaty Organization (NATO) model that created a Centre of Excellence for Joint Cyber Defense from NATO member States. The Centre includes specialists from 25 different States, monitors cyber threats to any NATO State and attempts to repel such attacks in coordination with all concerned States in order to prevent or minimize their impact. In order to be productive and effective, this cooperation must cover the three axes.

- People
- Policies, procedures and laws
- Possession of the appropriate technologies

It is also possible to share some technical information because of this cooperation with the relevant research centres in the Arab States, thereby enhancing their research capacity and developing their tools in response to cyberattacks.

### 5.1.6. ESTABLISHMENT AND DEVELOPMENT OF NATIONAL CYBER INCIDENT RESPONSE CENTRES

National Cyber Incident Response Centres are the first line of defense or units for early detection of cyberattacks. They play an important role in trying to identify the sources and objectives of such attacks and in trying to analyze their methods of work and the gaps targeted by such attacks. At the very least, there should be at least one State-level Centre, preferably coordination between the Centre and similar centres, which operate within a limited scope at the level of a specific institution or one of the ministries. It is also recommended to establish specialized centres at the level of different business sectors, such as health, communications, critical infrastructure... There are different types of requirements from sector to sector and the priorities, means and objectives of cyberattacks vary from sector to sector and from enterprise to enterprise. The Cyber Incident Response Centres are located in many Arab States but vary in their capabilities and potentials they also lack mechanisms for joint Arab cooperation and exchange of experience and information. In a number of States, there are no such centres, which necessarily requires an urgent plan to support the establishment of their national cyber response centres and the training of their personnel. Several international references can be drawn upon in this regard, notably the ITU releases on these Centres, as well as the European Union Agency for Cybersecurity (ENISA), as well as the National Institute of Standards and Technology of the United States of America.

### 5.1.7. LINK OF ACADEMIC STUDIES TO LABOR MARKET NEEDS

Largely, there is a significant gap between the technical or, if any, information security disciplines of university students and the actual needs of the labor market. One important step in providing trained cadres to fill the severe deficit between the needs of the labor market and the number of suitably qualified individuals to fill these posts will be to move towards the provision of cybersecurity-related disciplines. Large, well-trained numbers can be provided in a short period of time and at a small cost compared to specialized training costs or globally approved courses, which usually cost up to a few thousand dollars per course per trainee.

It is also possible on the one hand, to develop content based on the preparation and supervision of selected academics and professionals in order to produce curricula at appropriate cost to prepare generations of cybersecurity specialists to meet the requirements of the labor market in the Arab region. On the other hand, to support scientific research efforts in this important area. With the exception of a very limited number of Arab universities, the vast majority of them lack cybersecurity specialties and perhaps some relevant subjects.

### 5.1.8. DEVELOPMENT OF INSTITUTIONAL ADMINISTRATIVE STRUCTURES

One of the greatest problems and challenges facing most Arab States is the lack of a definition of cybersecurity, as well as where the responsibility for securing information and systems lies. IT responsibility may be the responsibility of a single person within an IT department institution or task force, and in rare cases cybersecurity departments present and directly dependent on senior management. The latter model represents the global best practices in this regard. When it comes to developing a common vision for Arab States on cybersecurity, it is essential that all State bodies and institutions have an information security department with clear and specific tasks, as well as an administrative structure in this department with an appropriate job description so that each organization has an administration that secures all its digital assets. This Department and its staff are subject to performance evaluation through specific performance indicators and are constantly developing and improving. The Department shall be under the management of the highest authority within the institution to support its operational tools to activate cybersecurity policies, tools and controls.

### 5.1.9. THE LEGAL ASPECT

To give effect to the National Cybersecurity Strategic Vision in its legal aspect, the following programs, actions and operational mechanisms shall be implemented:

- Update and review the strategy periodically in the light of changes and rapid technical development, and in the light of the accumulation of experience in the implementation of previous strategies.
- Update of cybersecurity legislation shall be guided by the best legislative practices of the world, taking into account international and regional conventions and legislations.

- Ensure that the legislative reforms to be introduced are balanced between addressing risks and cybercrime and protecting rights and freedoms, in particular privacy and online freedom of expression.
- Establish specialized units for forensic officers to investigate cybercrime.
- Encourage victims to report cybercrime to gather information and make remote reporting available.
- Capacity building in drafting cybersecurity laws and regulations.
- Organize awareness-raising and formative campaigns for judges, judicial officers, legislators, lawyers and enforcement agents involved in countering cybercrime.
- Organize awareness-raising campaigns for citizens, especially some targeted groups for cybercrime or vulnerable groups such as children, and the dissemination of a culture of privacy and cybersecurity.
- Develop the legal framework within which computer emergency response and response teams operate, and develop initiatives in the area of «ethical piracy» and overcome their difficulties.
- Develop frameworks, methods and procedures for judicial cooperation between Arab and other States to avoid safe havens for the commission of cybercrime;
- Harness and develop the skills of «ethical piracy» through talent competitions and hackatoons, and the development of manuals for local groups of researchers involved in ethical piracy
- Promote public-private partnerships in a cooperative and synergistic approach.
- Support Arab cooperation frameworks at the level of risk management and cybercrime based on a cooperative and synergistic approach
- Encourage public administrations, private institutions and associations to develop codes of conduct on cybersecurity and privacy protection.

## 5.2. COMPONENTS OF THE OPERATIONAL PLAN

The operational plan relies on the following key components:

### CYBERSECURITY LAWS AND REGULATIONS

- Addressing all types of cybercrime
- Protection of current and emerging technologies
- Strengthening the protection of small and medium-sized enterprises

### AN INTEGRATED AND DYNAMIC CYBERSECURITY ENVIRONMENT

- Supporting start-ups and promoting Cybersecurity Research and Development
- Cybersecurity capacity development
- Enhancing individuals awareness of cyber risks and the importance of cybersecurity
- Promoting cybersecurity excellence

### NATIONAL CYBER INCIDENT RESPONSE PLAN

- Standardized means of reporting cyber incidents
- Standard risk assessment model and plan for dealing with cyber incidents
- Inter-agency intelligence sharing

### CRITICAL INFORMATION INFRASTRUCTURE PROTECTION PROGRAMME

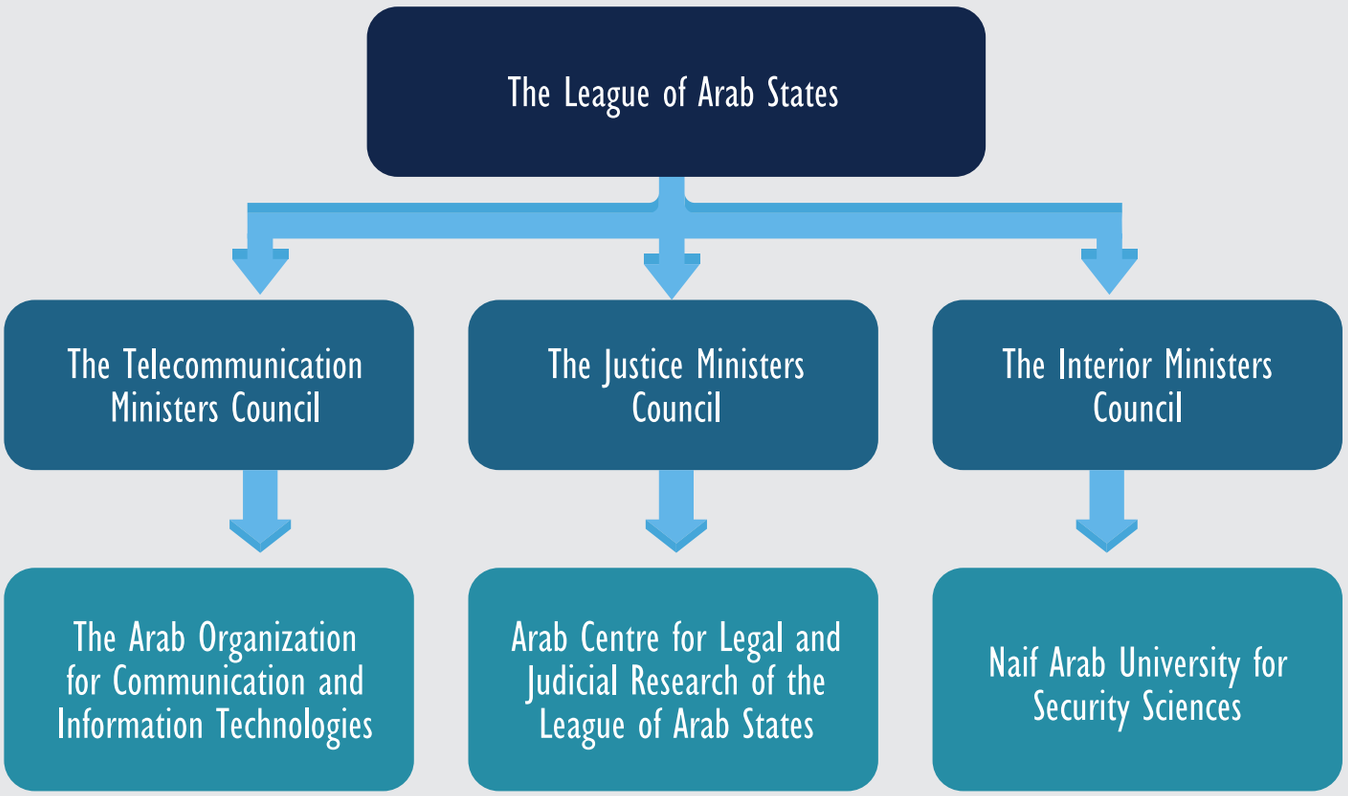
- Identification of critical assets
- Development of global standards for risk management
- Effective reporting, compliance and response processes

### PARTNERSHIPS

- Governmental sector
- Private sector
- Academic institutions
- Associations and regional and international organizations

### 5.2.1. CYBERSECURITY GOVERNANCE IN THE ARAB REGION

Given the structure of joint Arab action within the framework of the League of Arab States, and taking into consideration the competence of each body and organization, we propose the establishment of a regional council or any regional framework. This body shall manage, propose and establish regional initiatives and follow up their implementation, particularly in the areas of capacity development in the field of cybersecurity, the development of scientific research and the adequacy of legislations on IT safety and cybercrime. It shall also develop and monitor the development and dissemination of regional indicators and coordinate the preparations to counter the growing crime and cyber risks.



# REGIONAL INITIATIVES

Some of the regional initiatives that we propose:

The official establishment of a regionally and internationally recognized Arab Consortium, called Arab CERT. This Consortium could be established virtually as a first step to be one of the most important stage towards supporting Arab cooperation in this vital and strategic area.

This Consortium shall have as tasks:

- Coordinating a regional and international contact center to monitor security incidents related to information and communications technology
- Providing accurate and timely information on security threats, current or emerging vulnerabilities and proposed technical solutions
- Monitoring and providing proactive measures to reduce security incidents
- Coordinating with national, regional and international computer emergency response centres

Preparing, developing and updating of appropriate legislation and reference laws, especially in view of the rapid development of technological trends

Based on similar studies of the following laws:

- Cybersecurity laws
- Countering Cyber crime
- Protection of personal data
- Electronic transactions
- Protecting children and youth in the digital space

Capacity development in information and communication technologies and development of scientific research

through

- The development of an approved special training curriculum, which shall be completed with the certification of an Arab expert on cybersecurity and shall be implemented by a network of accredited Arab higher institutes, universities and educational institutions.
- The development of a package of catalytic regional initiatives in the field of scientific research and innovation in cybersecurity and network protection, and the organization of specialized Arab competitions in the field of Ethical hacking.
- Establishment of a database of Arab experts in the field of cybersecurity

Establishment of an observatory of cybersecurity indicators in the Arab region

through
- The development of a periodically updated platform that monitors and displays all indicators on cybersecurity in the Arab region. The platform shall also share all general reference documents on strategic and national plans.
- The formulation of regional standards taking into account global best practices, while keeping in mind the special needs of Arab States

# 6. Conclusion

We are fully convinced that, with regard to cybersecurity, many Arab States are making great efforts, but there is still a long way to go through to deal with the growing cyber risks, which require the consolidation of 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 strong cooperative relationships in order to establish a cooperative approach to promote open, free and secure digital space for all everywhere.

The Arab Organization for Communication and Information Technologies looks forward this initiative to be the nexus between Arab States in the area of information safety and cybersecurity. We look forward to cooperating with all Arab States and actors in the field in order to achieve our common objectives.

# .7 ANNEXES

## وضع رؤية عربية مشتركة
## في مجال التكنولوجيا والاقتصاد الرقمي والأمن السيبراني

**إن مؤتمر القمة العربية التنموية: الاقتصادية والاجتماعية في دورته العادية الرابعة،**

- **بعد اطلاعه على:**
  - مذكرة الأمانة العامة،
  - قرار المجلس الاقتصادي والاجتماعي رقم (2209) د.غ.ع بتاريخ 2018/12/20،
  - نتائج أعمال الاجتماع المشترك للمندوبين الدائمين وكبار المسؤولين والاجتماع المشترك لوزراء الخارجية والوزراء المعنيين بالمجلس الاقتصادي والاجتماعي للتحضير للقمة،
- **وبعد الاستماع إلى إيضاحات الأمانة العامة،**
- **وفي ضوء المناقشات،**

**يُقــرّر**

1. تثمين مبادرة حضرة صاحب السمو أمير دولة الكويت الشيخ صباح الأحمد الجابر الصباح لإنشاء صندوق للإستثمار في مجالات التكنولوجيا والاقتصاد الرقمي برأس مال وقدره مائتي مليون دولار أمريكي بمشاركة القطاع الخاص، ومساهمة دولة الكويت بمبلغ 50 مليون دولار، وكذلك مساهمة دولة قطر بمبلغ 50 مليون دولار من رأس مال هذا الصندوق بما يعادل نصف حجمه، على أن يوكل إلى الصندوق العربي للإنماء الاقتصادي والاجتماعي مسؤولية إدارة هذه المبادرة التنموية.
2. دعوة الدول العربية إلى دعم هذه المبادرة للإسهام في تعزيز الاقتصاد العربي المشترك وخلق فرص عمل واعدة للشباب العربي، وحث البنوك ومؤسسات التمويل العربية المشتركة المساهمة في دعم هذه المبادرة بالطرق التي توفر لها الاستمرارية لتحقيق أهدافها المنشودة.
3. تكليف الأمانة العامة بالتنسيق مع المجالس الوزارية المختصة والمنظمة العربية لتكنولوجيات الاتصال والمعلومات والخبرات المتوفرة لدى الدول العربية، بدراسة وضع رؤية عربية مشتركة في مجال التكنولوجيا والاقتصاد الرقمي والأمن السيبراني.

**(ق. ق: 56 د.ع (4) – ج 3 – 2019/1/20)**

# الاتفاقية العربية لمكافحة جرائم تقنية المعلومات

## الديباجة :

**إن الدول العربية الموقعة،**

***رغبة*** منها في تعزيز التعاون فيما بينها لمكافحة جرائم تقنية المعلومات التي تهدد أمنها ومصالحها وسلامة مجتمعاتها،

***واقتناعاً*** منها بضرورة الحاجة إلى تبني سياسة جنائية مشتركة تهدف إلى حماية المجتمع العربي ضد جرائم تقنية المعلومات،

***وأخذاً*** بالمبادئ الدينية والأخلاقية السامية ولا سيما أحكام الشريعة الإسلامية، وكذلك بالتراث الإنساني للأمة العربية التي تنبذ كل أشكال الجرائم، ومع مراعاة النظام العام لكل دولة،

***وإلتزاماً*** بالمعاهدات والمواثيق العربية والدولية المتعلقة بحقوق الإنسان ذات الصلة من حيث ضمانها واحترامها وحمايتها،

**فقد اتفقت على ما يلي :**

## الفصل الأول

## أحكام عامة

**المادة الأولى : الهدف من الاتفاقية :**

تهدف هذه الاتفاقية إلى تعزيز التعاون وتدعيمه بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، لدرء أخطار هذه الجرائم حفاظاً على أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها.

**المادة الثانية : المصطلحات :**

يقصد بالمصطلحات التالية في هذه الاتفاقية التعريف المبين إزاء كل منها:

1- **تقنية المعلومات :** أية وسيلة مادية أو معنوية أو مجموعة وسائل مترابطة أو غير مترابطة تستعمل لتخزين المعلومات وترتيبها وتنظيمها واسترجاعها ومعالجتها وتطويرها وتبادلها وفقاً للأوامر والتعليمات المخزنة بها ويشمل ذلك جميع المدخلات والمخرجات المرتبطة بها سلكياً أو لاسلكياً في نظام أو شبكة.

2- **مزود الخدمة :** أي شخص طبيعي أو معنوي عام أو خاص يزود المشتركين بالخدمات للتواصل بواسطة تقنية المعلومات، أو يقوم بمعالجة أو تخزين المعلومات نيابة عن خدمة الاتصالات أو مستخدميها.

3- **البيانات :** كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة تقنية المعلومات، كالأرقام والحروف والرموز وما إليها ...

4- **البرنامج المعلوماتي**: مجموعة من التعليمات والأوامر، قابلة للتنفيذ باستخدام تقنية المعلومات ومعدة لإنجاز مهمة ما.

5- **النظام المعلوماتي**: مجموعة برامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

6- **الشبكة المعلوماتية**: ارتباط بين أكثر من نظام معلوماتي للحصول على المعلومات وتبادلها.

7- **الموقـــع** : مكان إتاحة المعلومات على الشبكة المعلوماتية من خلال عنوان محدد.

8- **الالتقـــاط** : مشاهدة البيانات أو المعلومات أو الحصول عليها.

9- **معلومات المشترك**: أية معلومات موجودة لدى مزود الخدمة والمتعلقة بمشتركي الخدمات عدا المعلومات التي يمكن بواسطتها معرفة:

أ - نوع خدمة الاتصالات المستخدمة والشروط الفنية وفترة الخدمة.

ب- هويـــة المشـــترك وعنوانـــه البريـــدي أو الجغرافـــي أو هاتفـــه ومعلومات الدفع المتوفرة بناء على اتفاق أو ترتيب الخدمة.

ج - أية معلومات أخرى عن موقع تركيب معدات الاتصال بناء على اتفاق الخدمة.

**المادة الثالثة : مجالات تطبيق الاتفاقية :**

تنطبق هذه الاتفاقية ما لم ينص على خلاف ذلك، على جرائم تقنية المعلومات بهدف منعها والتحقيق فيها وملاحقة مرتكبيها، وذلك في الحالات الآتية :

1 - ارتكبت في أكثر من دولة.

2- ارتكبت في دولة وتم الإعداد أو التخطيط لها أو توجيهها أو الإشراف عليها في دولة أو دول أخرى.

3- ارتكبت في دولة وضلعت في ارتكابها جماعة إجرامية منظمة تمارس أنشطة في أكثر من دولة.

4- ارتكبت في دولة وكانت لها آثار شديدة في دولة أو دول أخرى.

**المادة الرابعة : صون السيادة :**

1- تلتزم كل دولة طرف وفقاً لنظمها الأساسية أو لمبادئها الدستورية بتنفيذ التزاماتها الناشئة عن تطبيق هذه الاتفاقية على نحو يتفق مع مبدأي المساواة في السيادة الإقليمية للدول وعدم التدخل في الشؤون الداخلية للدول الأخرى.

2- ليس في هذه الاتفاقية ما يبيح لدولة طرف أن تقوم في إقليم دولة أخرى بممارسة الولاية القضائية وأداء الوظائف التي يناط أداؤها حصراً بسلطات تلك الدولة الأخرى بمقتضى قانونها الداخلي.

## الفصل الثاني

## التجريم

**المادة الخامسة : التجريم:**

تلتزم كل دولة طرف بتجريم الأفعال المبينة في هذا الفصل، وذلك وفقاً لتشريعاتها وأنظمتها الداخلية.

**المادة السادسة : جريمة الدخول غير المشروع :**

1- الدخول أو البقاء وكل اتصال غير مشروع مع كل أو جزء من تقنية المعلومات أو الاستمرار به.
2- تشدد العقوبة إذا ترتب على هذا الدخول أو البقاء أو الاتصال أو الاستمرار بهذا الاتصال:
أ-محو أو تعديل أو تشويه أو نسخ أو نقل أو تدمير للبيانات المحفوظة وللأجهزة والأنظمة الالكترونية وشبكات الاتصال وإلحاق الضرر بالمستخدمين والمستفيدين.
ب- الحصول على معلومات حكومية سرية.

**المادة السابعة : جريمة الاعتراض غير المشروع :**

الاعتراض المتعمد بدون وجه حق لخط سير البيانات بأي من الوسائل الفنية وقطع بث أو استقبال بيانات تقنية المعلومات.

**المادة الثامنة : الاعتداء على سلامة البيانات :**

1- تدمير أو محو أو إعاقة أو تعديل أو حجب بيانات تقنية المعلومات قصدا وبدون وجه حق.
2- للطرف أن يستلزم لتجريم الأفعال المنصوص عليها في الفقرة (1) من هذه المادة، أن تتسبب بضرر جسيم.

**المادة التاسعة : جريمة إساءة استخدام وسائل تقنية المعلومات :**

1- إنتاج أو بيع أو شراء أو استيراد أو توزيع أو توفير:

أ - أية أدوات أو برامج مصممة أو مكيفة لغايات ارتكاب الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

ب- كلمة سر نظام معلومات أو شيفرة دخول او معلومات مشابهة يتم بواسطتها دخول نظام معلومات ما بقصد استخدامها لأية من الجرائم المبينة في المادة السادسة إلى المادة الثامنة.

2- حيازة أية أدوات أو برامج مذكورة في الفقرتين أعلاه، بقصد استخدامها لغايات ارتكاب أي من الجرائم المذكورة في المادة السادسة إلى المادة الثامنة.

**المادة العاشرة : جريمة التزوير :**

استخدام وسائل تقنية المعلومات من أجل تغيير الحقيقة في البيانات تغييراً من شأنه إحداث ضرر، وبنية استعمالها كبيانات صحيحة.

**المادة الحادية عشرة : جريمة الاحتيال :**

التسبب بإلحاق الضرر بالمستفيدين والمستخدمين عن قصد وبدون وجه حق بنية الاحتيال لتحقيق المصالح والمنافع بطريقة غير مشروعة، للفاعل أو للغير، عن طريق:
1- إدخال أو تعديل أو محو أو حجب للمعلومات والبيانات.
2- التدخل في وظيفة أنظمة التشغيل وأنظمة الاتصالات أو محاولة تعطيلها أو تغييرها.

3- تعطيل الأجهزة والبرامج والمواقع الالكترونية.

**المادة الثانية عشرة : جريمة الإباحية :**

1- انتاج أو عرض أو توزيع أو توفير أو نشر أو شراء أو بيع أو استيراد مواد إباحية أو مخلة بالحياء بواسطة تقنية المعلومات.
2- تشدد العقوبة على الجرائم المتعلقة بإباحية الأطفال والقصر.
3- يشمل التشديد الوارد في الفقرة ( 2 ) من هذه المادة، حيازة مواد إباحية الأطفال والقصر أو مواد مخلة بالحياء للأطفال والقصر على تقنية المعلومات أو وسيط تخزين تلك التقنيات.

**المادة الثالثة عشرة : الجرائم الأخرى المرتبطة بالإباحية :**

المقامرة والاستغلال الجنسي.

**المادة الرابعة عشرة : جريمة الاعتداء على حرمة الحياة الخاصة :**

الاعتداء على حرمة الحياة الخاصة بواسطة تقنية المعلومات .

**المادة الخامسة عشرة : الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات :**

1- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
2- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
3- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
4- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

**المادة السادسة عشرة : الجرائم المتعلقة بالجرائم المنظمة والمرتكبة بواسطة تقنية المعلومات :**

1- القيام بعمليات غسل أموال أو طلب المساعدة أو نشر طرق القيام بغسل الأموال.
2- الترويج للمخدرات والمؤثرات العقلية أو الاتجار بها.
3- الاتجار بالأشخاص.
4- الاتجار بالأعضاء البشرية.
5- الاتجار غير المشروع بالأسلحة.

**المادة السابعة عشرة : الجرائم المتعلقة بانتهاك حق المؤلف والحقوق المجاورة :**

انتهاك حق المؤلف كما هو معرف حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي، وانتهاك الحقوق المجاورة لحق المؤلف ذات الصلة كما هي معرفة حسب قانون الدولة الطرف، وذلك إذا ارتكب الفعل عن قصد ولغير الاستعمال الشخصي.

**المادة الثامنة عشرة : الاستخدام غير المشروع لأدوات الدفع الالكترونية :**

1- كل من زور أو اصطنع أو وضع أي أجهزة أو مواد تساعد على تزوير أو تقليد أي أداة من أدوات الدفع الالكترونية بأي وسيلة كانت.

2- كل من استولى على بيانات أي أداة من أدوات الدفع واستعملها أو قدمها للغير أو سهّل للغير الحصول عليها.
3- كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في الوصول بدون وجه حق إلى أرقام أو بيانات أي أداة من أدوات الدفع.
4- كل من قبل أداة من أدوات الدفع المزورة مع العلم بذلك.

**المادة التاسعة عشرة : الشروع والاشتراك في ارتكاب الجرائم:**

1- الاشتراك في ارتكاب أية جريمة من الجرائم المنصوص عليها في هذا الفصل مع وجود نية ارتكاب الجريمة في قانون الدولة الطرف.
2- الشروع في ارتكاب الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية.
3- يجوز لأي دولة طرف الاحتفاظ بحقها في عدم تطبيق الفقرة الثانية من هذه المادة كلياً أو جزئياً.

**المادة العشرون : المسؤولية الجنائية للأشخاص الطبيعية والمعنوية:**

تلتزم كل دولة طرف، مع مراعاة قانونها الداخلي، بترتيب المسؤولية الجزائية للأشخاص الاعتبارية عن الجرائم التي يرتكبها ممثلوها باسمها أو لصالحها دون الإخلال بفرض العقوبة على الشخص الذي يرتكب الجريمة شخصياً.

**المادة الحادية والعشرون : تشديد العقوبات على الجرائم التقليدية المرتكبة بواسطة تقنية المعلومات:**

تلتزم كل دولة طرف بتشديد العقوبات على الجرائم التقليدية في حال ارتكابها بواسطة تقنية المعلومات.

## الفصل الثالث

## الأحكام الإجرائية

**المادة الثانية والعشرون : نطاق تطبيق الأحكام الإجرائية:**

1- تلتزم كل دولة طرف بأن تتبنى في قانونها الداخلي التشريعات والاجراءات الضرورية لتحديد الصلاحيات والإجراءات الواردة في الفصل الثالث من هذه الاتفاقية.
2- مع مراعاة أحكام المادة التاسعة والعشرين، على كل دولة طرف تطبيق الصلاحيات والإجراءات المذكورة في الفقرة (1) على:
   أ- الجرائم المنصوص عليها في المواد السادسة إلى التاسعة عشرة من هذه الاتفاقية.
   ب- أية جرائم أخرى ترتكب بواسطة تقنية المعلومات.
   ج- جمع الأدلة عن الجرائم بشكل إلكتروني.
3- أ- يجوز لأي دولة طرف الاحتفاظ بحقها في تطبيق الإجراءات المذكورة في المادة التاسعة والعشرين فقط على الجرائم أو أصناف الجرائم المعنية في التحفظ بشرط أن لا

يزيد عدد هذه الجرائم على عدد الجرائم التي تطبق عليها الإجراءات المذكورة في المادة الثلاثين، وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادة التاسعة والعشرين.

ب- كما يجوز للدولة الطرف أن تحتفظ بحقها في عدم تطبيق تلك الإجراءات كلما كانت غير قادرة بسبب محدودية التشريع على تطبيقها على الاتصالات التي تبث بواسطة تقنية معلومات لمزود خدمة، وذلك إذا كانت التقنية:

- يتم تشغيلها لصالح مجموعة مغلقة من المستخدمين.
- لا تستخدم شبكات اتصال عامة وليست مرتبطةً بتقنية معلومات أخرى سواء كانت عامة أو خاصة.

وعلى كل دولة طرف أن تأخذ بعين الاعتبار محدودية التحفظ لإتاحة التطبيق الواسع للإجراءات المذكورة في المادتين التاسعة والعشرين والثلاثين.

**المادة الثالثة والعشرون : التحفظ العاجل على البيانات المخزنة في تقنية المعلومات :**

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأمر أو الحصول على الحفظ العاجل للمعلومات المخزنة بما في ذلك معلومات تتبع المستخدمين والتي خزنت على تقنية معلومات وخصوصاً إذا كان هناك اعتقاد أن تلك المعلومات عرضة للفقدان أو التعديل.

2- تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يتعلق بالفقرة (1) بواسطة إصدار أمر إلى شخص من أجل حفظ معلومات تقنية المعلومات المخزنة والموجودة بحيازته أو سيطرته ومن أجل إلزامه بحفظ وصيانة سلامة تلك المعلومات لمدة أقصاها 90 يوماً قابلة للتجديد، من أجل تمكين السلطات المختصة من البحث والتقصي.

3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لإلزام الشخص المسؤول عن حفظ تقنية معلومات للابقاء على سرية الإجراءات طوال الفترة القانونية المنصوص عليها في القانون الداخلي.

**المادة الرابعة والعشرون : التحفظ العاجل والكشف الجزئي لمعلومات تتبع المستخدمين :**

**تلتزم كل دولة طرف بتبني الإجراءات الضرورية فيما يختص بمعلومات تتبع المستخدمين من أجل :**

1 - ضمان توفر الحفظ العاجل لمعلومات تتبع المستخدمين بغض النظر عن اشتراك واحد أو أكثر من مزودي الخدمة في بث تلك الاتصالات.

2- ضمان الكشف العاجل للسلطات المختصة لدى الدولة الطرف أو لشخص تعينه تلك السلطات لمقدار كاف من معلومات تتبع المستخدمين لتمكين الدولة الطرف من تحديد مزودي الخدمة ومسار بث الاتصالات.

**المادة الخامسة والعشرون : أمر تسليم المعلومات :**

تلتزم كل دولة طرف بتبني الاجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى :

1 - أي شخص في إقليمها لتسليم معلومات معينة في حيازة ذلك الشخص والمخزنة على تقنية معلومات أو وسيط تخزين معلومات.

2 - أي مزود خدمة يقدم خدماته في إقليم الدولة الطرف لتسليم معلومات المشترك المتعلقة بتلك الخدمات في حوزة مزود الخدمه أو تحت سيطرته.

**المادة السادسة والعشرون : تفتيش المعلومات المخزنة :**

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين سلطاتها المختصة من التفتيش أو الوصول إلى :

أ - تقنية معلومات أو جزء منها والمعلومات المخزنة فيها أو المخزنة عليها.

ب - بيئة أو وسيط تخزين معلومات تقنية معلومات والذي قد تكون معلومات التقنية مخزنة فيه أو عليه.

2 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من التفتيش أو الوصول إلى تقنية معلومات معينة أو جزء منها بما يتوافق مع الفقرة ( 1 - أ ) اذا كان هناك اعتقاد بأن المعلومات المطلوبة مخزنة في تقنية معلومات أخرى أو جزء منها في إقليمها وكانت هذه المعلومات قابلة للوصول قانوناً أو متوفرة في التقنية الأولى فيجوز توسيع نطاق التفتيش والوصول للتقنية الأخرى.

**المادة السابعة والعشرون : ضبط المعلومات المخزنة :**

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من ضبط وتأمين معلومات تقنية المعلومات التي يتم الوصول إليها حسب الفقره ( 1 ) من المادة السادسة والعشرين من هذه الاتفاقية .

هذه الإجراءات تشمل صلاحيات :

أ - ضبط وتأمين تقنية المعلومات أو جزء منها أو وسيط تخزين معلومات تقنية المعلومات .

ب - عمل نسخة من معلومات تقنية المعلومات والاحتفاظ بها .

ج - الحفاظ على سلامة معلومات تقنية المعلومات المخزنة.

د - إزالة أو منع الوصول إلى تلك المعلومات في تقنية المعلومات التي يتم الوصول إليها .

3- تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من إصدار الأوامر إلى أي شخص لديه معرفة بوظيفة تقنية المعلومات أو الإجراءات المطبقة لحماية تقنية المعلومات من أجل تقديم المعلومات الضرورية لإتمام تلك الإجراءات المذكورة في الفقرتين ( 2,1 ) من المادة السادسة والعشرين من هذه الاتفاقية.

**المادة الثامنة والعشرون : الجمع الفوري لمعلومات تتبع المستخدمين :**

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لتمكين السلطات المختصة من :

أ - جمع أو تسجيل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف.

ب - إلزام مزود الخدمة ضمن اختصاصة الفني بأن :

- يجمع أو يسجل بواسطة الوسائل الفنية على إقليم تلك الدولة الطرف،أو
- يتعاون ويساعد السلطات المختصة في جمع وتسجيل معلومات تتبع المستخدمين بشكل فوري مع الاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية المعلومات.

2 - إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقره ( 1 – أ ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع أو التسجيل الفوري لمعلومات تتبع المستخدمين المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3 - تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود الخدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

**المادة التاسعة والعشرون : إعتراض معلومات المحتوى :**

1 - تلتزم كل دولة طرف بتبني الإجراءات التشريعية والضرورية فيما يختص بسلسلة من الجرائم المنصوص عليها في القانون الداخلي، لتمكين السلطات المختصة من :

أ - الجمع أو التسجيل من خلال الوسائل الفنية على إقليم الدولة الطرف، أو

ب - التعاون ومساعدة السلطات المختصة في جمع أو تسجيل معلومات المحتوى بشكل فوري للاتصالات المعنية في إقليمها والتي تبث بواسطة تقنية معلومات .

2 - إذا لم تستطع الدولة الطرف بسبب النظام القانوني الداخلي تبني الإجراءات المنصوص عليها في الفقرة ( 1 – أ ) فيمكنها تبني إجراءات أخرى بالشكل الضروري لضمان الجمع والتسجيل الفوري لمعلومات المحتوى المرافقة للاتصالات المعنية في إقليمها باستخدام الوسائل الفنية في ذلك الإقليم.

3- تلتزم كل دولة طرف باتخاذ الإجراءات الضرورية لإلزام مزود خدمة بالاحتفاظ بسرية أية معلومة عند تنفيذ الصلاحيات المنصوص عليها في هذه المادة.

## الفصل الرابع

## التعاون القانوني والقضائي

**المادة الثلاثون : الاختصاص :**

1 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد اختصاصها على أي من الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية وذلك إذا ارتكبت الجريمة كلياً أو جزئياً أو تحققت :

أ - في إقليم الدولة الطرف.

ب- على متن سفينة تحمل علم الدولة الطرف.

ج- على متن طائرة مسجلة تحت قوانين الدولة الطرف.

د- من قبل أحد مواطني الدولة الطرف إذا كانت الجريمة يعاقب عليها حسب القانون الداخلي في مكان ارتكابها أو إذا ارتكبت خارج منطقة الاختصاص القضائي لأية دولة.

هـ- إذا كانت الجريمة تمس أحد المصالح العليا للدولة.

2 - تلتزم كل دولة طرف بتبني الإجراءات الضرورية لمد الاختصاص الذي يغطي الجرائم المنصوص عليها في المادة الحادية والثلاثين الفقرة (1) من هذه الاتفاقية في الحالات التي يكون فيها الجاني المزعوم حاضراً في إقليم تلك الدولة الطرف ولا يقوم بتسليمه إلى طرف آخر بناء على جنسيته بعد طلب التسليم.

3- إذا ادعت أكثر من دولة طرف بالاختصاص القضائي لجريمة منصوص عليها في هذه الاتفاقية فيقدم طلب الدولة التي أخلت الجريمة بأمنها أو بمصالحها ثم الدولة التي وقعت الجريمة في إقليمها ثم الدولة التي يكون الشخص المطلوب من رعاياها وإذا اتحدت الظروف فتقدم الدولة الأسبق في طلب التسليم.

**المادة الحادية والثلاثون : تسليم المجرمين :**

1- أ- هذه المادة تنطبق على تبادل المجرمين بين الدول الأطراف على الجرائم المنصوص عليها في الفصل الثاني من هذه الاتفاقية بشرط أن تكون تلك الجرائم يعاقب عليها في قوانين الدول الاطراف المعنية بسلب الحرية لفترة أدناها سنة واحدة أو بعقوبة أشد.

ب- إذا انطبقت عقوبة أدنى مختلفة حسب ترتيب متفق عليه أو حسب معاهدة تسليم المجرمين فإن العقوبة الدنيا هي التي سوف تطبق.

2- إن الجرائم المنصوص عليها في الفقرة (1) من هذه المادة تعتبرجرائم قابلة لتسليم المجرمين الذين يرتكبونها في أية معاهدة لتسليم المجرمين قائمة بين الدول الأطراف.

3- إذا قامت دولة طرف ما بجعل تسليم المجرمين مشروطا بوجود معاهدة وقامت باستلام طلب لتسليم المجرمين من دولة طرف أخرى ليس لديها معاهدة تسليم فيمكن اعتبار هذه الاتفاقية كأساس قانوني لتسليم المجرمين فيما يتعلق بالجرائم المذكورة في الفقرة (1) من هذه المادة.

4- الدول الأطراف التي لا تشترط وجود معاهدة لتبادل المجرمين يجب أن تعتبر الجرائم المذكورة في الفقرة (1) من هذه المادة قابلة لتسليم المجرمين بين تلك الدول.

5- يخضع تسليم المجرمين للشروط المنصوص عليها في قانون الدولة الطرف التي يقدم إليها الطلب أو لمعاهدات التسليم المطبقة بما في ذلك الأسس التي يمكن للدولة الطرف الاستناد عليها لرفض تسليم المجرمين.

6- يجوز لكل دولة طرف من الأطراف المتعاقدة أن تمتنع عن تسليم مواطنيها وتتعهد في الحدود التي يمتد إليها اختصاصها، بتوجيه الاتهام ضد من يرتكب منهم لدى أي من الدول الأطراف الأخرى جرائم معاقباً عليها في قانون كل من الدولتين بعقوبة سالبة للحرية مدتها سنة أو بعقوبة أشد لدى أي من الطرفين المتعاقدين وذلك إذا ما وجهت إليها الدولة الطرف الأخرى طلباً بالملاحقة مصحوبا بالملفات والوثائق والأشياء والمعلومات التي تكون في حيازتها وتحاط الدولة الطرف الطالبة علما بما يتم في شأن طلبها، وتحدد الجنسية في تاريخ وقوع الجريمة المطلوب من أجلها التسليم.

7- أ- تلتزم كل دولة طرف وقت التوقيع أو إيداع أداة التصديق أو القبول أن تقوم بإيصال اسم وعنوان السلطة المسؤولة عن طلبات تسليم المجرمين أو التوقيف الإجرائي في

ظل غياب معاهدة إيصال هذه المعلومات إلى الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب.

ب- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل السلطات المعنية من قبل الدول الأطراف وعلى كل دولة طرف أن تضمن أن تفاصيل السجل صحيحة دائماً.

**المادة الثانية والثلاثون : المساعدة المتبادلة :**

1- على جميع الدول الأطراف تبادل المساعدة فيما بينها بأقصى مدى ممكن لغايات التحقيقات أو الإجراءات المتعلقة بجرائم معلومات وتقنية المعلومات أو لجمع الأدلة الالكترونية في الجرائم.

2- تلتزم كل دولة طرف بتبنى الإجراءات الضرورية من أجل تطبيق الالتزامات الواردة في المواد من الرابعة والثلاثين إلى المادة الثانية والأربعين.

3- يتم تقديم طلب المساعدة الثنائية والاتصالات المتعلقة بها بشكل خطي، ويجوز لكل دولة طرف في الحالات الطارئة أن تقدم هذا الطلب بشكل عاجل بما في ذلك الفاكس أو البريد الالكتروني على أن تضمن هذه الاتصالات القدر المعقول من الأمن والمرجعية (بما في ذلك إستخدام التشفير ) وتأكيد الإرسال حسبما تطلب الدولة الطرف ويجب على الدولة الطرف المطلوب منها المساعدة أن تقبل وتستجيب للطلب بوسيلة عاجلة من الاتصالات.

4- باستثناء ما يرد فيه نص في هذا الفصل فإن المساعدة الثنائية خاضعة للشروط المنصوص عليها في قانون الدولة الطرف المطلوب منها المساعدة أو في معاهدات المساعدة المتبادلة بما في ذلك الأسس التي يمكن للدولة الطرف المطلوب منها المساعدة الاعتماد عليها لرفض التعاون. ولا يجوز للدولة الطرف المطلوب منها أن تمارس حقها في رفض المساعدة فيما يتعلق بالجرائم المنصوص عليها في الفصل الثاني فقط بناء على كون الطلب يخص جريمة يعتبرها من الجرائم المالية.

5- حيثما يسمح للدولة الطرف المطلوب منها المساعدة المتبادلة بشرط وجود ازدواجية التجريم، فإن هذا الشرط يعتبر حاصلاً بغض النظر عما إذا كانت قوانين الدولة الطرف تصنف الجريمة في نفس تصنيف الدولة الطرف الطالبة وذلك إذا كان الفعل الذي يمهد للجريمة التي تطلب المساعدة فيها يعتبر جريمة بحسب قوانين الدولة الطرف.

**المادة الثالثة والثلاثون : المعلومات العرضية المتلقاة :**

1- يجوز لأي دولة طرف ـ ضمن حدود قانونها الداخلي- وبدون طلب مسبق أن تعطي لدولة أخرى معلومات حصلت عليها من خلال تحقيقاتها إذا اعتبرت أن كشف مثل هذه المعلومات يمكن أن تساعد الدولة الطرف المرسلة إليها في إجراء الشروع أو القيام بتحقيقات في الجرائم المنصوص عليها في هذه الاتفاقية أو قد تؤدي إلى طلب للتعاون من قبل تلك الدولة الطرف.

2- قبل إعطاء مثل هذه المعلومات يجوز للدولة الطرف المزودة أن تطلب الحفاظ على سرية المعلومات, وإذا لم تستطع الدولة الطرف المستقبلة الالتزام بهذا الطلب يجب عليها إبلاغ الدولة الطرف المزودة بذلك والتي تقرر بدورها مدى إمكانية التزويد بالمعلومات، وإذا قبلت الدولة الطرف المستقبلة المعلومات مشروطة بالسرية فيجب أن تبقى المعلومات بين الطرفين.

**المادة الرابعة والثلاثون : الإجراءات المتعلقة بطلبات التعاون والمساعدة المتبادلة :**

1- تطبق بنود الفقرات ( 2- 9 ) من هذه المادة في حالة عدم وجود معاهدة أو اتفاقية مساعدة متبادلة وتعاون على أساس التشريع النافذ بين الدولة الطرف الطالبة والمطلوب منها، أما في حال وجودها فلا تطبق الفقرات المشار اليها إلا إذا اتفقت الأطراف المعنية على تطبيقها كاملة أو بشكل جزئي.

2- أ- على كل دولة طرف تحديد سلطة مركزية تكون مسؤولة عن إرسال وإجابة طلبات المساعدة المتبادلة وتنفيذ هذه الطلبات وإيصالها إلى السلطات المعنية لتنفيذها.

ب- على السلطات المركزية أن تتصل ببعضها مباشرة.

ج- على كل دولة طرف - وقت التوقيع أو إيداع أدوات التصديق أو القبول أو الموافقة- أن تتصل بالأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب وتنقل إليهما أسماء وعناوين السلطات المحددة خصيصا لغايات هذه الفقرة.

د- تقوم الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بإنشاء وتحديث سجل للسلطات المركزية والمعينة من قبل الدول الأطراف. وعلى كل دولة طرف أن تتأكد من أن التفاصيل الموجودة في السجل صحيحة دائماً.

3- يتم تنفيذ مطالب المساعدة المتبادلة في هذه المادة حسب الإجراءات المحددة من قبل الدولة الطرف الطالبة لها باستثناء حالة عدم التوافق مع قانون الدولة الطرف المطلوب منها المساعدة.

4- يجوز للدولة الطرف المطلوب منها المساعدة أن تؤجل الإجراءات المتخذة بشأن الطلب إذا كانت هذه الإجراءات تؤثر على التحقيقات الجنائية التي تجري من قبل سلطاتها.

5- قبل رفض أو تأجيل المساعدة يجب على الدولة الطرف المطلوب منها المساعدة بعد استشارة الدولة الطرف الطالبة لها أن تقرر فيما إذا سيتم تلبية الطلب جزئياً أو يكون خاضعاً للشروط التي قد تراها ضرورية.

6- تلتزم الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بنتيجة تنفيذ الطلب , وإذا تم رفض أو تأجيل الطلب يجب إعطاء أسباب هذا الرفض أو التأجيل، ويجب على الدولة الطرف المطلوب منها المساعدة أن تعلم الدولة الطرف الطالبة لها بالأسباب التي تمنع تنفيذ الطلب بشكل نهائي أو الأسباب التي تؤخره بشكل كبير.

7- يجوز للدولة الطرف الطالبة للمساعدة أن تطلب من الطرف المطلوب منها المساعدة الإبقاء على سرية حقيقة ومضمون أي طلب يندرج في هذا الفصل ما عدا القدر الكافي لتنفيذ الطلب , وإذا لم تستطع الدولة الطرف المطلوب منها المساعدة الالتزام بهذا الطلب للسرية يجب عليها إعلام الدولة الطرف الطالبة والتي ستقرر مدى إمكانية تنفيذ الطلب.

8- أ- في الحالات العاجلة يجوز إرسال طلبات المساعدة المتبادلة مباشرة إلى السلطات القضائية في الدولة الطرف المطلوب منها المساعدة من نظيرتها في الدولة الطرف الطالبة لها، وفي مثل هذه الحالات يجب إرسال نسخة في نفس الوقت من السلطة المركزية في الدولة الطرف الطالبة إلى نظيرتها في الدولة الطرف المطلوب منها.

ب- يجوز عمل الاتصالات وتقديم الطلبات حسب هذه الفقرة بواسطة الإنتربول.

ج- حيثما يتم تقديم طلب حسب الفقرة(أ ) ولم تكن السلطة مختصة بالتعامل مع الطلب فيجب عليها إحالة الطلب إلى السلطة المختصة وإعلام الدولة الطرف الطالبة للمساعدة مباشرة بذلك.

د- إن الاتصالات والطلبات التي تتم حسب هذه الفقرة والتي لا تشمل الإجراء القسري يمكن بثها مباشرة من قبل السلطات المختصة في الدولة الطرف الطالبة للمساعدة إلى نظيرتها في الدولة الطرف المطلوب منها المساعدة.

هـ- يجوز لكل دولة طرف، وقت التوقيع أو التصديق أو القبول أو الإقرار أو الإنضمام إبلاغ الأمانة العامة لمجلس وزراء الداخلية العرب والأمانة الفنية لمجلس وزراء العدل العرب بأن الطلبات حسب هذه الفقرة يجب توجيهها إلى السلطة المركزية لغايات الفعالية.

**المادة الخامسة والثلاثون : رفض المساعدة :**

يجوز للدولة الطرف المطلوب منها المساعدة - بالاضافة إلى أسس الرفض المنصوص عليها في المادة الثانية والثلاثين الفقرة ( 4 ) أن ترفض المساعدة إذا:

1- كان الطلب متعلقاً بجريمة يعتبرها قانون الدولة الطرف المطلوب منها المساعدة جريمة سياسية.

2- اعتبر أن تنفيذ الطلب يمكن أن يشكل انتهاكاً لسيادته أو أمنه أو نظامه أو مصالحه الأساسية.

**المادة السادسة والثلاثون : السرية وحدود الاستخدام :**

1- عندما لايكون هناك معاهدة أو اتفاق للمساعدة المتبادلة على أساس التشريع الساري بين الدول الأطراف الطالبة والمطلوب منها فيجب تطبيق بنود هذه المادة ولا يتم تطبيقها إذا وجدت مثل هذه الاتفاقية أو المعاهدة إلا إذا اتفقت الدول الأطراف المعنية على تطبيق أي من فقرات هذه المادة أو كلها.

2- يجوز للدولة الطرف المطلوب منها توفير المعلومات أو المواد الموجودة في الطلب بشرط:

أ - الحفاظ على عنصر السرية للدولة الطرف الطالبة للمساعدة ولا يتم الالتزام بالطلب في غياب هذا العنصر.

ب- عدم استخدام المعلومات في تحقيقات أخرى غير الواردة في الطلب.

3- إذا لم تستطع الدولة الطرف الطالبة الالتزام بالشرط الوارد في الفقرة ( 2 ) فيجب عليها إعلام الدولة الطرف الأخرى والتي ستقرر بعدها مدى إمكانية توفير المعلومات، وإذا قبلت الدولة الطرف الطالبة بهذا الشرط فهو ملزم لها.

4- أي دولة طرف توفر المعلومات أو المواد بحسب الشرط في الفقرة ( 2 ) لتوفير المعلومات يجوز لها أن تطلب من الدولة الطرف الأخرى أن تبرر استخدام المعلومات أو المواد.

**المادة السابعة والثلاثون : الحفظ العاجل للمعلومات المخزنة على أنظمة المعلومات :**

1- لأي دولة طرف أن تطلب من دولة طرف أخرى الحصول على الحفظ العاجل للمعلومات المخزنة على تقنية المعلومات تقع ضمن إقليمها بخصوص ما تود الدولة الطرف الطالبة للمساعدة أن تقدم طلباً بشأنه للمساعدة المتبادلة للبحث وضبط وتأمين وكشف المعلومات.

2- يجب أن يحدد طلب الحفظ حسب الفقرة ( 1 ) ما يلي:

أ- السلطة التي تطلب الحفظ.

ب- الجريمة موضوع التحقيق وملخصاً للوقائع.

ج- معلومات تقنية المعلومات التي يجب حفظها وعلاقتها بالجريمة.

د- أيـة معلومـات متـوفرة لتحديـد المسـؤول عـن المعلومـات المخزنـة أو موقـع تقنيـة المعلومات.

هـ- موجبات طلب الحفظ.

و- رغبة الدولة الطرف بتسليم طلب المساعدة الثنائية للبحث أو الوصـول أو الضبط أو تأمين أو كشف معلومات تقنية المعلومات المخزنة.

3- عند استلام إحدى الدول الأطراف الطلب من دولة طرف أخرى فعليها أن تتخذ جميع الإجراءات المناسبة لحفظ المعلومات المحددة بشكل عاجل بحسب قانونها الداخلي، ولغايات الاستجابة إلى الطلب فلا يشترط وجود إزدواجية التجريم للقيام بالحفظ.

4- أي دولة طرف تشترط وجود ازدواجية التجريم للاستجابة لطلب المساعدة يجوز لها في حالات الجرائم عدا المنصوص عليها في الفصل الثاني من هذه الاتفاقية ، أن تحتفظ بحقها برفض طلب الحفظ حسب هذه المادة إذا كان هناك سبب للاعتقاد بأنه لن يتم تلبية شرط ازدواجية التجريم في وقت الكشف.

5- بالاضافة لذلك، يمكن رفض طلب الحفظ إذا :

أ- تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية.

ب- إعتبار الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سيادتها أو أمنها أو نظامها أو مصالحها.

6- حيثما تعتقد الدولة الطرف المطلوب منها المساعدة بأن الحفظ لن يضمن التوفر المستقبلي للمعلومات أو سيهدد سرية تحقيقات الدولة الطرف الطالبة لها أو سلامتها فيجب عليها إعلام الدولة الطرف الطالبة لها لتحدد بعدها مدى إمكانية تنفيذ الطلب.

7- أي حفظ ناجم عن الاستجابة للطلب المذكور في الفقرة ( 1 ) يجب أن يكون لفترة لا تقل عن ( 60 ) يوماً من أجل تمكين الدولة الطرف الطالبة من تسليم طلب البحث أو الوصول أو الضبط أو التأمين أو الكشف للمعلومات . وبعد إستلام مثل هذا الطلب يجب الاستمرار بحفظ المعلومات حسب القرار الخاص بالطلب.

**المادة الثامنة والثلاثون : الكشف العاجل لمعلومات تتبع المستخدمين المحفوظة :**

1 - حيثما تكتشف الدولة الطرف المطلوب منها - في سياق تنفيذ الطلب حسب المادة السابعة والثلاثين لحفظ معلومات تتبع المستخدمين الخاصة باتصالات معينة - بأن مزود خدمة في دولة أخرى قد اشترك في بث الاتصال فيجب على الدولة الطرف المطلوب منها أن تكشف للدولة الطرف الطالبة قدراً كافياً من معلومات تتبع المستخدمين من أجل تحديد مزود الخدمة ومسار بث الاتصالات.

2 - يمكن تعليق كشف معلومات تتبع المستخدمين حسب الفقره ( 1 ) إذا:

أ - تعلق الطلب بجريمة تعتبرها الدولة الطرف المطلوب منها جريمة سياسية.

ب- اعتبرت الدولة الطرف المطلوب منها بأن تنفيذ الطلب قد يهدد سلامتها أو أمنها أو نظامها أو مصالحها .

**المادة التاسعة والثلاثون : التعاون والمساعدة الثنائية المتعلقة بالوصول إلى معلومات تقنية المعلومات المخزنة:**

1- يجوز لأي دولة طرف أن تطلب من دولة طرف أخرى البحث أو الوصول أو الضبط أو التأمين أو الكشف لمعلومات تقنية المعلومات المخزنة والواقعة ضمن أراضى الدولة الطرف المطلوب منها بما في ذلك المعلومات التي تم حفظها بحسب المادة السابعة والثلاثين.

2- تلتزم الدولة الطرف المطلوب منها بأن تستجيب للدولة الطرف الطالبة وفقاً للأحكام الواردة في هذه الاتفاقية.

3- تتم الإجابة على الطلب على أساس عاجل إذا كانت المعلومات ذات العلاقة عرضه للفقدان أو التعديل.

**المادة الأربعون : الوصول إلى معلومات تقنية المعلومات عبر الحدود :**

يجوز لأي دولة طر، وبدون الحصول على تفويض من دولة طرف أخرى:

1- أن تصل إلى معلومات تقنية المعلومات المتوفرة للعامة (مصدر مفتوح) بغض النظر عن الموقع الجغرافي للمعلومات .

2- أن تصل أو تستقبل - من خلال تقنية المعلومات في إقليمها - معلومات تقنية المعلومات الموجودة لدى الدولة الطرف الأخرى وذلك إذا كانت حاصلة على الموافقة الطوعية والقانونية من الشخص الذي يملك السلطة القانونية لكشف المعلومات إلى تلك الدولة الطرف بواسطة تقنية المعلومات المذكورة.

**المادة الحادية والأربعون : التعاون والمساعدة الثنائية بخصوص الجمع الفوري لمعلومات تتبع المستخدمين:**

1- على الدول الأطراف توفير المساعدة الثنائية لبعضها البعض بخصوص الجمع الفوري لمعلومات تتبع المستخدمين المصاحبة لاتصالات معينه في أقاليمها والتي تبث بواسطة تقنية المعلومات.

2- على كل دولة طرف توفير تلك المساعدة على الأقل بالنسبة للجرائم التي يتوفر فيها الجمع الفوري لمعلومات تتبع المستخدمين لمثيلتها من القضايا الداخلية.

**المادة الثانية والأربعون : التعاون والمساعدة الثنائية فيما يخص المعلومات المتعلقة بالمحتوى :**

تلتزم الدول الأطراف بتوفير المساعدة الثنائية لبعضها فيما يتعلق بالجمع الفوري لمعلومات المحتوى لاتصالات معينه تبث بواسطة تقنية المعلومات إلى الحد المسموح بحسب المعاهدات المطبقة والقوانين المحلية .

**المادة الثالثة والأربعون : جهاز متخصص:**

1- تكفل كل دولة طرف، وفقاً للمبادئ الأساسية لنظامها القانوني، وجود جهاز متخصص ومتفرغ على مدار الساعة لضمان توفير المساعدة الفورية لغايات التحقيق أو الإجراءات

# TEAM

Dr Adel Abdel Moneim

Dr Mohamed Hamdi

Dr Kamel Rezgui

## COORDINATION

Sami Trimech

Nada Laabidi


AICTO
ARAB INFORMATION AND COMMUNICATION TECHNOLOGY ORGANIZATION


# ARAB INFORMATION & COMMUNICATION TECHNOLOGIES ORGANIZATION

The Arab ICT Organization (AICTO) is a specialized Arab governmental organization working under the aegis of the league of Arab States.

It aims at developing ICTs throughout the Arab region and providing the necessary mechanisms to support cooperation and complementarity between AICTO members, promote and enrich common policies and strategies to develop vital technological domains. AICTO is working with all stakeholders in the Arab region and other international partners to spread fair and sustainable access to technology and adapt it to serve the goals of economic development and achieve social advancement over the region.

---

Headquarters : Tunis, The Capital Of The Republic Of Tunisia
Address : 12 Rue D'angleterre, 1000 Tunis, Tunisia
Phone : +216 71 320 713 | Fax : +216 71 320 719
E-Mail : Contact@Aicto.org | Website : Www.aicto.org

TUNIS 21/10/2021