Egyptian Anti-Corruption Academy
(EACA)

English

French

The Role of International and Regional Agreements in Cybersecurity and Egypt's Position on Them

■ Judge:
Mohamed Ahmed Labib Ahmed
Vice President of the Court of Appeal

■ Judge:
Haitham Mohamed Bahaa El-Qadi
President of the Court of Appeal

■ Judge:
Mostafa Ahmed Kamal
Deputy of the State Council

■ Abstract:

Cybersecurity has become an indispensable field in our world due to the need to combat cyber-attacks and electronic crimes. Therefore, it is imperative for the international community to address this technological criminal invasion by enacting more legislative and punitive measures and procedural laws that match the severity of these crimes and by establishing necessary regulations to confront them.

For this purpose, various international organizations have taken several initiatives in the field of combating cybercrime, including the International Telecommunication Union, the National Institute of Standards and Technology, and the European Union Agency for Cybersecurity.

The European and international communities have also focused on regulating the field of information technology, making significant legislative efforts to combat the phenomenon of cybercrime. Among the most important of these efforts is the Budapest Convention on Cybercrime issued by the European Union, which aims primarily to harmonize the elements of substantive criminal law and provisions related to cybercrimes and to establish a rapid and effective system for international cooperation under the convention.

Additionally, the League of Arab States issued the Arab Convention on Combating Information Technology Crimes, aiming to enhance cooperation among Arab countries in the field of combating IT crimes.

Egypt has also witnessed strong momentum in the field of information and network security. The Supreme Council for Cybersecurity was established, chaired by the Minister of Communications and Information Technology, and includes representatives from the government, private sector, and civil society. Egypt also established the Egyptian Computer Emergency Readiness Team (EG-CERT), affiliated with the National Telecommunication Regulatory Authority, and created the Financial Sector Computer Emergency Readiness Team affiliated with the Central Bank. Furthermore, Egypt issued the National Cybersecurity Strategy for 2017-2021, followed by the National Cybersecurity Strategy for 2023-2027.

Keywords

Cybersecurity- Information Technology Agreements -Budapest Convention- Information Crime
Cybercrimes - Computer Emergency Response Team (CERT)- Cyber Attacks

Introduction:

The advent of computers and the expansion of Internet use have brought about some negative impacts and risks associated with this significant expansion. Consequently, attention has shifted toward cybersecurity, highlighting the critical importance of cooperation among international actors in establishing regulatory and institutional frameworks to coordinate various national efforts aimed at protecting cyberspace and addressing the growing cyber threats.

At the forefront of these efforts is the United Nations, along with several international organizations that have undertaken various initiatives in combating cybercrime. For instance, efforts by the International Telecommunication Union and the International Criminal Police Organization (Interpol) stand out.

In addition to the international efforts by the aforementioned organizations, there are also international initiatives by regional organizations. This became particularly evident when the Council of Europe convened in 2001 in Budapest, Hungary, where the European Convention on Cybercrime (Cybercrime Convention) was signed. This convention has since become the global legal framework for combating cybercrime.

The Arab League has also made efforts in this regard, issuing the Arab Convention on Combating Information Technology Offenses in 2010.

Egypt has witnessed significant activity in the field of information and network security. The country has worked towards establishing and building a system capable of protecting Egyptian cyberspace. The establishment of the Supreme Council for Cybersecurity and the creation of the Egyptian Computer Emergency Response Team (CERT) were key steps in this direction. Additionally, the Central Bank of Egypt established a CERT specifically for the financial sector. Egypt also issued its National Cybersecurity Strategy 2017–2021, followed by the National Cybersecurity Strategy 2023–2027.

I. Significance of the Research:

The advent of information and communication technology (ICT) has revolutionized all aspects of life and increased its dominance over the general pattern of life. The emergence of computers and the expansion of Internet use in various fields of life have brought about some negative impacts and risks associated with this significant expansion. The more reliance there is on these technologies for development, the greater the risks concerning information protection become. With the global increase in dependence on ICT, exposure to cybercrime has also escalated, making cyberspace vulnerable to violations by network hackers, whether they are states or other entities possessing this information technology.

Consequently, there has been a significant focus on cybersecurity, with the preservation of cybersecurity being equated with the preservation of national security for states. Therefore, cybersecurity has become a priority for many countries. The growing threats to cybersecurity have driven many nations to exert considerable efforts in developing laws to combat cybercrime. Thus, it has become essential to unify international efforts to establish legal, regulatory, and procedural frameworks to address cyber risks and their global impact, to confront the threats to cybersecurity, and to enhance forms of international cooperation in combating them (Abdel Halim, p. 20).

Based on this, the importance of the research lies in the novelty and ambiguity of cybersecurity threats for a wide sector of individuals, in the impact that cybersecurity attacks have on individuals, institutions, and entire societies, and finally in the global importance of protecting cybersecurity and countering the increasing cyberattacks. Consequently, there is a need to enrich the Arabic library with research efforts that contribute to bridging the knowledge gap and evaluating the current efforts made in Egypt in this field, with the aim of participating in proposing their development to achieve the national interest of the state.

II Research Objectives (Reasons for Choosing the Research Topic):

There is no doubt that the variation in national legislative frameworks, including laws, regulations, and rules enacted by different countries to combat cybercrime, is one of the difficulties facing the international community in coordinating efforts to curb this crime. Cybercriminals exploit this disparity, committing crimes across borders where the risk of law enforcement on criminals is lower compared to other countries.

National sovereignty of states is something that cannot be ignored, but the risks and challenges faced by the international community necessitate the coordination of efforts between countries to achieve the greater good for citizens. Therefore, it has become necessary to conclude international agreements to combat these crimes, establishing the broad guidelines that different countries should follow when developing legislative and regulatory frameworks to combat cybercrime.

III. Research Methodology:

Studying this topic requires a variety of research methods, rather than relying on a single approach, to serve the research objectives. Therefore, we will employ the following research methods in our study:

The theoretical approach to cybersecurity, which focuses on studying and analyzing the theories and concepts related to cybersecurity and applying them in practical contexts, understanding the theoretical foundations of cyber

threats and security measures. This will be achieved through studying published research and sources on cybersecurity by exploring scientific articles, books, and reports, leading to the analysis and interpretation of cyber behavior. This will contribute to understanding complex phenomena and processes and developing theories and frameworks that help improve cybersecurity strategies.

This study also aims to conduct an in-depth analysis of international legislation related to cybersecurity and document the findings, relying on the following methods:

1. **Inductive Method**: This method relies on examining the opinions of scholars and judicial rulings on the topics discussed in the research, to identify points of disagreement and determine the most prevailing views.

2. **Analytical Method**: This method is used to analyze existing texts to assess their relevance to the topics discussed in the research.

3. **Comparative Method**: This method involves comparing the legal situation in various international agreements.

Research Plan:

To provide a comprehensive understanding and establish a complete framework for our research topic, we have dedicated a preliminary section to discussing the nature of cybersecurity, divided as follows:

Requirement One: Introduction to cybersecurity and the terminology used in this field.
Requirement Two: A historical overview of cybersecurity.
Requirement Three: The importance of cybersecurity.
Requirement Four: The objectives of cybersecurity.

In the first chapter, we address international and regional agreements in the field of cybersecurity, detailed as follows:

Requirement One: The efforts of the United Nations in combating cybercrime.
Requirement Two: The efforts of international organizations in combating cybercrime.
Branch One: The role of the International Telecommunication Union (ITU) in cybersecurity.
Branch Two: The role of the National Institute of Standards and Technology (NIST) in cybersecurity.
Branch Three: The role of the European Union Agency for Cybersecurity (ENISA) in cybersecurity.

Requirement Three: The role of regional agreements in combating cybercrime.

Branch One: The Budapest Convention on Cybercrime.

Branch Two: The Arab Convention on Combating Information Technology Offenses.

In the second chapter, we discuss Egypt's efforts in the field of cybersecurity, which we have divided into six sections, detailed as follows:

Requirement One: The Supreme Council for Cybersecurity.

Requirement Two: The Egyptian Computer Emergency Response Team (CERT).

Requirement Three: The Financial and Banking Sector Computer Emergency Response Team.

Requirement Four: The National Cybersecurity Strategy of the Arab Republic of Egypt 2017-2021.

Requirement Five: The National Cybersecurity Strategy of the Arab Republic of Egypt 2023-2027.

Requirement Six: The outcomes of Egypt's efforts in the field of cybersecurity.

Introduction:

The Essence of Cybersecurity:

In this section, we aim to shed light on the essence of cybersecurity by first clarifying what is meant by cybersecurity and highlighting the key terms used in this field. Then, we will briefly review the historical background of cybersecurity to the extent that serves the objectives of this section. Next, we will discuss the increasing importance of cybersecurity, and finally, we will outline the main objectives of cybersecurity.

Requirement One: Definition of Cybersecurity and the Terms Used in This Field:

The term "cyber" refers to anything related to computers, various types of computer networks (such as the Internet), or electronic communications in general. The term "cyber" has come to denote everything associated with electronic computer networks and the Internet. For instance, when we say "cyberspace," we mean the electronic space. (Cambridge Dictionary)

As for the term "cybersecurity," there is no universally agreed-upon definition among different literatures and practitioners. However, it can be succinctly defined as the use of all necessary means to protect cyberspace from cyber-attacks. This involves a range of technical, regulatory, and administrative measures to prevent unauthorized access to electronic information and to prevent its illegal and improper exploitation. (Al-Anazi, 1443, p 22)

Several documents issued by some international governmental organizations, such as the International Telecommunication Union (ITU), have attempted to define cybersecurity. For example, the ITU-T Recommendation X.1205 defines cybersecurity as a collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user assets. The organization and user assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and stored information in the cyber environment.

From the above definition and the majority of other available definitions of the studied phenomenon "cybersecurity," we can infer that there are three fundamental elements or aspects of cybersecurity, which are as follows:

Prevention: Utilizing and implementing available policies, measures, and practices to obstruct any unauthorized potential access or breaches.

Detection: Identifying potential threats and vulnerabilities within protected systems and devices.

Response: Determining and implementing the best solutions necessary to stop, rectify, or mitigate the impact and consequences of security incidents and breaches.

The term "cyberspace," as defined by the National Institute of Standards and Technology (NIST) in the United States, refers to a global domain within the information environment, consisting of an interconnected network of information system infrastructures. This includes the Internet, telecommunications networks, computer systems, processors, and embedded control devices. (James, 2016, p34).

Finally, the term "cyber-attacks" refers to electronic assaults on a system, organization, or individual aimed at disrupting, stealing, or damaging assets. These assets may be digital (such as data, information, or user accounts), digital services (such as communications), or physical assets with electronic components (such as control systems in a building, aircraft, or nuclear refinery). Such attacks typically aim to compromise the confidentiality, integrity, or availability of digital assets.

Requirement Two: A Historical Overview of Cybersecurity:

The origins of cybersecurity trace back to the 1970s, a time when terms like spyware, viruses, and worms were not yet prevalent. As the rate of cybercrimes increased, these terms began appearing in daily news headlines. At the inception of cybersecurity, computers and the Internet were still under development, making it easier to identify potential threats to computers.

In the 1980s, scientist Robert T. Morris created the first computer virus, which received extensive media coverage due to its widespread impact and system disruptions. Morris was sentenced to prison and fined, a verdict that played a significant role in the development of cybersecurity laws.

The 1990s saw the continued evolution of cybersecurity alongside the advancement of computer viruses. The world became increasingly aware of electronic risks. One of the notable measures taken during this time was the implementation of web protection protocols such as HTTP, which provided users with secure access to the Internet.

The development of cyber-attacks and cybercrimes has continued to evolve, and so has cybersecurity, reaching the sophistication and complexity we see today. In the digital world we live in now, cybersecurity has become as crucial as military defense systems. Advanced cyber-attacks can cause damage that surpasses traditional warfare, both economically and in terms of human impact. Today, we rely on computers and the Internet for almost everything (Middleton Bruce, 2017, p 35).

Requirement Three: The Importance of Cybersecurity:

Modern technology is used in nearly every aspect of our daily activities. As the world becomes increasingly digital, individuals, businesses, and even governments heavily rely on modern technology. This makes cybersecurity essential and fundamental.

Statistics show a global increase in the frequency and cost of cybercrimes. Below are some of these statistics and estimates, clearly reflecting the growing number of cyber-attacks and the substantial financial losses resulting from cybercrimes. According to IBM's 2023 Cost of a Data Breach Report, "the average cost of a data breach in 2023 was $4.45 million, an increase of 15% over the past three years."

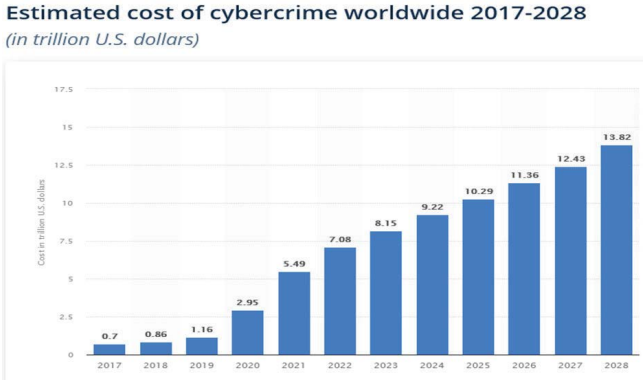


Figure1 "estimated cost of cybercrimes".(1)

In general, cyber-attacks have a severe impact on individuals, businesses, governments, and society at large. The following paragraphs will briefly highlight these effects.

Cyber-attacks can lead to financial losses through the hacking of financial

(1)-For a comprehensive reading of the emergence and evolution of Cyber Security, see A History of Cyber Security Attacks 1980 to Present, by Bruce Middleton, first edition 2017, Rout

See, "Cost of a Data Breach Report 2023", By IBM, which is a leading multinational computer software corporation, the report is available in the English language at https://www.ibm.com/reports/data-breach; last accessed 03/03/2024

accounts or unauthorized financial transactions. There is also the potential for identity theft, which can result in additional financial loss or even legal consequences. Additionally, the negative impact on reputation due to the publication of private information or photos can cause mental stress and psychological pressure.

The impact of cyber-attacks on businesses is critical, as such attacks can lead to:

1. **Operational Disruptions:** System failures or downtime, which can limit the company's ability to conduct business as usual.
2. **Financial Losses:** Costs incurred to repair the damage, such as restoring affected systems and devices, paying ransoms if unavoidable, potential loss of intellectual property, and resolving legal complexities arising from operational disruptions and non-compliance with laws.
3. **Reputational Damage:** Exposure of sensitive information, failure to provide services, or deliver products on time, which can negatively affect trust with various stakeholders, thereby undermining the institution's reputation and image. (Kala, 2023)Cyber-attacks can have several effects on governments, including:

1. **Operational Disruptions:** Disruption of critical public services such as healthcare and police services.

2. **Public Trust:** Damage to reputation, as citizens may become concerned about the quality and security of public services, and anxious about the potential exposure of their personal information from government databases.

3. **Financial Impact:** The cost of repairing damages caused by breaches can be substantial, and with the rise of ransomware attacks, some public institutions might find themselves compelled to pay ransoms to regain access to their data.

4. **National Security Concerns:** Cyber-attacks can target law enforcement or sensitive military agencies for purposes such as espionage, sabotage, or other malicious activities.

Given the significant risks and grave consequences of cyber-attacks, and the critical importance of cybersecurity, the International Monetary Fund (IMF) has recently recommended the necessity of international cooperation to enhance joint efforts in protecting financial institutions.(Nelson, Maurer,2021).

Requirement Four: Objectives of Cybersecurity:

The ultimate goal of cybersecurity is to secure devices, networks, and information, and to protect them from any type of breach or attack. To simplify the concept and establish security standards, even for cybersecurity experts, the CIA Triad model was developed. This model encompasses the three fundamental principles of cybersecurity:

1. Confidentiality: Equivalent to privacy, its goal is to prevent unauthorized access to data.

2. Integrity: Ensures that data remains accurate and unaltered from unauthorized modifications by hackers or unauthorized individuals.

3. Availability: Ensures that data is always accessible and usable by authorized individuals, guaranteeing that the system is not hindered or disrupted by various attacks. (Al-Samhani, 2020, p11)

Part One
International and Regional Agreements in the Field of Cybersecurity

In our discussion on the nature of cybersecurity, we highlighted the crucial importance of cooperation among international community actors, including states and international governmental and non-governmental organizations, towards establishing regulatory and institutional frameworks to coordinate the various national efforts made by countries to protect cyberspace and counter the increasing cyber threats, given their significant consequences as mentioned in the introductory chapter of this study.

Numerous international bodies, organizations, and councils play a notable role in facilitating and coordinating the establishment of international agreements in the field of cybersecurity. These efforts aim to solidify the necessity of international cooperation to combat cybercrimes, with the United Nations, the Council of Europe, and other organizations at the forefront.

Having examined the nature of cybersecurity, we now turn to the efforts of the United Nations in combating cybercrime, followed by the efforts of other international organizations in the same field. Finally, we will provide a brief overview of the role of regional agreements in combating cybercrime.

Requirement One
United Nations Efforts in Combating Cybercrime

The Economic and Social Council of the United Nations recommended that the international organization should take on a primary role in shaping crime prevention policy and achieving international criminal justice. This was realized with the United Nations General Assembly's approval in 1950 of the recommendation that led to the establishment of the Advisory Committee of Experts on the Prevention of Crime and the Treatment of Offenders. This committee was tasked with combating crime, advising the Secretary-General, creating programs, developing plans, and formulating policies for international

measures in crime prevention and the treatment of offenders. Following the United Nations Congress on the Prevention of Crime and the Treatment of Offenders in Kyoto, Japan, in 1970, the Advisory Committee was replaced by the Crime Prevention and Control Committee based on a recommendation from the Economic and Social Council in 1971.

In this study, we are particularly concerned with the United Nations' efforts through its conferences on crime prevention and the treatment of offenders, specifically regarding technical crimes or computer crimes. It is noteworthy that the Seventh United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in Milan, Italy, in 1985, produced a set of guidelines. These guidelines were completed in the preparatory regional research for the Eighth Congress, which approved these principles and was held in Havana, Cuba, in 1990. (Abayenah, 2009, p.156)

The Havana Congress emphasized the necessity of applying new scientific and technological developments globally for the public benefit and effective crime prevention. It also stressed that since technology can generate new forms of crime, appropriate measures must be taken against the misuse of modern technology. The Havana Congress of 1990 can be summarized with the following principles:

1. Updating national criminal laws, including institutional measures.
2. Enhancing computer security and robust measures.
3. Adopting adequate training procedures for employees and agencies responsible for dealing with economic crimes, computer-related crimes, investigation, and prosecution.
4. Incorporating computer ethics as part of the curriculum in communication and information courses and adopting policies to address issues related to victims of such crimes.
5. Increasing international cooperation to combat these crimes . (Abayenah, 2009, p.158)

Requirement Two
Efforts of Various International Organizations in Combating Cybercrime

Several international organizations have taken multiple initiatives in the field of combating cybercrime. Examples include the efforts of the International Telecommunication Union (ITU), the International Criminal Police Organization (Interpol), the Internet Corporation for Assigned Names and Numbers (ICANN), the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and Internet Engineering Task Forces (IETF), among other organizations and international institutions concerned with cybercrimes.

In the following paragraphs, we will discuss the most important efforts undertaken by some of the key international organizations in the field of cybersecurity. We will first cover the efforts of the International Telecommunication Union (ITU), then the efforts of the National Institute of Standards and Technology (NIST) in the United States, and finally, the efforts of the European Union Agency for Cybersecurity (ENISA).

Branch One
The Role of the International Telecommunication Union in Cybersecurity

The International Telecommunication Union (ITU) is a specialized United Nations agency in the field of information and communication technology (ICT). Founded in 1865, the ITU aims to facilitate global connectivity and improve international communications. It serves as the principal organization responsible for developing international ICT standards, promoting global connectivity, and enhancing access to ICTs worldwide(2).

In its efforts to fulfill its role in setting and developing international standards for the ICT community, the ITU has launched a guide for establishing a national cybersecurity strategy, which has been revised multiple times. In the latest edition of this guide, the ITU outlines and identifies the key actors in national cybersecurity ecosystems and the purpose of its creation. Twelve international partners, including the European Union Agency for Cybersecurity (ENISA), various intergovernmental organizations, international organizations, the private sector, and civil society, contributed to this guide.

The guide's primary purpose is outlined at the beginning: "to direct national leaders and policymakers in developing a national cybersecurity strategy, providing a useful, flexible, and user–friendly framework to define the context of the country's social and economic vision and current security posture."

The scope of the guide encompasses various aspects of cybersecurity challenges, including governance and policy, operational, technical, and legal aspects, and comprehensive principles and best practices to develop a strategy considering practical measures that countries take at different stages of the strategy and its actual content.

The intended audience of the guide includes national leaders and policymakers developing a national cybersecurity strategy, as well as other stakeholders such as government officials, regulatory bodies, ICT service providers, academic and research institutions.

The guide then discusses best practices in national cybersecurity strategy, focusing on specific concepts termed areas of focus:

(2) https://www.itu.int .

1. Governance: Establishing an effective and disciplined structure for national cybersecurity by setting clear goals and ambitions in the cybersecurity field, defining roles, and ensuring the highest level of support to achieve these goals. This also involves designating the responsible authority for implementing the cybersecurity strategy and engaging government agencies and other sectors affected by its implementation. The strategy should commit to setting specific, measurable, achievable, results-oriented, and time-bound objectives in its execution plan, recognizing the need to allocate resources (such as political will, funding, time, and personnel) to achieve satisfactory outcomes.

2. Cybersecurity Risk Management: This focus area involves adopting a national cybersecurity risk management approach, identifying and assessing the risks faced by the country, including cross-border dependencies and interrelationships, and managing these risks effectively. The risk management approach should cover the entire lifecycle, from provisioning to operation and replacement.

3. Preparedness and Resilience: Enhancing the ability of countries to deal with and withstand the effects of cyber-attacks by developing response and readiness capabilities to address and counter these attacks. This includes risk identification and assessment, developing contingency plans, establishing crisis management systems, and improving the verification capabilities of critical assets and services to ensure the continuity of infrastructure operations. It also involves providing training and awareness for information security teams in various institutions and conducting cybersecurity drills to enhance preparedness and resilience against cyber-attacks.

4. Critical Infrastructure and Essential Services: Enhancing the security of critical and essential infrastructure in countries by developing strategies to protect these assets and mitigate related risks. This includes identifying critical assets and services, developing risk management plans, providing security measures to protect these assets using advanced security technologies, and establishing continuous monitoring systems. Additionally, it involves providing training and awareness to information security teams in infrastructure institutions to raise their sensitivity to potential cyber threats and fostering cooperation among different stakeholders in this field.

5. Awareness, Capacity Building, and Raising Awareness: Strengthening the cybersecurity capabilities of individuals, institutions, and governments through developing training and educational programs to improve skills and expertise in this field. This includes strategies to

promote innovation in cybersecurity, supporting technical research, and developing new solutions for future challenges. It also involves raising awareness of the importance of cybersecurity through public awareness campaigns, media campaigns, and incorporating cybersecurity curricula in schools and universities.

6. Legislation and Regulation: Establishing a legal and regulatory framework to protect society from cybercrimes and encourage a secure and safe cyber environment. This includes defining illegal cyber activities, legally recognizing individual rights and civil liberties in the cyber environment, creating compliance and enforcement mechanisms, and developing legal procedures to combat cybercrimes. It also involves enhancing international cooperation in combating cybercrimes and sharing information and expertise in this field. Ultimately, the goal is to achieve a secure and safe cyber environment for individuals, businesses, and governments by applying appropriate legislation and regulations to protect society from cybercrimes.

7. International Cooperation: Enhancing international cooperation in cybersecurity through participation in international discussions and negotiations, fostering formal and informal cooperation in cyberspace, achieving international consensus on state conduct in this field, and developing mechanisms for information and experience exchange regarding cybercrimes among different countries. This also involves identifying best practices in this field.

Branch Two
The Role of the National Institute of Standards and Technology (NIST) in Cybersecurity

The National Institute of Standards and Technology (NIST) is an American governmental institution operating under the supervision of the U.S. Department of Commerce. Established in 1901, NIST is responsible for developing and enhancing measurements, standards, and technology in the United States. The institute comprises a collection of specialized science and technology laboratories, as well as a research and development center(3).

NIST's Cybersecurity Framework: NIST has developed several frameworks to regulate and improve the approach to cybersecurity at the industrial, corporate, and national levels. One of these frameworks is the Cybersecurity Framework, first issued in 2014, with subsequent enhancements and revisions planned for the coming year. This framework outlines five key elements, each encompassing detailed, structured, and sequential governance procedures, which will be discussed as follows:

(3) https://www.nist.gov/about-nist.

Element One: Identify This element involves identifying and understanding the cybersecurity risks facing an organization and pinpointing the critical and sensitive cyber assets that need protection. The identification process includes several steps that organizations must follow:

1. **Identifying Cyber Assets:** Organizations should identify their vital and sensitive cyber assets, such as sensitive data, private information, critical systems, and network-connected equipment. They should also determine the location, classification, and value of these assets.

2. **Identifying Cyber Risks:** Organizations need to identify and assess the cybersecurity risks they face, evaluating the potential impact of these risks on critical cyber assets and overall organizational operations.

3. **Identifying Legal and Regulatory Requirements:** Organizations must identify and comply with the legal and regulatory requirements related to cybersecurity, such as compliance rules issued by regulatory bodies and government cybersecurity regulations.

4. **Identifying General Cybersecurity Frameworks:** Organizations should identify the general cybersecurity frameworks applied within the organization, such as existing policies, procedures, and security requirements. These frameworks should be periodically evaluated and updated to align with new cybersecurity developments.

5. **Identifying Opportunities and Challenges:** Organizations should identify opportunities and challenges related to cybersecurity, such as opportunities for digital transformation and cybersecurity advancements, as well as new cybersecurity threats, sophisticated cyber-attacks, and resource limitations for implementing cybersecurity measures.

Element Two: Protect This element aims to provide the necessary protection for critical cyber assets by implementing required cybersecurity measures. The protection element includes several steps that organizations must follow, including:

1. **Implementing Security Measures:** Organizations should implement necessary security measures to protect critical cyber assets, such as establishing and enforcing security policies and procedures, applying identity verification and authentication measures, encryption, and other applicable security protocols.

2. **Enhancing Security Awareness:** Organizations should enhance security awareness among employees and staff, providing necessary training and education to increase their understanding of cybersecurity risks and how to address them.

3. Identity and Access Management: Organizations should implement identity and access management procedures to ensure that only authorized users can access critical cyber assets. This involves applying access control policies, identity verification, authorization, and access control, as well as logging and monitoring.

4. Improving Physical Security: Organizations should improve the physical security of critical cyber assets, such as securing devices, equipment, and critical facilities, and implementing necessary security measures to protect them.

5. Improving Supply Chain Cybersecurity: Organizations should enhance supply chain cybersecurity, ensuring that suppliers adhere to applicable cybersecurity standards, identifying potential cyber risks related to the supply chain, and applying necessary security measures to mitigate these risks.

6. Handling Cyber Incidents: Organizations should prepare and implement incident response plans to handle cyber–attacks, including identifying, verifying, responding to, and recovering from such incidents.

These elements outline NIST's comprehensive approach to managing and mitigating cybersecurity risks, emphasizing the importance of structured and proactive measures in safeguarding critical cyber assets and ensuring overall organizational security.

Element Three: Detect

This element aims to enhance the organization's ability to early detect and effectively verify cyber–attacks and unwanted security events. The detection element helps improve the organization's capability to analyze and classify security events and take appropriate measures to address potential cyber threats. It also enhances the efficiency and effectiveness of detection, analysis, and response operations through improved automation(4) and the use of modern technologies, thereby reducing the time required to respond to security incidents and minimizing the resulting damage.

Element Four: Respond

This element aims to enhance the organization's ability to respond to cyber–attacks, rehabilitate affected systems and data, and minimize the damage caused by these attacks. The activities under this element include several steps that organizations must follow, such as:

1. Incident Response: Organizations should develop and implement incident response plans as needed, defining roles, responsibilities, and

(4) Automation is a set of computational, mechanical, and electromechanical elements or processes that operate with minimal or no human intervention. Automation is typically used to enhance the operation of an industrial plant, a company, and other productive sectors that are ready to keep pace with digital transformation.

appropriate procedures for executing these plans, and ensuring the availability of necessary resources.

2. Damage Mitigation: Organizations should take the necessary steps to mitigate the damage caused by cyber–attacks, rehabilitate affected systems and data, assess the damage, and prioritize the restoration of the organization's infrastructure.

3. Digital Forensics: Organizations should conduct digital forensic analysis of cyber events and attacks, collecting, evaluating, and analyzing digital evidence to determine responsibilities, sources, and methods used in the attack, and identifying digital evidence that can be used in criminal investigations.

4. Improving Automation: Organizations should enhance automation in incident response operations by using automation tools, artificial intelligence, machine learning, automated analysis, and other modern technologies to improve the efficiency and effectiveness of response operations and reduce the time required to rehabilitate affected systems.

5. Training and Drills: Organizations should organize training and courses for employees on how to handle cyber–attacks and effectively implement incident response plans, as well as conduct drills to improve the organization's ability to respond to cyber–attacks and rehabilitate affected systems.

Overall, the response element is essential for maintaining and enhancing the cybersecurity of organizations. It helps improve the ability to deal with cyber–attacks, minimize the damage caused by these attacks, and increase organizational awareness of the importance of effective cyber–attack responses and implementing necessary plans.

Element Five: Recover

This element aims to provide the necessary procedures and plans to restore the organization's essential functions after cyber–attacks or other security incidents. Recovery activities include several steps that organizations must follow, such as:

1. Identifying Critical and Sensitive Resources: Organizations should identify vital resources, sensitive data, critical applications, and important systems to prioritize their recovery in the event of cyber–attacks or other security incidents. These are the resources most affected and widely impacted.

2. Backup Procedures: Organizations should implement necessary procedures to back up vital and sensitive data, systems, and applications, store them in secure locations, and regularly update them.

3. Data Recovery: Organizations should implement necessary procedures to recover lost or damaged data after cyber-attacks or other security incidents.

4. System Restoration: Organizations should implement necessary procedures to restore affected systems and rehabilitate them to their normal state after cyber-attacks or other security incidents.

5. Testing Recovery Plans: Organizations should regularly test recovery plans, update them based on test results, and train employees on how to execute and periodically update recovery plans. (Jaafar, El-Kady, and Labib,2023,p115-116)

Branch Three
The Role of the European Union Agency for Cybersecurity (ENISA) in Cybersecurity

The European Union Agency for Cybersecurity (ENISA), established in 2004 and part of the European Union, works to enhance the capacity of EU countries and private sector organizations within the EU to prevent, detect, and respond to cyber threats.

ENISA develops strategic plans and specific action plans for cybersecurity. These plans aim to improve the EU's ability to counter cyber threats and protect critical networks and information. The current strategic plan for cybersecurity includes various initiatives and activities, such as enhancing cooperation among member states, promoting cybersecurity awareness and training, developing European cybersecurity standards, and providing technical advice in this field.

ENISA aims to achieve several strategic objectives in the field of cybersecurity, which can be summarized as follows:

1. Enhancing security awareness and fostering a security culture in institutions, organizations, and communities.
2. Supporting the development and improvement of cybersecurity capabilities in Europe.
3. Strengthening cooperation and coordination among European countries, institutions, and organizations in the field of cybersecurity.
4. Providing support and assistance to institutions and organizations in countering cyber threats and security incidents.
5. Developing the necessary security standards, practices, and tools to achieve cybersecurity in Europe.

6. Enhancing the ability to deal with new and emerging cyber threats.
7. Assessing and improving cybersecurity in critical sectors, government services, digital services, and digital markets.
8. Providing cybersecurity support and assistance to citizens and users.
9. Promoting research and development in cybersecurity and applying modern technologies to achieve cybersecurity.
10. Working to enhance transparency and accountability in cybersecurity by providing comprehensive information, guidelines, advice, and security analyses to institutions, organizations, and communities.

Requirement Three:
The Role of Regional Agreements in Combating Cybercrime

In addition to the international efforts undertaken by the aforementioned international organizations, other international efforts are made by regional organizations. These efforts are no less significant than those made by multilateral international organizations (which include countries from more than one geographical region).

The role of regional organizations in combating cybercrime has become evident through the agreements they have produced in this field. For instance, the Council of Europe convened in Budapest, Hungary, on November 23, 2001, to discuss this emerging criminal phenomenon and agree on clear provisions to combat information technology crimes. The European Convention on Cybercrime (also known as the Budapest Convention) was adopted, becoming the global legal foundation for combating cybercrime. Similarly, the League of Arab States made efforts in this regard by issuing the Arab Convention on Combating Information Technology Offenses in 2010.

In the following paragraphs, we will discuss the Budapest Convention on Cybercrime and the Arab Convention on Combating Information Technology Offenses.

Branch One
The Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime was adopted after more than five years of work and meetings by the European Committee on Crime Problems. This convention, finalized on November 23, 2001, in Budapest, reflects the Council of Europe's commitment to combating the illicit use of computers and information networks. The convention resulted from extensive consultations between governments, law enforcement agencies, and the computer sector, with half of its drafting done by experts from the Council of Europe with assistance from several countries, including the United States. The convention has been a cornerstone since it came into force on July 1, 2004, for the member states of the Council of Europe. (Sulieman & Abdelhalim, p 34)

The convention pioneered the establishment of a list of crimes that ratifying countries must criminalize in their domestic laws. It was the first treaty to address internet crimes comprehensively, including terrorism, credit card fraud, child prostitution, and more. The convention aims to harmonize new laws in many countries.

Given its importance, thirty European countries, including four non-member states of the Council of Europe, signed the convention. Additionally, several non-European countries, such as Canada, Japan, South Africa, and the United States, joined. The convention comprises four chapters: Chapter One on terminology, Chapter Two on national measures, Chapter Three on jurisdiction and international cooperation, and Chapter Four on final provisions. (Ahmed, 2011,p 12) Below is a brief overview of each chapter.

Sub-branch One: Terminology and Definitions

Article One of the convention provides basic definitions for terms such as "information system," "service provider," "computer data," and "traffic data," as follows:

- **Information System:** Refers to any device or group of interconnected devices, which, alone or in combination with other elements, performs automatic data processing by executing a specific program.

- **Computer Data:** Means any representation of facts, information, or concepts in any form that is suitable for automated processing, including a program capable of performing a function by a computer.

- **Service Provider:** Refers to:

1. Any public or private entity that provides its users with the ability to communicate via an information system.

2. Any other entity that processes or stores computer data on behalf of a communication service or its users.

- **Traffic Data:** Refers to any data related to a communication that is generated by an information system, indicating the origin, destination, route, time, date, size, duration, or type of underlying service.

Sub-branch Two: Measures to Be Taken at the National Level

The convention addresses in its second chapter the measures that must be taken at the national level, and these measures are divided into two sections. The first section deals with substantive criminal law, while the second section addresses procedural law. In this part of the current study, we will focus only on the first section, which pertains to the substantive aspects of cybercrimes as outlined in Articles (2-13) of the convention.

First: Crimes Against the Confidentiality, Integrity, and Availability of Data and Information Systems:

These crimes include five specific offenses, which are highlighted below:

1. **Unauthorized Access Offense:** Article 2 of the convention stipulates that each party must adopt legislative or other measures deemed necessary to establish as a criminal offense, under its domestic law, the intentional access to the whole or any part of a computer system without right. Additionally, a party may require that the offense be committed by infringing security measures, with the intent to obtain computer data or any other criminal intent, or that the offense be committed on a computer system that is remotely connected to another computer system. Consequently, unauthorized interference or hacking, understood as unauthorized access to an information system, must be considered illegal in itself as a general principle.

2. **Unauthorized Interception Offense:** Article 3 of the convention requires each party to adopt legislative or other measures deemed necessary to establish as a criminal offense, under its domestic law, the intentional and unauthorized interception, by technical means, of non-public transmissions of computer data to, from, or within a computer system, including electromagnetic emissions from a computer system carrying such data. A party may also require that the offense be committed with criminal intent or fraudulent intent, or that the offense be committed on a computer system that is remotely connected to another computer system.

3. **Data Interference Offense:** Article 4 of the convention criminalizes data interference if it is committed intentionally, without right, and results in damage, deletion, deterioration, alteration, or suppression of computer data. A party may also reserve the right to require that the conduct described in the first paragraph result in significant harm. The explanatory memorandum indicates that the purpose of this provision is to ensure that computer data and programs are afforded similar protection against intentional harm as is given to tangible objects and to ensure the proper operation of data integrity or the proper use of stored computer data.

4. **System Interference Offense:** Article 5 of the convention criminalizes serious hindrance, if done intentionally and without right, to the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering, or suppressing computer data. The explanatory memorandum clarifies that Recommendation No. (89) referred to this offense under the term "computer system sabotage," and the provision aims to criminalize intentional interference with the legitimate use of information systems, including communication

systems, by using or affecting computer data. The protected legal interests are the interests of the operators and users of the computer or communication system in the proper functioning of these systems, and the provision is drafted in a neutral manner to protect all types of functions. The term "hindrance" relates to actions that impair the proper functioning of a computer system, and this hindrance must result from the input, transmission, deterioration, alteration, deletion, or suppression of computer data.

5. **Misuse of Devices Offense:** Article 6 of the convention states:

- Each party must adopt legislative or other measures deemed necessary to criminalize, under its domestic law, if the act is committed intentionally and without right:

- The production, sale, procurement for use, importation, distribution, or otherwise making available of:

▪ A device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses established in Articles 2–5 mentioned above.

▪ A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent that it be used for the purpose of committing any of the offenses mentioned in Articles 2–5.

▪ The possession of any of the items referred to in points 1–(1), 1–(2) of Article 6 of the Budapest Convention(5), with the intent to use them to commit any of the offenses referred to in Articles 2–5.

- A party may require, under its domestic law, the presence of certain elements to establish criminal liability.

- This article should not be interpreted as imposing criminal liability when the production, sale, procurement for use, importation, distribution, or making available referred to in the first paragraph of this article is not intended to commit an

(5) Article 6 of the Budapest Convention states the following:

Misuse of Devices: Each State Party shall adopt such legislative and other measures as may be necessary to criminalize the following acts under its national law, if committed intentionally and without right:

a. The production, sale, procurement for use, importation, distribution, or otherwise making available of:

A device, including a computer program, that has been designed or adapted primarily for the purpose of committing any of the offenses established in Articles 2 through 5.

A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with the intent to commit any of the offenses established in Articles 2 through 5.

offense, according to Articles 2–5 of this convention, such as in the case of authorized testing or protection of a computer system.

- Each party may reserve the right to apply the first paragraph of this article provided that this reservation does not include the sale, distribution, or making available of any of the items referred to in points 1-(1), 1-(2). The commission of these offenses often requires possession of access tools, such as hacking tools or other similar tools, which are strongly incentivized for criminal purposes, potentially leading to the creation of a black market for the production and distribution of such tools.

Secondly: Computer-Related Crimes:
This category includes two crimes, which we will highlight below:

Computer-Related Forgery: Article 7 of the convention criminalizes the intentional and unauthorized input, deletion, alteration, or suppression of computer data, resulting in inauthentic data, with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless of whether or not the data is readable and intelligible. Any party may require that the offense be committed with fraudulent or similar criminal intent to establish criminal liability under its domestic law. The explanatory memorandum specifies that the purpose of this article is to create an offense equivalent to traditional document forgery. It aims to fill gaps in criminal law related to traditional forgery, which requires the visible readability of the declarations contained in the document, a requirement that does not apply to data stored on electronic media.

Computer-Related Fraud: Article 8 of the convention criminalizes causing a loss of property to another person by: A – Inputting, altering, deleting, or suppressing computer data. B – Any interference with the functioning of a computer system with fraudulent or similar criminal intent to procure an economic benefit for oneself or another without right. The explanatory memorandum indicates that with the technological revolution, the possibilities for committing economic crimes, particularly credit card fraud, have multiplied. Assets represented or transmitted through computer systems, such as electronic funds or deposits, have become targets for manipulation in ways similar to traditional property crimes. These offenses primarily involve manipulating system inputs by feeding the computer with false data, manipulating programs, or other interventions in data processing. The purpose of this article is to establish criminal penalties for any unlawful manipulation in the context of automated data processing that results in the illegal transfer of property.

Thirdly: Content-Related Offenses:

This chapter covers offenses related to content, specifically the unlawful production or distribution of child pornography through computer systems, representing one of the most serious forms of cybercrime, which has recently emerged. It is noteworthy that while drafting the convention, the committee discussed the possibility of including other content-related offenses, such as the dissemination of racist propaganda through computer systems. However, the committee could not reach a consensus on criminalizing such behavior. Despite broad support for criminalizing such dissemination, some delegations raised significant reservations, citing the principle of freedom of expression. Given the complexity of the issue, the committee decided to instruct the European Committee on Crime Problems to propose the preparation of an additional protocol to the current convention. Below are the provisions of Article 9 concerning offenses related to child pornography, which state that each party shall adopt legislative or other measures necessary to criminalize the following intentional and unauthorized conduct under its domestic law: A- The production of child pornography for the purpose of its distribution through a computer system. B- Offering or making available child pornography through a computer system. C- Distributing or transmitting child pornography through a computer system. D- Procuring or obtaining child pornography through a computer system for oneself or another person. E- Possessing child pornography in a computer system or on a computer-data storage medium.

For the purposes of paragraph 1 above, child pornography includes any pornographic material that visually depicts: A- A minor engaged in sexually explicit conduct. B- A person appearing to be a minor engaged in sexually explicit conduct. C- Realistic images representing a minor engaged in sexually explicit conduct.

For the purposes of paragraph 2 above, a "minor" is any person under the age of 18 years. However, any party may require a lower age limit, which shall be no less than 16 years.

Any party may reserve the right not to apply, in whole or in part, paragraphs 1(d) and 1(e) and paragraphs 2(b) and (c).

Fourthly: Offenses Related to Infringements of Intellectual Property and Related Rights:

The fourth chapter defines offenses related to the infringement of intellectual property and related rights. The convention includes such offenses because intellectual property violations are among the most common forms of cybercrime, and their increasing prevalence is a growing concern globally. Below are the provisions of Article 10 related to offenses involving intellectual property and related rights. Article 10 states that each party shall adopt legislative or other measures necessary to criminalize, under its domestic law, the infringement of intellectual property rights as defined by that party's law, in accordance with the

obligations set forth under the World Intellectual Property Organization (WIPO) Copyright Treaty signed in Paris on July 24, 1971, the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS), and the WIPO Performances and Phonograms Treaty, excluding any moral rights granted by these treaties, if such acts are committed intentionally, on a commercial scale, and through a computer system. (Explanatory Report to the Convention on Cybercrime Budapest,.2001)

Fifthly: Liability of Legal Persons

Article 12 of the convention states:

1. Each party shall adopt legislative or other measures necessary to ensure that legal persons can be held liable for criminal offenses established in this convention, if such offenses are committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within, based on: A- A power of representation of the legal person. B- An authority to take decisions on behalf of the legal person. C- An authority to exercise control within the legal person.

2. In addition to the cases already provided for in paragraph 1, each party shall take the necessary measures to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offense established in this convention for the benefit of that legal person by a natural person acting under its authority.

3. Depending on the legal principles of the party, the liability of legal persons may be criminal, civil, or administrative.

4. Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offense.

The convention establishes the criminal liability of legal persons, aligning with the current legal trend recognizing the liability of legal entities. Four conditions must be met to establish the liability of a legal person: the offense committed must be one of the offenses mentioned in the convention; the offense must have been committed for the benefit of the legal person; the person who committed the offense must have a leading position, including partners, with the term "leading position" referring to a natural person holding a high position in the institution such as a director; and the person in the leading position must be acting within their authority, such as decision-making or exercising control, indicating that the natural person acted within their powers, making the legal person liable.

Sub-branch Three: Provisions Related to Transnational Cybercrimes

Firstly: International Cooperation:

Article 23 of the convention sets out the general provisions related to international cooperation, stating that parties shall cooperate with each other to the widest extent possible in the application of international cooperation principles in criminal matters, international agreements based on uniform or reciprocal legislation, and national laws for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. (The Explanatory Report ,p44-46)The explanatory memorandum of this convention indicates that this article establishes three general principles governing international cooperation: The first principle: Parties must cooperate with each other to the widest extent possible. This principle imposes an obligation on parties to assist each other broadly, minimizing obstacles that could impede the rapid flow of information and evidence internationally. The second principle: The scope of cooperation must cover all criminal offenses related to computer systems and data, as referred to in Article 14, paragraph 2, subparagraphs (a) and (b) of the convention. The third principle: This cooperation must be implemented according to the provisions of this chapter and the application of international cooperation principles in criminal matters, international agreements based on uniform or reciprocal legislation, and national laws. This final point concerning national law establishes a general principle that the provisions of Chapter 3 do not invalidate the provisions of international documents concerning judicial assistance and reciprocal agreements on the extradition of criminals between parties for those documents, detailed further in the analysis of Article 27, or the provisions of national law concerning international cooperation. This principle is clearly supported in Articles 24 on the extradition of criminals, 25 on general principles of mutual assistance, 26 on spontaneous information, 27 on procedures for mutual assistance requests in the absence of applicable international agreements, 28 on confidentiality and limitation on use, 31 on mutual assistance regarding access to stored computer data, 33 on mutual assistance regarding real-time collection of traffic data, and 34 on mutual assistance regarding the interception of content data.

Secondly: Extradition of Offenders

Article 24 of the convention states:

1. a. This article applies to the extradition of offenders between parties for the criminal offenses defined under Articles 2-11 of this convention, provided that these offenses are punishable under the laws of both parties by a deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. b. If a different minimum penalty applies under an extradition agreement in force between two or more parties, including the European Convention on Extradition or any agreement based on uniform or

reciprocal legislation, the penalty specified in this convention shall apply.

2. The criminal offenses described in paragraph 1 of this article shall be deemed extraditable offenses in any extradition treaty existing between or among the parties. The parties undertake to include such offenses as extraditable offenses in every extradition treaty to be concluded between them or to be made applicable to them.

3. If a party makes extradition conditional on the existence of a treaty and receives a request for extradition from another party with which it has no extradition treaty, it may consider this convention as the legal basis for extradition in respect of any criminal offense referred to in paragraph 1 of this article.

4. Parties that do not make extradition conditional on the existence of a treaty shall recognize the offenses referred to in paragraph 1 of this article as extraditable offenses between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested party or by applicable extradition treaties, including the grounds on which the requested party may refuse extradition.

6. If extradition is refused solely on the basis of the nationality of the person sought, or because the requested party deems itself competent to prosecute the offense, the requested party shall submit the case at the request of the requesting party to its competent authorities for the purpose of prosecution, and these authorities shall make their decision in the same manner as in the case of any other offense of a similar nature under the laws of that party. The authorities shall promptly inform the requesting party of the final outcome of the case.

7. Each party shall designate at the time of signature, ratification, acceptance, approval, or accession to this convention, an authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

8. The Secretary General of the Council of Europe shall establish and keep updated a register of the designated authorities communicated by the parties. Each party shall ensure that the details included in this register are correct at all times.

It is observed from paragraph 1 of Article 24 that the obligation to extradite offenders only applies to offenses defined under Articles 2–11 of the convention, which are punishable under the laws of both parties by a deprivation of liberty for a maximum period of at least one year or by a more severe penalty.

Thirdly: Mutual Legal Assistance

Here we will discuss two articles of the convention, namely Article 25 on general principles governing mutual legal assistance and Article 26 on spontaneous information.

Article 25 of the convention states:

1. The parties shall afford each other mutual legal assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense.

2. Each party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3. Where, in the case of urgency, a party makes a request for mutual assistance or communications by expedited means of communication, such as fax or email, which offer the conditions to provide sufficient security and authentication (including encryption where necessary), the requested party shall accept and respond to the request via the same means, subject to subsequent formal confirmation where required by the requested party.

4. Except as otherwise provided in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested party or by applicable mutual assistance treaties, including the grounds on which the requested party may refuse cooperation. The requested party shall not exercise its right to refuse mutual legal assistance in respect of offenses referred to in Articles 2–11 of the convention solely on the grounds that the request concerns a fiscal offense.

5. Where, in accordance with the provisions of this chapter, the requested party is permitted to make mutual assistance conditional on the existence of dual criminality, that condition shall be deemed fulfilled if the conduct constituting the offense for which assistance is sought is a criminal offense under the laws of both parties, whether or not the laws of the requested party place the offense within the same category of offense or denominate the offense by the same terminology as the requesting party.

The obligation to provide assistance should be met to the widest extent possible, thus mutual legal assistance should, in principle, be comprehensive and extended, minimizing obstacles to the greatest extent possible. The obligation to cooperate, as stipulated in Article 23, applies as a general principle to all

criminal offenses related to computer systems and data and the collection of electronic evidence related to a criminal offense. This broad scope of the obligation to cooperate justifies the necessity of international cooperation mechanisms in these areas. However, Articles 34 and 35 allow parties to adjust the scope of these measures.

Fourthly: Establishing a Permanent Emergency Network for Activating Mutual Assistance

Here, we will discuss a single article from the convention, Article 35, regarding the establishment of a permanent emergency network to activate mutual assistance, known as the 24/7 network. This network operates 24 hours a day, 7 days a week, to ensure the provision of immediate assistance for investigations related to criminal offenses involving computer systems and data, or for collecting electronic evidence of a criminal offense. This assistance must include facilitating or directly implementing the following procedures: (The Explanatory Report, p185)

- Providing technical advice.
- Preserving data in accordance with Articles 29 and 30.
- Collecting evidence and providing legal information, and identifying the location of suspects.

Furthermore, the article specifies the following requirements:

1. Each party's point of contact must have the ability to communicate rapidly with a point of contact from another party.

2. If the designated point of contact by a party does not belong to the authority or authorities responsible for international assistance or extradition, it must be able to cooperate promptly with such authority or authorities.

3. Each party must have a trained staff equipped with tools that facilitate the operation of the network.

The establishment of this network is one of the most critical measures stipulated in this convention, as it ensures not only the most successful means of addressing cybercrime problems but also overcoming the significant challenges posed by the information age to law enforcement authorities. The point of contact aims to either facilitate the rapid exercise of network functions or directly implement several measures, including providing technical guidance, preserving data, collecting evidence, and locating suspects.

Branch Two: The Arab Convention on Combating Information Technology Offenses

The Arab Convention on Combating Information Technology Offenses was signed in Cairo on December 21, 2010. Egypt agreed to join it by Presidential Decree No. 276 of 2014, dated August 19, 2014, and published in the Official Gazette, Issue 46, on November 13, 2014, with reservations subject to ratification. This convention aims to enhance cooperation among Arab countries in combating information technology crimes to mitigate the dangers of these crimes, safeguarding the security, interests, and well-being of Arab countries, their societies, and individuals. The convention obliges each member state to criminalize the acts outlined in the second chapter of the convention, titled Criminalization. (Abdel Azim,2016, p166)

This convention is one of the most important Arab agreements in the field of combating cybercrime, aiming to prevent, investigate, and prosecute such crimes, (Batikh, p22) including attacks on data integrity, misuse of information technology tools, forgery, fraud, pornography, invasion of privacy, and terrorism-related crimes committed using information technology, such as spreading terrorist group ideologies, promoting terrorist operations, disseminating methods for making explosives, and organized crime activities like money laundering, drug trafficking, human trafficking, and trafficking in human organs and weapons. (Abdel Sadeq, 2018, p5)

The Arab Convention consists of forty-three articles obliging member states to amend their laws to criminalize information technology offenses, such as hacking, illegal interception, data integrity breaches, privacy violations, intellectual property infringements, misuse of information technology, forgery, fraud, terrorism-related crimes, money laundering, drug trafficking, human trafficking, and weapons trafficking. The third and fourth chapters of the convention clarify the scope of procedural provisions and legal and judicial cooperation related to extradition, mutual assistance between countries, and assistance related to investigative authorities. It also emphasizes that each member state must adopt internal legislation and procedures to combat cybercrime.

The convention has had a legislative impact on the Arab world, with many Arab countries keeping pace with technological advancements in information technology and striving to combat emerging cybercrimes by issuing specific legislation based on and building upon the provisions of the convention. Top of Form

Part Two
Egyptian Efforts in Cybersecurity

Egypt has witnessed a significant movement in the field of information and network security, coinciding with the increasing international attention to information security, especially in light of the security breaches experienced by some countries in the region affecting their infrastructure, networks, and information due to rapid technological advancements.

Egypt has sought to build and establish a modern system capable of protecting its cyberspace (Hekayat Watan: 2023, pp. 275, 276, 277). The Supreme Council for Cybersecurity was established, along with the Egyptian Computer Emergency Response Team (CERT). Additionally, the Financial Sector Computer Emergency Response Team under the Central Bank was created. Furthermore, the National Cybersecurity Strategy 2017-2021 was issued, followed by the National Cybersecurity Strategy 2023-2027, which will be discussed in the upcoming sections.

We will cover Egypt's efforts in the field of cybersecurity in five sections as follows:

1. **Requirement One:** The Supreme Council for Cybersecurity
2. **Requirement Two:** The Egyptian Computer Emergency Response Team (CERT)
3. **Requirement Three:** The Financial Sector Computer Emergency Response Team under the Central Bank
4. **Requirement Four:** The National Cybersecurity Strategy of the Arab Republic of Egypt 2017-2021
5. **Requirement Five:** The National Cybersecurity Strategy of the Arab Republic of Egypt 2023-2027
6. **Requirement Six:** Results of Egypt's efforts in the field of cybersecurity

Requirement One
The Supreme Cybersecurity Council

The Supreme Cybersecurity Council in Egypt was established by a decree from the former Prime Minister, Eng. Ibrahim Mahlab, No. 2259 in December 2014. The council aims to protect information and data within various entities, focusing on the information and communications departments in ministries and other bodies, ensuring the necessary funding to implement the cybersecurity system, and clarifying the relevant legislative framework(6).

The council is chaired by the Minister of Communications and Information Technology and includes representatives from the Ministries of Defense, Foreign Affairs, Interior, Petroleum and Mineral Resources, Electricity, Health, Water Resources and Irrigation, Supply, Communications, the General Intelligence Service, the Central Bank, and three experts. Prime Minister's Decree No. 1630 of 2016 defined the council's

(6) www.escc.gov.eg

functions, duties, and meeting schedules. Additionally, Prime Minister's Decree No. 994 of 2017 tasked the Minister of Communications with setting and overseeing the implementation of security rules and following up on the council's decisions.

The Supreme Cybersecurity Council is responsible for developing a national strategy to address cyber threats and attacks, overseeing its implementation and updates, and the following tasks:

- Approving the identification of critical telecommunications and information infrastructure across all state sectors and establishing frameworks for their security evaluation and monitoring.
- Approving frameworks, strategies, and policies for securing critical telecommunications and information infrastructure in all state sectors.
- Developing plans and programs to advance the cybersecurity industry, preparing the necessary workforce to face cyber challenges and threats, and establishing a framework for scientific research and development in cybersecurity.
- Cooperating and coordinating regionally and internationally with relevant entities in cybersecurity and securing critical telecommunications and information infrastructure, and recommending necessary legislative interventions for security.
- Setting mandatory standards for all entities as a minimum requirement to secure critical telecommunications and information infrastructure and mandating the preparation of emergency plans.
- Establishing mechanisms to monitor risks and periodically follow up on cyber-attacks, and distributing roles at the national level.
- Establishing and activating standards and mechanisms to identify dependencies among elements of critical infrastructure and those responsible for them, to avoid cascading effects.
- Approving cybersecurity standard specifications for systems in various sectors and incorporating cybersecurity quality standards.
- Approving security evaluations for those operating critical telecommunications and information infrastructure.
- Establishing a mechanism to monitor and protect official government websites on the internet.

By establishing these frameworks and councils, Egypt aims to create a robust cybersecurity environment that not only addresses current threats but also prepares for future challenges in the ever-evolving landscape of information technology.

Requirement Two
The Egyptian Computer Emergency Readiness Team (EG-CERT)

The Ministry of Communications and Information Technology has adopted the initiative to form a Supreme Council for the Protection of Critical Telecommunications and Information Technology Infrastructure. The team comprises sixteen specialists providing 24-hour technical support to protect critical information infrastructure. Since 2012, EG-CERT has been supporting various entities across the information and communications technology sectors, banking services, and government services to help them combat cybersecurity threats, including denial-of-service attacks.

The mission of EG-CERT revolves around providing an early warning system against malware and widespread cyber-attacks targeting Egypt's critical information infrastructure. Currently, EG-CERT is expanding its development of laboratories in the four main operational departments, with plans for additional cybersecurity laboratories in mobile security and industrial control systems.

The center's objectives also include establishing an appropriate legislative framework for cybersecurity, creating a suitable regulatory framework for establishing a national cybersecurity system and emergency response centers, and building the necessary infrastructure to ensure trust in electronic transactions and protect digital identity, such as public key infrastructure and credit bureaus with private sector participation. Additionally, the center aims to collect and analyze security incident information, and coordinate and mediate among all parties to resolve such incidents.

EG-CERT consists of five departments: Cyber Incident Handling and Business Continuity, Cyber Attack Monitoring and Early Warning, Vulnerability Assessment and Penetration Testing, Critical Information Infrastructure Protection and Emergency Plans, and Cybersecurity Awareness and Business Development.

The Critical Information Infrastructure Protection and Emergency Plans department focuses on protecting information in critical sectors of the state by studying the needs of specific sectors and assessing the implementation levels of cybersecurity standards and procedures.

The Cybersecurity Awareness department is dedicated to building and enhancing the culture and awareness of cybersecurity and information security, recognizing the risks of the internet, and understanding cyber threats and attacks. This department targets ministries and government institutions with critical infrastructure, conducting awareness campaigns through training courses, workshops, periodic bulletins, guides, awareness videos, and participation in school and university events(7).

(7) https://egcert.eg/ar/.

Requirement Three
Financial Sector Computer Emergency Response Team (FS-CERT)

The Financial Sector Computer Emergency Response Team specializes in handling cyber incidents and internet emergencies within the financial and banking sector by predicting and addressing security incidents, mitigating their effects, and preventing recurrence. This is achieved through a non-traditional technical system for security monitoring and analysis of digital evidence and security vulnerabilities associated with cybercrimes in the financial sector to understand their causes and prevent future occurrences. The center also handles malware and conducts reverse engineering.

The mission and strategy of FS-CERT are summarized as follows:

- Securing IT and communications emergency response to support government agencies, critical national infrastructure, and the general public through legally recognized, reliable, licensed, and centrally coordinated initiatives at the national level.

- Promoting security and protection by disseminating important information such as early warnings, alerts, security advisories, and supporting best security practices.

- Supporting and maintaining these initiatives by adopting advanced technologies and techniques, establishing methodologies, and researching threat analysis and mitigation.

The strategy of the National Computer Emergency Response Center prioritizes the protection of national IT and communications by:

- Adopting all necessary initiatives for the National Computer Emergency Response Center.

- Securing sensitive information through regional cooperation with international multilateral partnerships against cyber threats, regional CERTs, and international cooperation.

- Gathering threat intelligence with international and global sources through its own technological facilities.

- Coordinating with the International Union, authorized CERTs in other countries, and other entities concerned with IT and communications security.

FS-CERT at the Central Bank of Egypt successfully obtained accreditation and membership in the Forum of Incident Response and Security Teams (FIRST), after meeting all technical and organizational requirements within a short

timeframe, becoming the first sector-specific center of its kind internationally recognized in Egypt. This accomplishment aligns with the Central Bank's strategy to build an integrated framework for enhancing cybersecurity in the financial and banking sector, and crowns the efforts of FS-CERT over the past four years in adhering to and complying with international security standards and specifications.

Membership in FIRST, which aims to enhance cooperation and coordination in preventing and mitigating cyber incidents, enables rapid response and effective incident handling. It also helps maximize and develop the technical and technical capabilities of CERTs by providing access to the latest global practices in the field, real-time sharing of security information on cyber incidents, and promoting rapid response and proactive measures.

The forum also facilitates strategic cooperation and partnerships between countries and global institutions, enhances communication between incident response teams worldwide through the exchange of technological and security intelligence expertise, and allows members to attend specialized seminars featuring cybersecurity experts, as well as practical training sessions and lectures. Members can also participate in the annual global conference on cybersecurity incident response, access the latest cybersecurity methodologies and publications, and engage in online forums and discussions among members.

All these efforts align with the Central Bank of Egypt's strategy to enhance FS-CERT's participation in effectively implementing the national cybersecurity strategy, alongside improving the capacity of state institutions and entities to respond swiftly and coordinate efforts to prevent cyber incidents.

Requirement Four
The National Cybersecurity Strategy of the Arab Republic of Egypt 2017-2021

Egypt has been an early adopter of cybersecurity measures and has sought to lead the Arab and African regions in international indices. It has been at the forefront of efforts to continuously improve and create a pioneering experience in the Middle East.

In light of national cybersecurity governance, Egypt issued the National Cybersecurity Strategy 2017-2021 in alignment with modern global trends and in accordance with the Egyptian Constitution of 2014. Article 31 of the constitution stipulates that cybersecurity is an integral part of the national economy and security system, and the state is obligated to take necessary measures to protect it as regulated by law.

Pillars of the National Cybersecurity Strategy

Strategy Objective The objective of Egypt's National Cybersecurity Strategy is to address cyber risks and enhance trust in the telecommunications and information infrastructure and its applications and services across various vital sectors. The aim is to secure these sectors to create a safe and reliable digital environment for the diverse Egyptian community. The primary focus is on identifying and addressing risks, enhancing trust and security in vital sectors and their interactions, and establishing a secure and reliable digital environment.

1. Targeted Vital Sectors The strategy identifies several critical sectors that require protection, efficiency enhancement, and readiness improvement:

- **Telecommunications and Information Technology Sectors:** Including wired and wireless communication networks, submarine and terrestrial cables, communication towers, communication satellites, and internet and telecommunication service providers.

- **Financial Services Sector:** Including banking networks and websites, electronic transactions, stock exchanges, securities trading companies, and postal financial services networks.

- **Energy Sector:** Including systems, networks, and control stations for the production and distribution of electricity, petroleum, and gas, the High Dam stations, nuclear power stations, and more.

- **Transportation Sector:** Including land, sea, air, and river transport, covering all control systems, centers, and networks for trains and metro, traffic networks, and navigation control systems for air and sea.

- **Health Sector:** Including emergency and ambulance services, relief and ambulance networks, blood banks, hospital systems and networks, and health care service networks and websites.

- **Government Services Sector:** Including the government electronic portal, government institution websites, national databases and information, especially the national ID database and connected networks and websites.

2. Risk Mitigation Mechanisms

- **Strategic and Executive Political and Institutional Support:** This includes awareness of the severity of cyber threats and the necessity to treat them as a priority with the utmost seriousness, along with proactive preparedness, strategic and executive plans, emergency plans, horizontal coordination mechanisms, and the preparation of technical and logistical personnel and equipment.

- **Legislative Framework:** Establishing an appropriate legislative framework for cybersecurity, combating cybercrime, protecting privacy, digital identity security, and information security, with participation from relevant stakeholders, private sector experts, and civil society organizations, guided by international experiences and programs. This includes training specialists in law enforcement within judicial and police authorities.

- **Regulatory Framework:** Creating a regulatory framework for cybersecurity protection, establishing a national system to secure telecommunications and information technology infrastructure, national databases and information systems, and government services portals and websites.

- **Establishing and Activating Computer and Network Emergency Response Teams:** These teams, in vital sectors at the national level, are responsible for the security monitoring of national telecommunications and information networks and connected computers, dealing with any cyber threats or attacks, and raising awareness and preparedness for these risks.

- **Encouraging and Supporting Scientific Research and Development:** Promoting collaboration between research entities and national companies in areas such as advanced malware analysis, digital evidence analysis, securing and protecting industrial control systems, developing security devices and systems, encryption and electronic signatures, protecting telecommunications and IT infrastructure, cloud computing security, large databases, artificial intelligence technologies, and the Internet of Things.

- **Human Resource Development:** Enhancing the necessary expertise and skills for activating the cybersecurity system across various sectors, in cooperation and partnership with the private sector, universities, and civil society organizations.

- **International Cooperation:** Collaborating with friendly countries and relevant international and regional organizations, exchanging experiences, and coordinating positions on cybersecurity and combating cybercrime, as these crimes are not confined by geographical or political boundaries.

- **Community Awareness Campaigns:** Implementing awareness campaigns to highlight the importance of cybersecurity and protecting electronic services for individuals and institutions from potential risks and challenges, protecting privacy, and launching programs for child and youth protection on the internet.

Key Programs of the Strategy for the 2017-2021 Period

1. Program for Developing a Suitable Legislative Framework for Cybersecurity: This program focuses on combating cybercrimes, protecting privacy and digital identity, with participation from relevant stakeholders and experts in the governmental, private, academic sectors, and civil society organizations. Laws such as the Cybercrimes Law No. 175 of 2008 and the Personal Data Protection Law No. 151 of 2020 have been issued, with the legislative framework still in progress.

2. Program for Developing an Integrated National Cybersecurity System: This involves securing the telecommunications and IT infrastructure by establishing and activating emergency response teams in critical sectors at the national level.

3. Program for Protecting Digital Identity: This program aims to activate digital citizenship and the necessary infrastructure to support trust in electronic transactions generally and specifically in e-government services, including the implementation of electronic signatures.

4. Community Awareness Program: This program focuses on raising awareness about the opportunities and benefits provided by electronic services to individuals, institutions, and government entities, and the importance of cybersecurity in protecting these services from risks and challenges. It includes nationwide annual celebrations, campaigns, conferences, seminars, and specialized workshops across various sectors.

5. Program to Support Scientific Research and Develop the Cybersecurity Industry: This involves supporting cooperation projects between research entities and national companies, particularly in areas such as advanced malware analysis, digital evidence analysis, industrial control systems security, developing security systems and network devices, encryption and electronic signatures, telecommunications and

IT infrastructure security, cloud computing and large database security, artificial intelligence technologies, and the Internet of Things.

6. **Human Resources Development Program:** This program aims to prepare the necessary expertise and skills to activate the cybersecurity system across different sectors in cooperation and partnership with the government, private sector, and universities. (Ali, 2020,p168)

Requirement Five
The National Cybersecurity Strategy of the Arab Republic of Egypt 2023-2027

In the first week of February 2024, the Supreme Cybersecurity Council announced the launch of the National Cybersecurity Strategy for the 2023–2027 period. This strategy aims to provide a secure environment for various sectors and unify the national vision to achieve a secure Egyptian cyberspace capable of withstanding cyber threats and attacks, and fostering economic growth and prosperity.

This strategy serves as a comprehensive roadmap that includes national projects aimed at establishing frameworks and controls to address increasing cyber incidents and threats. It also aims to create opportunities in the Egyptian market by building qualified human resources and establishing an effective and impactful national industry that contributes to the country's GDP. Finally, it aims to build a culture of cybersecurity awareness across all segments of society to reduce the risks of cybercrimes.

The strategy includes six main areas:

1. Building an integrated legislative framework.
2. Changing societal culture around cybersecurity.
3. Enhancing national partnerships.
4. Building robust and resilient cyber defenses.
5. Encouraging scientific research, enhancing innovation and growth.
6. Enhancing international cooperation.

The strategy is divided into nine parts, summarized as follows:

First: Cybersecurity in Egypt: This part provides an introduction to the strategy, explaining its importance, strengths, weaknesses, opportunities, and threats (SWOT) analysis, and identifying the sources used to prepare the strategy, including experts, academics, and global best practices from leading countries in cybersecurity.

Second: Foundations and Pillars of the Strategy: This section outlines the vision, mission, and constitutional legislative basis for the strategy, along with its programs and pillars, which include building an integrated legislative framework, changing societal culture around cybersecurity, enhancing national

partnerships, building resilient cyber defenses, encouraging scientific research and innovation, and enhancing international cooperation.

Third: Building an Integrated Legislative Framework: This part reviews the current legislative structure. The legislator aims to address two main axes: criminalizing acts and perpetrators through the Cybercrimes Law No. 175 of 2018, and imposing standards and controls through the Personal Data Protection Law No. 151 of 2020 and its executive regulations. The forthcoming Cybersecurity Law is expected to complete this legislative framework.

Fourth: Enhancing National Partnerships: This section discusses the governance efforts of Egypt's cybersecurity system by coordinating cooperation between government entities, private cybersecurity companies, and educational institutions. It also includes the creation of a central database for the cybersecurity market to facilitate information and experience exchange, supporting decision-making processes among various parties. Additionally, it organizes bilateral cooperation agreements with owners and operators of critical infrastructure units to ensure the highest levels of cybersecurity for critical information infrastructure. Finally, this section outlines the establishment of a Cybersecurity Industry Development Fund to ensure continuous funding for cybersecurity projects.

Fifth: Building Strong and Resilient Cyber Defenses

This section outlines five types of programs targeting different sectors. These include programs aimed at integrating with national projects, those focused on critical infrastructure, programs targeting private sector units and institutions, programs aimed at establishing security standards and policies, and finally, programs aimed at improving service levels.

Sixth: Enhancing International Cooperation

International cooperation in the field of cybersecurity is of utmost importance, as cybercrime transcends geographical boundaries and requires the concerted efforts of countries and organizations to combat it. Enhancing international cooperation involves developing Egypt's strategy for international cooperation in cybersecurity, establishing principles and directions for Egyptian cyber diplomacy, focusing on leadership and innovation, ensuring the prevention, detection, and response to cyber threats, and prosecuting perpetrators.

Seventh: Changing Community Culture Regarding Cybersecurity

This section covers various efforts to change community culture regarding cybersecurity. This is crucial since many sectors lack basic knowledge of cybersecurity principles, leading to vulnerability to cyber attacks. To change community culture, several activities are planned, targeting different groups.

These include creating a simplified cybersecurity awareness platform through audio-visual media, developing educational games for children to convey necessary information in an engaging manner, integrating cybersecurity curricula in schools, conducting awareness campaigns in schools, launching general awareness campaigns for various community segments, and providing specialized training programs to prepare professionals capable of competing in the cybersecurity field.

Eighth: Encouraging Scientific Research and Enhancing Innovation and Growth

This section highlights efforts to encourage scientific research and enhance innovation and growth, which are essential due to the continuous evolution of technologies and methods used in cyber attacks. Keeping pace with these developments requires advancements in defensive technologies and the creation of new technologies to enhance cybersecurity. Efforts in this area include supporting small project incubators, encouraging local and foreign investment to increase the number of cybersecurity service providers, providing qualified personnel to offer cybersecurity services, and promoting cooperation with universities, research centers, and public and private sector companies to support research and development.

Ninth: Performance Indicators

This part is among the most important sections of the strategy, as key performance indicators are crucial for monitoring the implementation of the strategy and measuring progress. The indicators consist of several quantitative and qualitative measures, including overall indicators, national talent indicators, growth and innovation indicators, national partnership indicators, and awareness indicators.

Requirement Six
Results of Egyptian Efforts in Cybersecurity

Any international agreement is always met with a commitment, prompting the international community to establish mechanisms for measuring performance, commitment, and progress over a specific period. This led to the emergence of several international and global indicators, including the **Global Cybersecurity Index (GCI)** issued by the Global Cybersecurity Center of the International Telecommunication Union (ITU), which analyzes countries' performance based on 80 sub-indicators, and the **National Cyber Security Index (NCSI)** issued by the National Cybersecurity Center in Estonia (NCSC). Based on these two indices, Egypt ranked 23rd globally in the ITU's 2020 cybersecurity readiness assessment and 60th globally in the NCSI in November 2021.

Egypt has achieved significant successes in the field of cybersecurity, summarized as follows:

- Participation in the Budapest Conference on Cyberspace in October 2012 in Hungary.
- Participation in the Arab Regional Workshop on Protecting Children Online organized by the ITU in June 2012.
- Formation of the National Committee for Protecting Children Online in March 2013.
- The Egyptian Computer Emergency Response Team (EG-CERT) ranked third in the ITU's Global Cybersecurity Index in October 2013.
- EG-CERT obtained membership in the steering committee of the Organization of Islamic Cooperation's Computer Emergency Response Team in November 2013.
- Hosting the fifth regional cybersecurity conference and the FIRST regional forum for the Arab and African regions in November 2016.
- Participation of EG-CERT in the ITU regional forum and the emergency response readiness workshop for the Arab and African regions in November 2017.
- Egypt organized the CAISEC'22 Information Security and Cybersecurity Exhibition and Conference on June 13-14, 2022, under the title "Cybersecurity in Times of Crisis," supported by various ministries.
- Egypt was elected to chair the Supreme Council of Communications and Information Technology of the African Union for two years and also to chair the Executive Bureau of the Arab Council of Ministers for Communications and Information Technology for two years.
- Egypt chaired the 24th session of the Arab Council of Ministers for Communications and Information.
- Egypt won membership in the ITU's Administrative Council for Africa and the ITU's Radio Regulations Committee for 2023.

Results and Recommendations

First: Institutional Aspects

1. Define a Work Plan, Responsibilities, and Timely Tasks: Ensure the allocation of digital resources (according to the principles of availability, integrity, and transparency).

2. Expand Issuance of Sectoral Strategies Across All State Institutions: Enforce adherence and impose penalties for non-compliance, as digital assets are critical state assets.

3. Increase Transparency in Publishing the Strategy and Its Implementation Stages: Achieve the strategy's goals by activating the role of the Supreme Council for Cybersecurity in setting sectoral plans, monitoring the strategy's implementation, and ensuring compliance.

4. Develop a Cybersecurity Guideline: Each governmental agency and institution should publish and disseminate this under the supervision and follow-up of the Supreme Council for Cybersecurity.

5. Align Strategy Implementation with the State's Approach: Ensure coordination with other national strategies such as the AI Strategy, Anti-Corruption Strategy, Climate Strategy, Sustainable Development Plans, and Economic Plans.

6. Include Legislative Representatives in the Supreme Council for Cybersecurity: Ensure continuous and permanent updates of governing legislation to keep pace with rapid developments in cybersecurity protection and cyberattacks, as stipulated in the third pillar of the strategy, "Building a Comprehensive Legislative Framework."

7. Include Scientific Research Representatives: Appoint research bodies related to cybersecurity within the membership of the Supreme Council for Cybersecurity, alongside experts at the consultant level or equivalent, as outlined in the ninth pillar of the strategy, "Programs to Promote Scientific Research and Enhance Innovation and Growth."

Second: Legislative and Judicial Aspects

1. Complete the Optimal Legislative Framework: In line with the strategy's third pillar, "Building a Comprehensive Legislative Framework," strengthen the institutional and regulatory framework to protect digital assets and achieve cybersecurity by enhancing existing legislation with effective and comprehensive laws to address cybercrimes and protect individuals and institutions.

- **Amend the Cybercrimes Law No. 175 of 2018:** Eliminate reconciliation in cybercrimes and increase penalties to felonies if

the criminal act is related to national security or economic stability, or is executed for terrorist purposes.

- **Amend the Telecommunications Regulation Law:** Create an independent IT experts' department under the Ministry of Justice experts' administration as part of the Ministry of Justice experts' office.
- **Confidential Trials for Cybersecurity Crimes:** While the Egyptian legislature has appropriately assigned the Economic Court to handle all cybersecurity disputes and crimes, it is proposed that trials be confidential to encourage victims of cybercrimes to report without fear of defamation.

Third: Awareness, Education, and Workforce Development

1. **Promote Awareness Campaigns Across All Media Forms:** Use various media platforms (visual, auditory, print, and online) to conduct awareness campaigns suited to different cultures, age groups, specializations, and education levels.

2. **Enhance Security Awareness:** Educate individuals and institutions on the importance of cybersecurity and basic prevention and defense methods, organizing awareness campaigns and training to enhance knowledge and skills in cybersecurity.

3. **Integrate Cybersecurity Culture in Education:** Adopt educational curricula at all levels to spread awareness among students of all ages, creating a generation that values cybersecurity and can face challenges.

4. **Focus on Innovation and Research and Development:**

- **Support Innovation and Research in Cybersecurity:** Address evolving and future threats by investing in developing new technologies and tools for detecting, preventing, and responding to cybercrimes.

- **Invest in Human Resources:** Train and continuously develop effective personnel with updated skills to face challenges and manage crises.

Fourth: International Cooperation and Performance Monitoring

1. **International Cooperation and National Commitment:**

- **Effective International Collaboration:** Cooperate with other countries in combating cybercrimes, exchanging information and expertise, sharing best practices, and collaborating in cybercrime investigations to address common threats.

- **Strengthen Partnerships:** Encourage collaboration among public, private, and academic sectors locally and internationally to combat cybercrimes, sharing information, expertise, and developing effective technological solutions and strategies.

2. Performance Monitoring:

- **Adopt International Best Practices:** Use international plans and best practices in strategy formulation, tailoring them to fit the Egyptian vision and specific challenges, with constant updates from the ITU guide.

- **Track Global Indicators:** Follow global indicators and adopt their evaluation methodologies to achieve leading positions, aiming for the top.

- **Establish Audit and Review Mechanisms:** Implement mechanisms for auditing and reviewing cybersecurity policies and strategies to measure performance and apply relevant global standards and benchmarks.

■ References:

First: Arabic References*:

Al-Awadi, Aws. (n.d.). Cyber Information Security. Bayan Center for Studies and Planning.

General Information Authority. (n.d.). General Information Authority Report of the Arab Republic of Egypt.

Jaafar, Hatem, Al-Qadi, Haitham, and Labeeb, Mohamed. (2023). Strategic and Legal Frameworks for Cybersecurity. National Anti-Corruption Academy.

Al-Hussein, Hassan. (2022). Basics of Cybersecurity. Syria.

Aquas, Khaled. (2018). Cybersecurity in the Arab Convention on Combating Information Technology Crimes, pp. 303-306.

Egyptian Cabinet. (2023). Nation's Tale. Volume One.

Abd Al-Sadiq, Adel. (2018). Cyber Attacks: New Patterns and Challenges to Global Security. Arab Center for Cyber Space Research.

Al-Otaibi, Abdulrahman, and Mirghani, Al-Murshidi. (2020). The Role of Cybersecurity in Achieving Vision 2030. Naif Arab University for Security Sciences.

Al-Amarat, Fares, and Al-Hamamseh, Ibrahim. (2022). Cybersecurity: Concept and Challenges of the Era. First Edition.

Suleiman, Qataf, and Boukreen, Abdelhalim. (n.d.). Confronting Cyber Crimes in Light of International Agreements. Faculty of Law and Political Sciences - Amar Telidji University, Laghouat, Algeria.

*References in all journal papers are arranged following the Arabic alphabetical order

Al-Tayeb, Mustafa. (n.d.). Introduction to Cybersecurity: An Introduction to Cybersecurity, Networks, and Operating Systems. Scientific Blog.

Al-Samhani, Mona. (2020). Requirements for Achieving Cybersecurity for Information Management Systems. Journal of the Faculty of Education, Mansoura University, Issue 11.

Al Khalifa, Mai. (2023). The Role of Digital Transformation in Achieving Cybersecurity: An Applied Study on the Ministry of Justice in the State of Qatar. Journal of Administrative Research, Issue 1.

Ahmed, Hilali. (2011). Budapest Convention on Cybercrime: A Commentary. Dar Al-Nahda Al-Arabiya.

Ahmed, Hilali. (1997). Inspection of Computer Systems and Guarantees of the Information Accused. Dar Al-Nahda Al-Arabiya Printing House.

Batikh, Hatim, (2021)"The Evolution of Legislative Policy in the Field of Combating Cybercrimes: A Comparative Analytical Study." Journal of Legal and Economic Studies, Sadat University, Vol. 5, Issue 1.

Wazir, Abdel Azim. 2009. **Explanation of the Penal Code - General Section.** Part One: The General Theory of Crime. Dar Al-Nahda Al-Arabia.

Second: Articles and Websites:

Arab National Development Planning Portal affiliated with ESCWA. (n.d.).

Al-Youm Al-Sabea Newspaper. (2015, January 14). Combating Electronic Terrorism.

Egyptian Ministry of Communications and Information Technology. (n.d.). Official Website.

Media Center of the Egyptian General Information Authority. (n.d.).

Al-Masdar Newspaper. (2014, December 18).

Al-Rayes, Suzy. (n.d.). Definition of Strategy. Al-Maqal Website.

E-Government Survey 2022: The Future of Digital Government. (n.d.).

American National Institute of Standards and Technology. (n.d.). Issuance of a Cybersecurity Strategies Governance Framework.

Saudi National Cybersecurity Guidance Center. (n.d.). Official Website.

Al-Youm Al-Sabea Website. (n.d.).

Egypt's Status Report according to the 2021 National Cybersecurity Index Report. (n.d.).

National Information Center Report. (n.d.).

Third: English References and Websites:

[This section will be populated with the relevant English references and websites].

1- Draft Explanatory Memorandum to the Draft convention on cybercime", Strasbourg, 14, February 2001.

2- Final activity report", "Draft explanatory memorandum, prepared by committee of experts on crime in cyber - Space, Strasbourg 25 May 2001.

3- Cambridge Dictionary, available online via the link https://dictionary.cambridge.org/dictionary/english/cyber; last accessed 03/03/2024.

4- Recommendation X.1205 (04/08) Overview of cybersecurity, available in different languages including the Arabic language, available at https://www.itu.int/rec/T-REC-X.1205-200804-I; last accessed 03/03/2024.

5- https://csrc.nist.gov/glossary/term/cybersecurity; last accessed 03/03/2024.

6- Cyber Warfare: A Multidisciplinary Analysis, Edited By James A. Green , Chapter 2 Understanding Cyber-Attacks by Duncan Hodges and Sadie Creese, first edition 2016, Routledge, ISBN 9780415787079.

7- A History of Cyber Security Attacks 1980 to Present, by Bruce Middleton, first edition 2017, Routledge, ISBN 9780367657857.

8- "Cost of a Data Breach Report 2023", By IBM, which is a leading multinational computer software corporations, the report is available in the English language and is available at https://www.ibm.com/reports/data-breach; last accessed 03/03/2024.

9- Estimated cost of cybercrime worldwide 2017-2028, available at, https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide; last accessed 03/03/2024.

10- Emerging Cyber Threats and Cognitive Vulnerabilities, edited by: Vladlena Benson and John Mcalane, Chapter 4 - The social and psychological impact of cyberattacks by Maria Bada and Jason R.C. Nurse, first edition 2020 Academic Press, ISBN 978-0-12-816203-3, page 73-74.

11- The Impact of Cyber Security on Business: How to Protect Your Business, by Emiles Mbungu Kala, Open Journal of Safety Science and Technology, Vol.13 No.2, June 2023, available at https://www.scirp.org/journal/paperinformation?paperid=126109; last accessed 03/03/2024.

12- The Global Cyber Threat: Cyber threats to the financial system are growing, and the global community must cooperate to protect it; by Tim Maurer and Arthur Nelson; a report issued by the International Monetary Fund March 2021, available at https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf; last accessed 03/03/2024.

13- https://www.nist.gov/about-nist

14- https://www.nist.gov/cyberframework

15- https://rm.coe.int/budapest-convention-in-arabic/1680739173

16- Explanatory Report to the Convention on Cybercrime: Budapest, 23.XI.2001, available at, https://rm.coe.int/16800cce5b; last accessed 03/03/2024.

17- https//:www.escc.gov.eg/

18- https://egcert.eg/ar/

19- https://gate.ahram.org.eg/News/3187514.aspx

20- https://andp.unescwa.org/sites/default/files/2021-11/AR_National_Cybersecurity_Strategy_2017_2021.pdf

21- https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

22- https://ncsi.ega.ee/

23- https://andp.unescwa.org/sites/default/files/2021-11/AR_National_Cybersecurity_Strategy_2017_2021.pdf

24- http://www.itu.int/md/S06-PP-C-0024-en.

25- www.bayancenter.org

26- https://www.oolom.com/6124/

Fourth: French References:

Melanie Kowalski، «Cybercriminalité، enjeux، sources de données et faisabilité de recueillir des données auprès de la police»، Centre canadien de la statistique juridique، catalogue No 85-558-XIF، Décembre 2002.

Rôle des Conventions Internationales et Régionales dans le Domaine de la Cybersécurité et la Position de l'Egypte à leur égard

Le juge/
Dr/ Mohamed Ahmed Labib Ahmed
Vice- président de la Cour d'Appel

Le juge/
Haitham Mohamed Bahaa El-Kady
Président de la Cour d'Appel

Le juge/
Mostafa Ahmed Kamal
Vice-Président du Conseil d'État

Résumé:

La cybersécurité est devenue un domaine incontournable dans notre monde en raison de la nécessité de contrer les attaques et les crimes informatiques. Par conséquent, il est impératif que la communauté internationale lutte contre cette invasion criminelle technologique en adoptant davantage de législations et de lois punitives et procédurales adaptées à la gravité de ces crimes, et en mettant en place les mesures nécessaires pour les affronter.

Pour cette raison, plusieurs organisations internationales ont pris diverses initiatives dans le domaine de la lutte contre la cybercriminalité, telles que l'Union Internationale des Télécommunications, l'Institut National des Normes et de la Technologie, et l'Agence Européenne de la Cybersécurité.

La communauté internationale, notamment en Europe, a porté une attention particulière à la réglementation du domaine des technologies de l'information, en déployant de nombreux efforts législatifs pour lutter contre la cybercriminalité. Parmi ces efforts, l'Union européenne a adopté la Convention de Budapest sur la cybercriminalité, visant principalement à harmoniser les éléments du droit pénal substantiel national et à établir un système de coopération internationale rapide et efficace.

De même, la Ligue des États arabes a émis la Convention arabe sur la lutte contre les crimes informatiques, visant à renforcer la coopération entre les pays arabes pour protéger leur sécurité, leurs intérêts, et le bien-être de leurs sociétés contre les menaces de la cybercriminalité.

De plus, L'Égypte a connu une forte dynamique dans le domaine de la sécurité de l'information et des réseaux. Elle s'est efforcée de construire et de mettre en place un système moderne capable de protéger le cyberespace égyptien. À cette fin, le Conseil Supérieur de la Cybersécurité a été créé sous la présidence du Ministre des Communications et des Technologies de l'Information, avec des représentants du gouvernement, du secteur privé et de la société civile. L'Égypte a également mis en place le Centre Égyptien de Réponse aux Urgences Informatiques (CERT), affilié à l'Autorité Nationale de Régulation des Télécommunications, et a créé un Centre de Réponse aux Urgences Informatiques pour le secteur financier, affilié à la Banque Centrale. Ensuite, elle a publié la Stratégie Nationale de Cybersécurité de la République Arabe d'Égypte 2017-2021, suivie par la Stratégie Nationale de Cybersécurité de la République Arabe d'Égypte 2023-2027.

Mots-clés :
Cybersécurité, Conventions sur les technologies de l'information, cybercriminalité, Convention de Budapest, Criminalité informatique, CERT, Cyberattaques.

■ Introduction

L'émergence de l'informatique et l'expansion de l'utilisation d'Internet ont entraîné des effets négatifs et des risques. Cela a conduit à un intérêt croissant pour la cybersécurité. Par conséquent, la coopération internationale est devenue cruciale pour établir des cadres réglementaires et institutionnels afin de coordonner les efforts nationaux visant à protéger le cyberespace et à faire face aux menaces croissantes.

L'ONU a été à l'avant-garde de ces efforts, accompagnée d'autres organisations internationales comme l'Union internationale des télécommunications et Interpol, qui ont lancé diverses initiatives pour lutter contre la cybercriminalité.

En plus des efforts internationaux des organisations susmentionnées, d'autres initiatives ont été prises au niveau régional. En 2001, le Conseil de l'Europe s'est réuni à Budapest et a adopté la Convention européenne sur la cybercriminalité, qui est devenue la base juridique mondiale pour la lutte contre la cybercriminalité.

La Ligue arabe a également contribué à ces efforts en adoptant la Convention arabe sur la cybercriminalité en 2010.

En Égypte, des efforts significatifs ont été déployés dans le domaine de la sécurité de l'information et des réseaux. Le pays a œuvré à la création d'un système capable de protéger le cyberespace égyptien, notamment par la création du Conseil supérieur de la cybersécurité. L'Égypte a également mis en place le centre égyptien de réponse aux urgences informatiques (CERT) et le Centre de réponse aux urgences informatiques pour le secteur financier, rattaché à la Banque centrale. Par la suite, l'Égypte a publié la stratégie nationale de cybersécurité 2017-2021, suivie de la stratégie nationale de cybersécurité 2023-2027.

■ Premièrement : Importance de la recherche

La technologie de l'information et de la communication a provoqué une révolution complète dans tous les aspects de la vie, augmentant ainsi la domination des technologies de l'information et de la communication sur le mode de vie général. Avec l'apparition de l'ordinateur et l'expansion de l'utilisation d'Internet dans divers domaines de la vie, certaines conséquences négatives et risques associés à cette grande expansion ont émergé. Plus la dépendance à ces technologies pour le développement augmente, plus les risques, liés à la protection de l'information, augmentent également. Avec la dépendance mondiale croissante aux technologies de l'information et de la communication, l'exposition aux cybercrimes a également augmenté, rendant le cyberespace vulnérable aux violations par des pirates informatiques, qu'il s'agisse d'États ou d'autres entités possédant ces technologies informatiques.

En conséquence, l'attention s'est fortement tournée vers la cybersécurité, et la protection de celle-ci est devenue une question de sécurité nationale pour les États. La sécurité du cyberespace est devenue une priorité pour de nombreux pays, et les menaces croissantes à la sécurité du cyberespace ont poussé de nombreux États à entreprendre de grands efforts pour établir des lois visant à lutter contre la cybercriminalité. Par

conséquent, il est devenu nécessaire d'unifier les efforts internationaux pour mettre en place des cadres juridiques, réglementaires et procéduraux afin de faire face aux risques cybernétiques et à leurs impacts au niveau international, et de renforcer les formes de coopération internationale pour les combattre (Abdel Halim, p. 20).

Aussi l'importance de cette recherche réside-t-elle dans la nouveauté et l'obscurité des menaces à la cybersécurité pour un large secteur de la population, ainsi que dans l'impact des cyberattaques sur les individus, les institutions et même les sociétés dans leur ensemble. Enfin, l'importance mondiale de la protection de la cybersécurité et de la lutte contre les cyberattaques croissantes met en évidence le besoin d'enrichir la bibliothèque arabe avec une recherche qui contribue à combler le déficit de connaissances et à évaluer les efforts actuels déployés en Égypte dans ce domaine, dans le but de participer à la proposition d'améliorations susceptibles de servir les intérêts des citoyens et du pays.

- **Deuxièmement : Objectifs de la recherche (Raisons du choix du sujet) :**

Il est indéniable que la diversité des cadres législatifs nationaux, des lois, des règlements et des réglementations adoptés par les différents pays pour faire face aux cybercrimes représente l'une des difficultés auxquelles la communauté internationale est confrontée dans la coordination des efforts pour réduire ces crimes. Les criminels de la sécurité de l'information exploitent cette divergence en commettant leurs crimes à travers les frontières des pays où les risques d'application des lois sont moindres par rapport à d'autres pays.

Bien que la souveraineté nationale des États soit une réalité incontournable, les risques et les défis auxquels la communauté internationale est confrontée exigent la nécessité de coordonner les efforts entre les pays pour réaliser l'intérêt supérieur des citoyens. Par conséquent, il est nécessaire de conclure des accords internationaux pour lutter contre ces crimes, en définissant les grandes lignes que les différents pays doivent suivre lors de l'élaboration de cadres législatifs et réglementaires visant à faire face aux cybercrimes.

- **Troisièmement : Méthode de la recherche :**

L'étude de ce sujet nécessite une diversité de méthodes de recherche, sans se limiter à une seule méthode, afin de servir les objectifs de la recherche. Par conséquent, nous suivrons les méthodes de recherche suivantes dans notre étude :

L'approche théorique dans la recherche sur la cybersécurité, basée sur l'étude et l'analyse des théories et des concepts liés à la cybersécurité et leur application dans des contextes pratiques, la compréhension des bases théoriques des cyber-menaces et des solutions de sécurité, à travers l'étude des recherches et des sources publiées sur la cybersécurité dans des articles scientifiques, des livres et des rapports, jusqu'à l'analyse et l'interprétation du cyber-comportement, contribuerait à comprendre les phénomènes et les processus complexes, et à développer des théories et des cadres conceptuels afin d'améliorer les stratégies de cybersécurité.

Cette étude vise également à effectuer une analyse approfondie des législations internationales relatives à la cybersécurité et à documenter les résultats, en s'appuyant sur les méthodologies suivantes :

1. **La méthode inductive** : reposant sur l'examen des opinions doctrinales et des décisions judiciaires concernant les sujets abordés par la recherche, afin d'identifier les points de divergence et de mettre en évidence les avis les plus probants.

2. **La méthode analytique** : visant à analyser les textes existants, afin d'évaluer leur pertinence par rapport aux sujets traités par la recherche.

3. **La méthode comparative :** en comparant la situation juridique dans les différentes conventions internationales.

■ Quatrièmement: Plan de recherche

Pour donner une idée complète et établir une structure intégrale pour notre sujet de recherche, nous avons consacré **une préface** dans laquelle nous avons traité de la nature de la cybersécurité, et nous l'avons divisée comme suit :

1- Définition de la cybersécurité et des termes utilisés dans ce domaine

2- Aperçu historique de la cybersécurité

3- L'Importance de la cybersécurité

4- Objectifs de la cybersécurité

Ensuite, dans **la première partie** de notre recherche, nous avons abordé les conventions internationales et régionales dans le domaine de la cybersécurité, selon les détails suivants :

1- Efforts des Nations Unies dans la lutte contre la cybercriminalité

2- Efforts des organisations internationales dans la lutte contre la cybercriminalité

A- Rôle de l'Union Internationale des Télécommunications (UIT) dans le domaine de la cybersécurité

B- Rôle de l'Institut National des Normes et de la Technologie (NIST) dans le domaine de la cybersécurité

C- Rôle de l'Agence Européenne pour la Sécurité des Réseaux et de l'Information (ENISA) dans le domaine de la cybersécurité

3- Rôle des conventions régionales dans la lutte contre la cybercriminalité

A- Convention de Budapest sur la cybercriminalité

B- Convention arabe sur la lutte contre les crimes de technologies de l'information

Dans **la deuxième partie**, nous avons abordé les efforts égyptiens dans le domaine de la cybersécurité et nous l'avons divisée en six points, comme suit :

1- Le Conseil Supérieur de la Cybersécurité

2- Le Centre Égyptien de Réponse aux Urgences Informatiques (EG-CERT)

3- Le Centre de Réponse aux Urgences Informatiques du Secteur Financier

4- La Stratégie Nationale de Cybersécurité de la République Arabe d'Égypte 2017-2021

5- La Stratégie Nationale de Cybersécurité de la République Arabe d'Égypte 2023-2027

6- Évaluation des efforts égyptiens dans le domaine de la cybersécurité

Préface

Qu'est-ce que la cybersécurité

A travers cette préface, nous visons à mettre en évidence la notion de cybersécurité. Nous commencerons par définir la cybersécurité et présenterons les principaux termes utilisés dans ce domaine. Ensuite, nous offrirons un bref aperçu historique de la cybersécurité dans la mesure où cela sert les objectifs de la préface. Puis, nous discuterons de l'importance croissante de la cybersécurité et, enfin, nous aborderons les principaux objectifs de la cybersécurité.

1- Définition de la cybersécurité et des termes utilisés dans ce domaine

Signification du terme «cyber» : Le terme «cyber» se rapporte à tout ce qui est lié à l'informatique, aux réseaux informatiques de tous types (comme l'Internet) ou aux communications électroniques en général (Dictionnaire Cambridge). Le terme «cyber» est ainsi utilisé pour désigner tout ce qui concerne les réseaux électroniques informatiques et l'Internet. Par exemple, lorsque nous parlons de cyberespace, nous faisons référence à l'espace électronique.

Il n'existe pas de définition universelle et consensuelle de la **cybersécurité** parmi les différentes littératures et praticiens. Cependant, nous pouvons la définir de manière succincte comme l'utilisation de tous les moyens nécessaires pour protéger le cyberespace contre les cyber-attaques. Cela inclut un ensemble de mesures techniques, organisationnelles et administratives visant à empêcher l'accès non autorisé aux informations électroniques et à prévenir leur exploitation illégale et non réglementée (El-Anzi, 1443 Hijri, p.22).

Plusieurs documents émis par des organisations internationales gouvernementales, comme l'Union Internationale des Télécommunications (UIT), ont tenté de définir la cybersécurité. Par exemple, la recommandation (UIT-T X.1205) définit la cybersécurité comme un ensemble d'outils, de politiques, de concepts de sécurité, de garanties, de lignes directrices, de démarches de gestion des risques, de procédures, de formations, de meilleures pratiques, de moyens d'assurance et de technologies pouvant être utilisés pour protéger l'environnement cybernétique, l'organisation et les actifs des utilisateurs. L'organisation et les actifs des utilisateurs comprennent les équipements informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de communication et l'ensemble des informations transmises ou stockées dans l'environnement cybernétique (Aperçu de la cybersécurité).

Nous pouvons tirer de la définition ci-dessus, ainsi que de la majorité des autres définitions disponibles de la «cybersécurité», qu'il y a trois éléments ou aspects essentiels à la cybersécurité :

- Prévention: Utiliser et mettre en œuvre les politiques, mesures et pratiques disponibles pour empêcher tout accès ou violation non autorisés.

- Détection : Identifier les menaces et les vulnérabilités potentielles existant dans les systèmes et dispositifs protégés.

- Réponse : Déterminer et mettre en œuvre les meilleures solutions nécessaires pour arrêter, réparer ou atténuer l'impact et les résultats des incidents et violations de sécurité.

Le terme «cyberespace», tel que défini par l'Institut National des Normes et de la Technologie (NIST) des États-Unis, désigne un domaine global au sein de l'environnement de l'information, constitué d'un réseau indépendant d'infrastructures des systèmes d'information. Cela inclut les réseaux Internet, les réseaux de communication, les systèmes informatiques, les processeurs et les dispositifs de contrôle intégrés (NIST).

Des «cyber-attaques» font référence à des assauts électroniques contre un système, une organisation ou un individu, visant à perturber, voler ou endommager les actifs numériques ou physiques contenant des composants électroniques, mettant en péril la confidentialité, l'intégrité ou la disponibilité des actifs numériques (James, 2016, p. 34).

2- Aperçu historique de la cybersécurité

L'histoire de la cybersécurité remonte aux années 1970, à une époque où certains termes comme logiciels espions, virus et vers informatiques n'étaient pas encore courants. En raison de l'augmentation du taux de cybercriminalité, ces termes ont commencé à apparaître fréquemment dans les gros titres des journaux. Lorsque l'on remonte à l'époque de la création de la cybersécurité, on constate que les ordinateurs et Internet étaient encore en développement, et il était facile d'identifier les menaces auxquelles les ordinateurs pouvaient être exposés.

Dans les années 1980, le scientifique Robert T. Morris a créé le premier virus informatique, qui a fait l'objet d'une couverture médiatique immense en raison de sa propagation rapide entre les appareils et des dysfonctionnements qu'il a causés dans les systèmes. Morris a été condamné à une peine de prison et à une amende, et cette condamnation a joué un rôle dans le développement des lois relatives à la cybersécurité.

Puis, dans les années 1990, les événements marquant le développement de la cybersécurité se sont succédés au fil du temps, avec l'évolution des virus infectant les appareils. Le monde a pris conscience des risques informatiques. Parmi les mesures prises dans les années 1990, on trouve la mise en place de protocoles de protection des sites web comme le (HTTP), qui est un type de protocole permettant aux utilisateurs d'accéder de manière sécurisée à Internet.

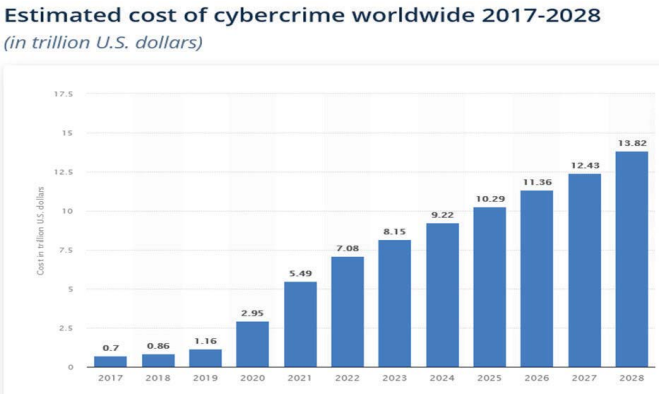
Ainsi, les cyberattaques et la cybercriminalité ont continué à évoluer, tout comme la cybersécurité, jusqu'à atteindre le niveau de sophistication et de complexité que nous observons aujourd'hui. Dans le monde numérique dans lequel nous vivons, la cybersécurité est devenue aussi importante que les systèmes de défense militaire, car les cyberattaques sophistiquées peuvent causer des dommages surpassant ceux des guerres, qu'ils soient économiques ou même humains. Aujourd'hui, nous dépendons des ordinateurs et d'Internet pour presque tout (Middleton, Bruce 2017, p.35).

3- L'importance de la cybersécurité

La technologie moderne est utilisée dans presque tous les aspects de nos activités quotidiennes ; le monde devient de plus en plus numérique, et les individus, les entreprises et même les gouvernements dépendent fortement de la technologie moderne. C'est pourquoi la cybersécurité est devenue un enjeu crucial et fondamental.

Les statistiques montrent une augmentation du rythme et des coûts des cybercrimes dans le monde entier. Voici quelques-unes de ces statistiques et estimations, qui illustrent clairement l'augmentation des cyberattaques et des pertes financières énormes causées par la cybercriminalité. Selon le rapport sur le coût de la violation de données de 2023 publié par IBM, «le coût moyen d'une violation de données en 2023 était de 4,45 millions de dollars américains.

Figure n° (1) Coût estimé de la cybercriminalité dans le monde 2017-2028 (1)



Au niveau international, le coût de la cybercriminalité s'est élevé à 8,15 billions de dollars en 2023. Le graphique précédent reflète les prévisions mondiales du coût estimé de la cybercriminalité.

De manière générale, les cyberattaques ont un impact sévère sur les individus, les entreprises, les gouvernements et la société dans son ensemble ; cet impact sera brièvement souligné dans les quelques paragraphes suivants.

Les cyberattaques affectent les individus de plusieurs façons : des pertes financières peuvent survenir à la suite du piratage de comptes financiers ou de transactions non autorisées. Le vol d'identité est également une possibilité (ce qui peut entraîner des pertes financières supplémentaires ou même des conséquences légales). De plus, les cyberattaques peuvent nuire à la réputation des victimes si des informations ou des photos privées sont divulguées. Enfin, les conséquences peuvent inclure un stress mental en raison des pressions psychologiques et nerveuses (Benson et Mcalane, 2020 pp. 73-74.).

Pour les entreprises, l'impact des cyberattaques est crucial car elles peuvent entraîner :

1. Des perturbations opérationnelles comme des pannes de système ou des interruptions

(1) Voir « Rapport sur le coût d'une violation de données 2023", Par IBM, qui est une multinationale de premier plan dans le domaine des logiciels informatiques, le rapport est disponible en anglais sur https://www.ibm.com/reports/data-breach dernière consultation le 03/03/2024.
Voir Estimation du coût de la cybercriminalité dans le monde 2017-2028, disponible sur, https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide; dernière consultation le 03/03/2024

de service, réduisant la capacité de l'entreprise à fonctionner normalement.

2. Des pertes financières dues aux coûts de réparation des dommages causés par l'attaque, tels que la restauration des systèmes et des équipements endommagés, le paiement de rançons si elles ne peuvent être évitées, la perte potentielle de propriété intellectuelle, et les complications légales découlant des perturbations opérationnelles et du non-respect des lois.

3. Des dommages à la réputation résultant de la divulgation d'informations sensibles, de l'incapacité à fournir des services ou à livrer des produits en temps voulu, ce qui peut affecter négativement la confiance des différentes parties prenantes de l'entreprise et ainsi compromettre la réputation et l'image de l'institution (Kala, 2023).

Les cyberattaques peuvent également avoir un impact significatif sur les gouvernements, notamment :

1. Des perturbations opérationnelles des services publics vitaux comme les services de santé et les forces de l'ordre.

2. Une atteinte à la confiance du public (dommages à la réputation), car les citoyens peuvent s'inquiéter de la qualité et de la sécurité des services publics, ainsi que de la possibilité de divulgation de leurs informations personnelles à partir des bases de données gouvernementales.

3. Des conséquences financières, car la réparation des dommages causés par les cyberattaques peut coûter très cher, et avec l'augmentation des rançongiciels, certaines institutions publiques peuvent se voir contraintes de payer des rançons pour récupérer leurs données.

4. Des préoccupations liées à la sécurité nationale, car les cyberattaques peuvent viser des agences de maintien de l'ordre ou des agences militaires sensibles à des fins d'espionnage, de sabotage ou autres.

En raison des risques énormes et graves des cyberattaques, et de l'importance cruciale de la cybersécurité, le Fonds Monétaire International (FMI) a recommandé dans un rapport récent que la communauté internationale renforce la coopération mutuelle pour protéger les institutions financières (Maurer et Nelson; 2021).

4- Objectifs de la cybersécurité

Puisque l'objectif ultime de la cybersécurité est de sécuriser les appareils, les réseaux et les informations, et de les protéger contre toute intrusion ou attaque, quel que soit leur type, il n'est pas suffisant d'expliquer le concept et de définir les normes de sécurité, même pour les experts en cybersécurité. C'est pour cette raison qu'ils ont élaboré le modèle ou le triangle CIA, qui rassemble les trois concepts fondamentaux de la cybersécurité, à savoir :

1. Confidentialité : C'est l'équivalent de la « vie privée ». L'objectif est d'empêcher tout accès non autorisé aux données.

2. Intégrité : Il s'agit de maintenir les données précises et intègres, en les protégeant de toute modification ou altération non autorisée par un pirate ou une personne non

habilitée.

3. Disponibilité : Il s'agit de rendre les données accessibles et utilisables à tout moment par les personnes autorisées, en garantissant que le système ne soit pas entravé ou désactivé par diverses attaques (Al-Samhani, « 2020, P. 11).

Première partie

Les Conventions Internationales et Régionales dans le domaine de la Cybersécurité

En abordant la nature de la cybersécurité, nous avons souligné l'importance cruciale de la coopération entre les acteurs de la communauté internationale, qu'il s'agisse d'États ou d'organisations internationales gouvernementales ou non gouvernementales, pour établir des cadres réglementaires et institutionnels visant à coordonner les divers efforts nationaux des pays pour protéger le cyberespace et lutter contre les cybermenaces croissantes, en raison de leurs conséquences graves susmentionnées dans la préface de cette étude.

De nombreuses entités, organisations et conseils internationaux jouent un rôle notable dans la facilitation et la coordination de la conclusion de conventions internationales en matière de cybersécurité, dans le but de renforcer la nécessité de la coopération internationale pour faire face aux cybercrimes. Parmi ces organisations figurent les Nations Unies, le Conseil de l'Europe et certaines autres entités.

Ainsi, après avoir expliqué la nature de la cybersécurité, nous examinerons les efforts des Nations Unies dans la lutte contre la cybercriminalité, puis ceux des autres organisations internationales à cet égard, et nous terminerons par un aperçu du rôle des conventions régionales dans la lutte contre la cybercriminalité.

1- Efforts des Nations Unies dans la lutte contre la Cybercriminalité

Le Conseil économique et social des Nations Unies a recommandé que l'organisation internationale prenne un rôle principal dans l'élaboration de politiques de prévention du crime et de justice pénale internationale. Cette recommandation a été approuvée par l'Assemblée générale des Nations Unies en 1950, entraînant la création du Comité consultatif d'experts pour la prévention du crime et le traitement des délinquants, chargé de lutter contre la criminalité, de conseiller le Secrétaire général, de développer des programmes, d'élaborer des plans et de définir des politiques pour des mesures internationales dans la prévention du crime et le traitement des délinquants. Après la tenue de la Conférence des Nations Unies sur la prévention du crime et le traitement des délinquants à Kyoto, au Japon, en 1970, le Comité consultatif a été remplacé par le Comité de prévention du crime et de lutte contre le crime, basé sur une recommandation du Conseil économique et social en 1971.

Ce qui nous intéresse dans cette étude, ce sont les efforts des Nations Unies à travers leurs conférences spécifiques à la prévention du crime et au traitement des délinquants en relation avec les crimes technologiques ou les cybercrimes. À cet égard, la septième

Conférence des Nations Unies sur la prévention du crime et le traitement des délinquants, qui s'est tenue à Milan, en Italie, en 1985 (Abayneh, 2009, p. 156), a produit un ensemble de directives, finalisées dans les recherches régionales préparatoires pour la huitième conférence, qui a approuvé ces principes et s'est tenue à La Havane, à Cuba, en 1990.

Cette conférence a insisté sur la nécessité d'appliquer les nouvelles avancées scientifiques et technologiques dans l'intérêt public partout, et ainsi de prévenir efficacement le crime. Elle a également souligné que la technologie, bien qu'elle puisse générer de nouvelles formes de criminalité, nécessite des mesures appropriées contre les abus de la technologie moderne. Les recommandations de la conférence de La Havane de 1990 peuvent être résumées selon les principes suivants :

1. Modernisation des lois pénales nationales, y compris les mesures institutionnelles.

2. Amélioration de la sécurité informatique et des mesures de protection.

3. Adoption de procédures de formation adéquates pour le personnel et les agences responsables de la prévention des crimes économiques et des cybercrimes, ainsi que des enquêtes et des poursuites.

4. Enseignement de l'éthique informatique dans le cadre des programmes de communication et d'information, et adoption de politiques traitant des problèmes des victimes de ces crimes.

5. Renforcement de la coopération internationale pour lutter contre ces crimes (Abayneh, 2009, p. 158).

2- Efforts des Organisations internationales dans la lutte contre la Cybercriminalité

De nombreuses organisations internationales ont pris diverses initiatives dans le domaine de la lutte contre la cybercriminalité. Par exemple, les efforts déployés par l'Union internationale des télécommunications, l'Organisation internationale de police criminelle (Interpol), la Société pour l'attribution des noms de domaine et des numéros sur Internet (ICANN), l'Organisation internationale de normalisation (ISO), la Commission électrotechnique internationale et les groupes de travail de l'ingénierie Internet, ainsi que d'autres organisations et institutions internationales concernées par les crimes cybernétiques.

Dans les paragraphes suivants, nous examinerons les principaux efforts déployés par certaines des organisations internationales les plus importantes dans le domaine de la cybersécurité. Nous aborderons d'abord les efforts de l'Union internationale des télécommunications, puis ceux de l'Institut national des normes et de la technologie des États-Unis, et enfin ceux de l'Agence de l'Union européenne pour la cybersécurité.

A- Rôle de l'Union Internationale des Télécommunications (UIT) dans le domaine de la cybersécurité

L'Union internationale des télécommunications (UIT) est une agence spécialisée des Nations Unies dans le domaine des technologies de l'information et de la communication, fondée en 1865 pour faciliter la connectivité mondiale et améliorer les communications internationales. L'UIT est l'organisation principale chargée de développer les normes

internationales pour les technologies de l'information et de la communication, de promouvoir la connectivité mondiale et d'améliorer l'accès à ces technologies dans le monde entier ([2]).

Dans le cadre de ses efforts pour assumer son rôle de création et de développement de normes internationales pour la société de l'information et des technologies de l'information, l'UIT a lancé un guide pour l'élaboration de la Stratégie nationale de cybersécurité, révisée plusieurs fois. Dans la dernière version de ce guide, l'UIT a défini les parties prenantes dans les systèmes de cybersécurité des pays et les objectifs de cette initiative.

Douze partenaires internationaux, dont l'Agence de l'Union européenne pour la cybersécurité, ainsi que des organisations gouvernementales internationales, des organisations internationales, le secteur privé et la société civile, ont contribué à l'élaboration de ce guide.

Au début du manuel, l'objectif principal de ce manuel était défini : «guider les dirigeants nationaux et les décideurs dans l'élaboration d'une stratégie nationale de cybersécurité, en fournissant un cadre utile, flexible et facile à utiliser pour définir le contexte de la vision socio-économique du pays et son état de sécurité actuel».

Le champ d'application du guide a été défini pour inclure divers aspects des défis de la cybersécurité, notamment la gouvernance et la politique, les aspects opérationnels, techniques et juridiques, ainsi que les principes généraux et les bonnes pratiques pour élaborer une stratégie en tenant compte de la réalité pratique, c'est-à-dire les mesures «concrètes» prises par les pays à différents stades de la stratégie (Gaafar, El-Kady et Labib, 2023, pp. 93, 92).

Le public cible du guide comprend principalement les dirigeants nationaux et les décideurs chargés de développer une stratégie nationale de cybersécurité, ainsi que d'autres parties prenantes telles que les gouvernements, les organismes de réglementation, les fournisseurs de services de technologies de l'information et de la communication, les institutions académiques et de recherche.

Le guide a ensuite présenté les bonnes pratiques dans la Stratégie nationale de cybersécurité en se concentrant sur des concepts spécifiques appelés domaines de focalisation, à savoir :

1. Gouvernance :

Il est essentiel de mettre en place une structure disciplinaire et efficace pour la cybersécurité nationale en définissant des objectifs et ambitions souhaités dans le domaine de la cybersécurité, en identifiant les rôles , en assurant le plus haut niveau de soutien nécessaire pour atteindre ces objectifs, ainsi qu'en désignant une autorité compétente responsable de la mise en œuvre de la stratégie de cybersécurité et en impliquant les organismes gouvernementaux et les autres secteurs concernés dans la mise en œuvre de cette stratégie.

La stratégie doit s'engager à établir des objectifs spécifiques, mesurables, réalisables

(2) https://www.itu.int.

et axés sur les résultats et le temps dans le plan de mise en œuvre de la stratégie. Elle doit également reconnaître la nécessité de ressources adéquates (volonté politique, financement, temps et personnel) afin d'obtenir des résultats satisfaisants.

2. Gestion des risques en cybersécurité nationale :

Le domaine de «Gestion des risques» concerne la nécessité d'adopter une approche de gestion des risques identifiant et évaluant les risques auxquels le pays est exposé, et ce en déterminant les risques découlant des dépendances transfrontalières et des relations mutuelles et en gérant ces risques de manière très efficace. La gestion des risques dans le domaine de la cybersécurité doit également couvrir tout le cycle de vie, du placement ou de la fourniture à l'exploitation et au remplacement.

3. Préparation et Résilience :

Il s'agit de renforcer la capacité des pays à gérer et à résister aux cyberattaques en développant des capacités de réponse et de préparation à faire face à ces attaques. Cela inclut l'identification et l'évaluation des risques, l'élaboration de plans d'urgence, la mise en place de systèmes de gestion de crise et l'amélioration des capacités de vérification des actifs et services importants afin d'assurer la continuité des diverses opérations d'infrastructure. Il est également crucial de fournir des formations et des sensibilisations aux équipes spécialisées en sécurité de l'information dans diverses institutions ainsi que des formations en cybersécurité, afin d'élever le niveau de préparation et de résilience en cas de cyberattaque.

4. Infrastructures critiques et Services essentiels :

Ce domaine vise à renforcer la sécurité des infrastructures critiques en élaborant des stratégies de protection et de réduction des risques associés. Cela inclut l'identification des actifs et services essentiels, , le développement de plans de gestion des risques, ainsi que la mise en place de mesures de sécurité pour protéger ces actifs, y compris l'utilisation de technologies de sécurité avancées et la mise en place de systèmes de surveillance continue. La sensibilisation et la formation des équipes de sécurité de l'information sont également essentielles, afin d'accroître le niveau de sensibilité de ces institutions à toute cybermenace potentielle, tout en renforçant la coopération entre elles et les diverses parties intéressées travaillant dans ce domaine.

5. Capacité, Renforcement des compétences et Sensibilisation:

L'accent est mis sur le renforcement des capacités des individus, des institutions et des gouvernements en matière de cybersécurité à travers des programmes de formation et d'éducation afin d'améliorer les compétences et l'expertise dans ce domaine. Cela inclut également l'élaboration de stratégies visant à stimuler l'innovation dans le domaine de la cybersécurité en soutenant la recherche technologique et en développant de nouvelles solutions pour les défis futurs, ainsi que la sensibilisation à l'importance de la cybersécurité en général et dans des institutions spécifiques, par des campagnes de sensibilisation, des campagnes médiatiques, et l'intégration de cours de cybersécurité dans les programmes scolaires et universitaires.

6. Législation et Réglementation :

Ce domaine vise à établir un cadre juridique et réglementaire pour protéger la société contre les cybercrimes et promouvoir un environnement cybersécurisé. Cela inclut la définition des activités cybernétiques illégales, la reconnaissance des droits individuels et des libertés civiles dans le cyberenvironnement , la mise en place de mécanismes de conformité et de vérification de l'application de la législation, le développement de procédures juridiques pour lutter contre les cybercrimes, y compris le renforcement de la coopération internationale dans le domaine de lutte contre les cybercrimes, et l'échange d'informations et d'expériences dans ce domaine. En fin de compte, le sixième domaine de la stratégie de cybersécurité vise à créer un environnement cybersécurisé pour les individus, les entreprises et les gouvernements, grâce à l'application de la législation et de la réglementation appropriées afin de protéger la société contre les cybercrimes.

7. Coopération internationale :

Le dernier domaine vise à renforcer la coopération internationale en matière de cybersécurité à travers des discussions et des négociations internationales, la collaboration formelle et informelle dans le cyberespace, et l'établissement d'un consensus sur les règles de conduite pour les États. Il s'agit également de développer des mécanismes pour l'échange d'informations et d'expériences sur les cybercrimes et les meilleures pratiques entre les différents pays.

B- Rôle de l'Institut National des Normes et de la Technologie (NIST) dans le domaine de la cybersécurité

L'Institut National des Normes et de la Technologie, connu mondialement sous l'acronyme (NIST), est une institution gouvernementale américaine opérant sous la supervision du Département du Commerce des États-Unis. Fondé en 1901, le NIST est responsable du développement et de la promotion des mesures, des normes et de la technologie aux États-Unis. L'institut comprend un ensemble de laboratoires spécialisés en sciences et en technologies, ainsi qu'un centre de recherche et de développement ([3]).

Le Cadre de Cybersécurité du NIST

Le NIST a élaboré plusieurs cadres pour organiser et améliorer la gestion de la cybersécurité au niveau des industries, des entreprises et des institutions, ainsi qu'au niveau national. Parmi ces cadres, on trouve le cadre de travail en matière de cybersécurité, dont la première version a été publiée en 2014. Ce cadre a connu des améliorations et des ajustements ultérieurs prévus pour l'année prochaine.

Le cadre de cybersécurité identifie cinq éléments essentiels sous lesquels se déclinent de nombreux détails sur les procédures et opérations de gouvernance précis, disciplinés et séquentiels, que nous aborderons comme suit :

Premier élément : Identifier

Il s'agit de déterminer et comprendre les risques cybersécuritaires auxquels l'institution est confrontée, et d'identifier les actifs cybersécuritaires importants et sensibles à protéger. Ce processus comprend plusieurs étapes que les institutions doivent suivre, à savoir :

(3) www.nist.gov/about-nist

1. Identifier les actifs cybersécuritaires : Les institutions doivent identifier les actifs cybersécuritaires vitaux et sensibles pour elles, comme les données sensibles, les informations privées, les systèmes vitaux, et les équipements connectés au réseau. Elles doivent également localiser, classer et évaluer la valeur de ces actifs.

2. Identifier les risques cybersécuritaires : Les institutions doivent identifier et évaluer les risques cybersécuritaires, ainsi que déterminer l'impact potentiel de ces risques sur les actifs vitaux et sur les opérations de l'institution en général.

3. Identifier les exigences légales et réglementaires : Les institutions doivent identifier les exigences légales et réglementaires liées à la cybersécurité et s'y conformer, comme les règles de conformité émises par les organismes de réglementation et les lois gouvernementales en matière de cybersécurité.

4. Identifier les cadres généraux de cybersécurité : Les institutions doivent identifier les cadres généraux de cybersécurité en vigueur, comme les politiques, procédures et exigences de sécurité, et les évaluer régulièrement pour garantir leur conformité avec les évolutions cybersécuritaires.

5. Identifier les opportunités et défis : Les institutions doivent identifier les opportunités et défis liés à la cybersécurité, comme les opportunités de transformation numérique et les nouveaux défis liés à la cybersécurité, tels que les nouvelles cybermenaces et les cyberattaques sophistiquées, ainsi que le manque de ressources pour mettre en œuvre la cybersécurité.

Deuxième élément : Protéger

Cet élément vise à fournir la protection nécessaire aux actifs cybersécuritaires importants en mettant en œuvre les mesures de cybersécurité nécessaires, notamment les suivantes:

1. Mise en œuvre des mesures de sécurité : Les institutions doivent mettre en œuvre les mesures de sécurité nécessaires pour protéger les cyberactifs importants, comme la mise en place de politiques et de procédures de sécurité, le contrôle des accès et d'identité, l'authentification, le cryptage, et d'autres mesures de sécurité applicables.

2. Sensibilisation à la sécurité : Les institutions doivent sensibiliser leurs fonctionnaires et employés aux risques cybersécuritaires et leur fournir les formations nécessaires pour les aider à mieux comprendre et gérer ces risques.

3. Gestion des identités et des accès : Les institutions doivent mettre en œuvre des mesures pour gérer les identités et les accès afin de garantir que seuls les utilisateurs autorisés puissent accéder aux actifs importants, en appliquant des politiques de vérification d'accès et d'identité, d'autorisation et de contrôle d'accès, d'enregistrement et de surveillance.

4. Amélioration de la sécurité physique et matérielle : Les institutions doivent améliorer la sécurité physique des cyber-actifs importants, en sécurisant les appareils, les équipements, les installations vitales et en mettant en œuvre les mesures de protection nécessaires.

5. Amélioration de la cybersécurité dans la chaîne d'approvisionnement : Les

institutions doivent améliorer la cybersécurité de la chaîne d'approvisionnement en garantissant que les fournisseurs respectent les normes de cybersécurité en vigueur, en identifiant les risques potentiels liés à l'approvisionnement et en mettant en œuvre les mesures nécessaires pour atténuer ces risques.

6. Gestion des cyberincidents : Les institutions doivent préparer des plans de réponse aux cyberincidents et les mettre en œuvre pour faire face aux cyberattaques, les identifier, les vérifier, y répondre et restaurer le système.

Troisième élément : Détecter

Cet élément vise à améliorer la capacité de l'institution à détecter rapidement et à vérifier efficacement les cyberattaques et les incidents de sécurité indésirables. Cela aide à améliorer la capacité de l'institution à analyser les incidents de sécurité, à classifier les événements et à prendre les mesures appropriées pour faire face aux cybermenaces potentielles. Le processus de détection, d'analyse, et de réponse est optimisé par ''l'automatisation'' ([4]) et l'utilisation des technologies modernes, réduisant ainsi le temps de réaction et minimisant les dommages potentiels.

Quatrième élément : Répondre

Cet élément vise à améliorer la capacité de l'institution à répondre aux cyberattaques, à réhabiliter les systèmes et données affectés, et à réduire les dommages causés par ces attaques. Les activités incluent plusieurs étapes que les institutions doivent suivre, à savoir :

1. Réponse aux incidents : Les institutions doivent élaborer et mettre en œuvre des plans de réponse aux incidents, en définissant les rôles, responsabilités et procédures appropriés pour mettre en œuvre ces plans et s'assurer de la disponibilité des ressources nécessaires.

2. Réduction des dommages : Les institutions doivent prendre les mesures nécessaires pour réduire les dommages causés par les cyberattaques et réhabiliter les systèmes et données affectés, évaluer les dommages et identifier les priorités dans la reconstruction de l'infrastructure de l'institution.

3. Analyse forensique numérique : Les institutions doivent réaliser des analyses forensiques numériques des cyberincidents et des attaques qui y sont liées, collecter, évaluer et analyser les preuves numériques liées aux cyberincidents, afin de déterminer les responsabilités, les sources et les méthodes utilisées dans l'attaque, et identifier les preuves numériques qui peuvent être utilisées dans enquêtes criminelles.

4. Amélioration de l'automatisation : Les institutions doivent améliorer l'automatisation des réponses aux incidents en utilisant des outils d'automatisation, l'intelligence artificielle, l'apprentissage automatique et d'autres technologies modernes, afin d'améliorer l'efficience et l'efficacité des opérations de réponse et de réduire le temps nécessaire pour réhabiliter les systèmes affectés.

(4) L'automatisation, ou Automation, fait référence à un ensemble de processus informatiques, mécaniques et électromécaniques conçus pour fonctionner avec un minimum d'intervention humaine, voire aucune. Elle est couramment utilisée pour optimiser le fonctionnement d'usines industrielles, d'entreprises et d'autres secteurs qui cherchent à s'adapter à la transformation numérique.

5. Formation et exercices : Les institutions doivent organiser des formations et exercices pour leurs fonctionnaires sur la façon de faire face aux cyberattaques, sur la manière de mettre en œuvre efficacement des plans de réponse aux incidents, ainsi que d'organiser des formations sur la réponse aux incidents pour améliorer la capacité de l'institution à répondre aux cyberattaques et réhabiliter les systèmes affectés.

De manière générale, l'élément de réponse est un aspect fondamental pour maintenir et renforcer la cybersécurité des institutions. Il aide à améliorer la capacité à gérer les cyberattaques et à réduire les dommages qu'elles peuvent causer. De plus, il contribue à sensibiliser les institutions à l'importance d'une réponse efficace aux cyberattaques et à la mise en œuvre des plans nécessaires à cet effet.

Cinquième élément : Récupérer

Cet élément vise à mettre en œuvre les procédures et plans nécessaires pour restaurer les fonctions essentielles de l'institution après une cyberattaque ou d'autres incidents de sécurité. Les activités de récupération comprennent de nombreuses étapes et actions que les institutions doivent suivre, entre autres :

1. Identifier les ressources sensibles et critiques : Les institutions doivent identifier les ressources vitales, les données sensibles, les applications essentielles et les systèmes importants pour déterminer les priorités de restauration en cas de cyberattaques ou d'incidents de sécurité. Ce sont les ressources les plus affectées et les plus répandues.

2. Mesures de précaution : Les institutions doivent mettre en œuvre les mesures nécessaires pour préparer des copies de sauvegarde des données, systèmes et applications vitaux, les stocker dans des emplacements sécurisés et les mettre à jour régulièrement.

3. Récupération des données : Les institutions doivent mettre en œuvre les procédures nécessaires pour récupérer les données perdues ou endommagées après une cyberattaque ou d'autres incidents de sécurité.

4. Restauration des systèmes : Les institutions doivent mettre en œuvre les mesures nécessaires pour restaurer les systèmes affectés et les réhabiliter à leur état normal après une cyberattaque ou d'autres incidents de sécurité.

5. Tester la récupération : Les institutions doivent régulièrement tester et mettre à jour les plans de récupération en fonction des résultats des tests et former les fonctionnaires sur la façon de mettre en œuvre et de mettre à jour ces plans périodiquement (Gaafar, El-Kady et Labib, 2023, pp. 115 et 116).

C- Rôle de l'Agence Européenne pour la Sécurité des Réseaux et de l'Information (ENISA) dans le domaine de la cybersécurité

L'Agence de l'Union européenne pour la cybersécurité (ENISA), créée en 2004, travaille à renforcer la capacité des États membres et des organisations du secteur privé de l'UE à prévenir, détecter et répondre aux cybermenaces.

L'Agence élabore des plans stratégiques et des plans d'action exécutifs spécifiques pour la cybersécurité, visant à améliorer la capacité de l'Union européenne à faire face aux cybermenaces et à protéger les réseaux et les informations critiques. Le plan stratégique

actuel de cybersécurité de l'agence comprend de nombreuses initiatives et activités, telles que l'amélioration de la coopération entre les États membres, le renforcement de la sensibilisation et de la formation en matière de cybersécurité, le développement de normes européennes pour la cybersécurité et la fourniture de conseils techniques dans ce domaine.

L'Agence s'efforce d'atteindre plusieurs objectifs stratégiques en matière de cybersécurité, que l'on peut résumer comme suit :

1. Renforcer la sensibilisation à la sécurité et promouvoir une culture de sécurité au sein des institutions, organisations et communautés.

2. Soutenir le développement et l'amélioration des capacités de cybersécurité en Europe.

3. Améliorer la coopération et la coordination entre les États européens, ainsi qu'entre les différentes institutions et organisations dans le domaine de la cybersécurité.

4. Fournir un soutien et une assistance aux institutions et organisations pour faire face aux cybermenaces et aux incidents de sécurité.

5. Développer les normes, pratiques et outils de sécurité nécessaires pour assurer la cybersécurité en Europe.

6. Accroître la capacité à traiter les nouvelles cybermenaces émergentes.

7. Évaluer et améliorer la cybersécurité dans les secteurs vitaux et gouvernementaux, les services numériques et les marchés numériques.

8. Fournir un soutien et une assistance en matière de cybersécurité aux citoyens et aux utilisateurs.

9. Promouvoir la recherche et le développement dans le domaine de la cybersécurité et appliquer des technologies modernes pour garantir la cybersécurité.

10. Renforcer la transparence et la responsabilité en matière de cybersécurité en fournissant des informations, des orientations, des conseils et des analyses de sécurité complètes aux institutions, organisations et communautés.

3- Rôle des conventions régionales dans la lutte contre la cybercriminalité

En plus des efforts internationaux menés par les organisations internationales susmentionnées, il existe d'autres initiatives internationales menées par des organisations de caractère régional, dont l'importance n'est pas moindre que celle des efforts réalisés par les organisations et institutions internationales multilatérales (comprenant des pays de plusieurs régions géographiques).

Le rôle des organisations régionales dans la lutte contre les cybercrimes est devenu évident à travers les conventions qu'elles ont mises en place dans ce domaine. Le Conseil de l'Europe s'est réuni à la capitale hongroise Budapest le 23/11/2001, pour discuter de ce phénomène criminel émergent et convenir de clauses claires pour combattre les crimes informatiques. Cela a abouti à la Convention internationale européenne sur la cybercriminalité (criminalité sur internet), qui est devenue la base juridique mondiale pour la lutte contre la cybercriminalité. De même, la Ligue des États arabes a pris des

initiatives à cet égard, en publiant en 2010 la Convention arabe sur la lutte contre les crimes informatiques.

Par conséquent, les paragraphes suivants traiteront de la Convention de Budapest (la convention sur la cybercriminalité), puis de la Convention arabe sur la lutte contre les crimes informatiques.

A- Convention de Budapest sur la cybercriminalité

La Convention de Budapest sur la cybercriminalité a été adoptée après plus de cinq ans de travaux et de réunions du Comité européen pour les problèmes criminels. Cette convention, résultat de nombreuses tentatives depuis les années 1980, a pris sa forme finale le 23 novembre 2001 à Budapest. Elle reflète la volonté du Conseil de l'Europe de lutter contre l'utilisation illégale des ordinateurs et des réseaux d'information. La convention est le fruit de longues consultations entre les gouvernements, les forces de police et le secteur informatique, et a été formulée au sein du Conseil de l'Europe avec l'aide de plusieurs pays, dont les États-Unis. Depuis son entrée en vigueur le 1er juillet 2004, elle constitue une pierre angulaire pour les États membres du Conseil de l'Union européenne (Suleiman Abdel Halim, Op. cit. p. 34).

La convention a été la première à établir une liste de crimes que les États parties doivent incriminer dans leurs législations nationales. Elle est la première convention à lutter contre les crimes sur Internet, couvrant un large éventail de crimes tels que le terrorisme, la fraude par carte de crédit, et la prostitution infantile. La convention vise à harmoniser les nouvelles lois dans de nombreux pays.

En raison de l'importance de la convention en question, trente pays européens, compris quatre pays non membres du Conseil de l'Europe, l'ont signée, à savoir le Canada, le Japon, l'Afrique du Sud et les États-Unis. . En effet, cette convention est ouverte aux pays membres du Conseil de l'Europe ainsi qu'à des pays extérieurs à ce dernier. De nombreux États non membres du Conseil de l'Europe y ont adhéré, et en juin 2023, le nombre total de pays signataires s'élevait à 89, dont la Tunisie au cours du second semestre de cette même année. Bien que de nombreux pays non européens aient rejoint la convention, l'Égypte n'a ni signé ni ratifié cette convention à ce jour. La convention comprend quatre parties: la première traite des termes utilisés, la deuxième aborde les mesures à prendre au niveau national, la troisième concerne la juridiction et la coopération internationale, et la quatrième présente les dispositions finales (Ahmed, 2011, pp. 12).

Nous présentons ci-dessous un bref aperçu de chaque partie de la convention.

A.1 Définitions et termes utilisés dans la Convention

L'article premier de la convention présente les définitions fondamentales de plusieurs termes clés, à savoir le système informatique, le prestataire de services, les données informatiques, et les données relatives au trafic, comme suit :

a - Système informatique :

Désigne tout appareil, seul ou avec d'autres appareils connectés ou associés, qui peuvent, seuls ou avec d'autres éléments, exécuter un programme spécifique pour

effectuer un traitement automatique de données.

b – Données informatiques :

Désigne toute représentation de faits, d'informations ou de concepts sous quelque forme que ce soit, préparée pour un traitement automatique, y compris les programmes de la même nature permettant à l'ordinateur d'accomplir une tâche.

c – Prestataire de services :

Fait référence à :

1. Toute entité, publique ou privée, offrant à ses utilisateurs la possibilité de se connecter via un système informatique.

2. Toute autre entité traitant ou stockant des données informatiques en remplacement du service de connexion ou pour le compte des utilisateurs de ce service.

d – Données relatives au trafic :

Il s'agit de l'ensemble des données traitant une communication, qui transitent par un système informatique ou sont générées par celui-ci, constituant un élément de la chaîne de communication. Cela inclut les informations sur la source de la communication, le lieu de destination, l'itinéraire, l'heure, la date, le volume, la durée de la communication, ou le type de service utilisé.

A.2 Les mesures à prendre au niveau national

Dans la deuxième partie, la Convention aborde les mesures à prendre au niveau national, divisées en deux parties : la première concerne le droit pénal substantiel, et la deuxième concerne le droit procédural. Notre étude se concentrera uniquement sur la première partie, relative aux aspects substantiels des infractions informatiques, mentionnés dans les articles 2 à 13 de la Convention.

Premièrement : Les infractions contre la confidentialité, l'intégrité et la disponibilité des données et des systèmes informatiques :

Ces infractions se divisent en cinq catégories que nous allons examiner ci-dessous :

1. Infraction d'accès illégal

L'article 2 de la convention stipule que chaque partie doit adopter les mesures législatives ou autres nécessaires pour criminaliser, conformément à son droit interne, l'accès intentionnel et non autorisé à tout ou partie d'un système informatique. Cette infraction peut être conditionnée à la violation des mesures de sécurité avec l'intention d'obtenir des données ou dans tout autre but criminel, ou bien lorsque l'infraction est commise via un ordinateur relié à distance à un autre ordinateur.

Ainsi, toute intrusion non autorisée, tout piratage ou toute entrée illégale dans le système d'information est considérée illégale en soi comme principe général.

2. Infraction d'interception illégale

L'article 3 de la convention exige que chaque partie adopte les mesures législatives ou toutes autres qu'elLe juge nécessaires pour criminaliser, conformément à son droit interne, l'interception intentionnelle et non autorisée, par des moyens techniques, de

transmissions de données informatiques non publiques au lieu d'arrivée, à l'origine, ou au sein du système d'information, y compris les émissions électromagnétiques provenant d'un ordinateur transportant ces données. Cette infraction peut aussi être conditionnée par l'intention de commettre une fraude ou lorsqu'elle est commise via un ordinateur connecté à distance à un autre ordinateur (Rapport final d'activité», «Projet d'exposé des motifs» , 2001).

3. Infraction d'atteinte à l'intégrité des données

L'article 4 de la convention incrimine toute atteinte intentionnelle et non autorisée à l'intégrité des données informatiques entraînant des dommages, des suppressions, des désactivations, des destructions ou des altérations des données. Chaque partie peut aussi exiger que ces actes, prévus au premier paragraphe, entraînent des dommages significatifs pour être considérés comme une infraction.

La note explicative précise que ce texte vise à protéger les données et programmes informatiques contre les dommages intentionnels, similaires à la protection accordée aux biens matériels contre les dommages causés intentionnellement. Le bon fonctionnement signifie l'intégrité des données ou des programmes, ou la bonne utilisation des données informatiques enregistrées.

4. Infraction d'atteinte à l'intégrité du système

L'article 5 de la convention incrimine toute atteinte grave intentionnelle et non autorisée à la fonctionnalité d'un système informatique par l'introduction, la transmission, le dommage, la suppression, la désactivation, la destruction ou l'altération des données.

La note explicative fait référence à la recommandation n° 89 qui désigne cette infraction comme sabotage de système informatique, visant à pénaliser toute obstruction intentionnelle à l'utilisation légitime des systèmes informatiques, y compris les systèmes de communication par l'utilisation ou l'altération des données informatiques.

Les intérêts juridiques protégés sont ceux des opérateurs et des utilisateurs de systèmes informatiques ou de communication, pour assurer le bon fonctionnement de ces dispositifs. Le texte est rédigé de manière neutre afin de protéger toutes les fonctions concernées, et le terme «obstruction» se réfère aux actions qui compromettent le bon fonctionnement d'un système informatique, cette obstruction devant résulter de l'introduction, du dommage, de la transmission, de la destruction, de la suppression ou de l'altération des données informatiques.

5. Infraction de mauvaise utilisation des dispositifs informatiques :

L'article 2 de la convention stipule que :

- Chaque partie doit adopter les mesures législatives ou autres nécessaires pour criminaliser, conformément à son droit interne, les actes suivants s'ils sont commis intentionnellement et sans droit :

- La production, la vente, l'acquisition en vue de l'utilisation, l'importation, la diffusion ou toute autre forme de mise à disposition de :

– Tout dispositif contenant un programme informatique principalement conçu pour commettre l'une des infractions prévues aux articles 2 à 5 susmentionnés.

– Un mot de passe, un code d'accès ou toute donnée similaire permettant d'accéder à tout ou partie d'un système informatique avec l'intention de l'utiliser pour commettre l'une des infractions mentionnées aux articles 2 à 5.

– La possession de l'un des éléments mentionnés aux points 1–(1) et 1–(2) de l'article 6 de la Convention de Budapest ((5)) avec l'intention de l'utiliser pour commettre l'une des infractions prévues aux articles 2 à 5.

– Chaque partie peut, dans son droit interne, exiger la présence de certains de ces éléments pour établir la responsabilité pénale.

– Cet article ne doit pas être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'acquisition en vue de l'utilisation, l'importation, la diffusion ou la mise à disposition mentionnées au premier paragraphe de cet article ne visent pas à commettre une infraction selon les articles 2 à 5 de cette convention, par exemple dans le cadre de tests autorisés ou de la protection d'un système informatique.

– Chaque partie peut se réserver le droit d'appliquer le premier paragraphe de cet article, à condition que cette réserve n'inclue pas la vente, la distribution ou la mise à disposition de tout élément mentionné aux points 1–(1) et 1–(2).

Puisque la commission de ces infractions nécessite souvent la possession de moyens d'accès comme des outils de piratage ou d'autres dispositifs similaires, il existe une forte motivation pour les acquérir à des fins criminelles, ce qui peut finalement conduire à la création d'un marché noir pour la production et la distribution de tels outils.

Deuxièmement : Les infractions informatiques liées aux ordinateurs

Ces infractions comprennent deux types que nous allons détailler ci–dessous :

1. Infraction de falsification informatique

L'article 7 de la convention criminalise l'introduction, la destruction, la suppression ou l'altération intentionnelle et non autorisée de données informatiques, entraînant la création de données incorrectes, destinées à être prises en compte comme si elles étaient correctes lorsqu'elles sont utilisées à des fins légales, qu'elles soient facilement lisibles et claires ou non. Chaque partie peut, dans son droit interne, exiger l'intention de frauder ou toute autre intention criminelle similaire pour établir la responsabilité pénale.

La note explicative précise que cette disposition vise à créer une infraction parallèle à celle de la falsification de documents papier, comblant ainsi les lacunes du droit pénal concernant la falsification traditionnelle, laquelle exige une lisibilité visuelle aisée

(5) L'article 6 de la Convention de Budapest sur la cybercriminalité, intitulé « Abus des dispositifs », stipule que chaque État partie doit adopter des mesures législatives et autres nécessaires pour incriminer certains actes commis intentionnellement et illégalement. Ces actes incluent la production, la vente, l'achat, l'importation, la distribution ou la mise à disposition de dispositifs (y compris des logiciels informatiques) conçus ou adaptés pour commettre des infractions énumérées dans les articles 2 à 5, ainsi que l'acquisition de mots de passe ou de codes d'accès pour les mêmes fins.

des déclarations contenues dans le document, critère non applicable aux données enregistrées sur un support électronique.

2. Infraction de fraude informatique

L'article 8 de la convention criminalise la causation intentionnelle de dommages financiers à autrui par :

a. L'introduction, la destruction, la suppression ou l'altération de données informatiques.

b. Toute forme d'atteinte à la fonction d'un ordinateur dans l'intention de frauder ou avec toute autre intention criminelle similaire afin d'obtenir un avantage économique pour soi-même ou pour autrui sans droit.

La note explicative souligne qu'avec la révolution technologique, les possibilités de commettre des infractions économiques, en particulier la fraude et l'escroquerie avec des cartes de crédit, ont considérablement augmenté. Les actifs représentés ou échangés via des systèmes informatiques, tels que l'argent électronique ou les dépôts, sont devenus des cibles de manipulation, de la même manière que les formes traditionnelles de propriété.

Ces infractions se caractérisent principalement par des manipulations des entrées du système, c'est-à-dire l'alimentation de l'ordinateur avec des données incorrectes, des manipulations de logiciels, ou d'autres interventions dans le traitement des données. Cette disposition vise à imposer une sanction pénale pour toute manipulation arbitraire dans le cadre du traitement automatisé des données, conduisant à un transfert illégal de propriété.

Troisièmement : Infractions liées au contenu

Cette partie couvre les infractions liées au contenu, c'est-à-dire la production ou la diffusion illégale de matériel pornographique impliquant des enfants via les systèmes informatiques, représentant l'une des formes les plus graves d'infractions, récemment apparues.

Il est à noter qu'au cours de l'élaboration de l'ébauche de la convention en question, la commission a discuté de la possibilité d'inclure d'autres infractions liées au contenu, telles que la diffusion de propagande raciste via les systèmes informatiques. Cependant, la commission n'a pas pu parvenir à un consensus ou à un accord collectif sur la criminalisation de ce comportement.

Bien que l'idée de considérer cette diffusion comme une infraction pénale ait bénéficié d'un large soutien, certaines délégations ont exprimé des réserves importantes, invoquant le principe de la liberté d'expression.

Compte tenu de la complexité de cette question, la commission a décidé de charger le Comité européen pour les problèmes criminels de proposer la préparation d'un protocole additionnel à intégrer à la présente convention.

Nous présentons ci-dessous les dispositions de l'article 9 relatives aux infractions liées à la pornographie enfantine, qui stipulent que :

1- Chaque partie doit adopter les mesures législatives ou autres nécessaires pour

criminaliser, selon son droit interne, les comportements suivants s'ils sont commis intentionnellement et sans droit :

a- Produire du matériel pornographique impliquant des enfants en vue de sa diffusion via un système informatique.

b- Offrir ou rendre disponible du matériel pornographique impliquant des enfants via un système informatique.

c- Diffuser ou transmettre du matériel pornographique impliquant des enfants via un système informatique.

d- Procurer ou fournir à autrui du matériel pornographique impliquant des enfants via un système informatique.

e- Posséder du matériel pornographique impliquant des enfants dans un système informatique ou sur tout support de stockage de données informatiques.

2- Aux fins du paragraphe 1 ci-dessus, le matériel pornographique impliquant des enfants comprend tout matériel pornographique représentant visuellement :

a. Un mineur se livrant à un comportement sexuel explicite.

b. Une personne paraissant être un mineur se livrant à un comportement sexuel.

c. Des images réalistes représentant un mineur se livrant à un comportement sexuel explicite.

3- Aux fins du paragraphe 2 ci-dessus, le terme «mineur» désigne toute personne de moins de 18 ans. Cependant, chaque partie peut fixer une limite d'âge inférieure, à condition qu'elle ne soit pas inférieure à 16 ans.

4-Chaque partie a le droit de ne pas appliquer, en tout ou en partie, les paragraphes [1-(d)], [1-(e)] et [2-(b)] et [2-(c)].

Quatrièmement : Les infractions liées aux atteintes portées à la propriété intellectuelle et aux droits voisins(6) :

Le quatrième chapitre définit les infractions relatives aux atteintes portées à la propriété intellectuelle et aux droits voisins ou connexes. La convention a inclus ce type d'infractions car les violations de la propriété intellectuelle sont l'une des formes les plus courantes de criminalité informatique. Avec l'augmentation de ces violations, le monde entier s'inquiète de plus en plus. Ci-dessous, nous exposons les dispositions de l'article 10 relatives aux infractions liées aux atteintes portées à la propriété intellectuelle et aux droits voisins.

L'article 10 stipule les infractions liées aux atteintes portées à la propriété intellectuelle et aux droits voisins :

(6) Les droits voisins (Related rights) sont les droits accordés à certaines catégories de personnes et d'entités qui contribuent à la diffusion ou à l'exécution des œuvres créatives, tels que les artistes interprètes, les producteurs d'enregistrements sonores et les organismes de radiodiffusion. Ces droits sont considérés comme «voisins» ou «parallèles» aux droits d'auteur, car ils concernent les œuvres créatives, mais ne sont pas les droits principaux liés à la création de l'œuvre elle-même.

1. Chaque partie doit adopter les mesures législatives ou autres qu'elLe juge nécessaires pour criminaliser, conformément à son droit interne, les violations de la propriété intellectuelle définies dans la législation de cette partie, conformément aux obligations souscrites en vertu de la Convention universelle sur le droit d'auteur signée à Paris le 24 juillet 1971, de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de la Convention sur les aspects commerciaux des droits de propriété intellectuelle, et la Convention de l'Organisation mondiale de la propriété intellectuelle (OMPI), à l'exception de tout droit moral accordé par cette convention – si de tels actes sont commis intentionnellement, à une échelle commerciale, et par le biais d'un système informatique.

2. Chaque partie doit adopter les mesures législatives ou autres qu'elLe juge nécessaires pour criminaliser, conformément à son droit interne, les violations des droits voisins définies dans la législation de cette partie, conformément aux obligations souscrites en vertu de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion conclue à Rome (Convention de Rome).

3. Chaque partie peut, dans des circonstances extrêmement limitées, se réserver le droit de ne pas appliquer la responsabilité pénale pour les paragraphes premier et deuxième de cet article, à condition qu'il existe d'autres moyens efficaces et disponibles, et que cette réserve ne porte pas atteinte aux obligations internationales imposées à cette partie dans l'application des conventions internationales mentionnées aux paragraphes premier et deuxième de cet article.

La note explicative souligne que les violations des droits de propriété intellectuelle, en particulier le droit d'auteur, sont parmi les infractions les plus répandues sur Internet, ce qui intéresse à la fois les détenteurs de droits d'auteur et les spécialistes des réseaux informatiques.

Il convient de noter que la facilité avec laquelle des copies non autorisées peuvent être réalisées grâce à la technologie numérique, et l'ampleur avec laquelle elles peuvent être reproduites et distribuées via les réseaux électroniques, ont imposé la nécessité de mettre en place des dispositions incluant des sanctions pénales visant à renforcer la coopération internationale dans ce domaine.

En vertu des principes mentionnés dans cet article, chaque partie est tenue de criminaliser les violations intentionnelles de la propriété intellectuelle et des droits connexes, désignés sous le titre de droits voisins, si ces violations sont commises par le biais d'un système informatique, à une échelle commerciale (Rapport explicatif de la Convention sur la cybercriminalité,2001).

Cinquièmement : Responsabilité des personnes morales :

L'article douze de la convention stipule que :

1. Chaque partie doit adopter des mesures législatives, ou toute autre mesure jugée nécessaire, pour considérer les personnes morales comme responsables des infractions mentionnées dans la présente convention, s'ils sont commis à leur bénéfice, par toute personne physique agissant individuellement ou en tant que membre d'une institution

de la personne morale, et exerçant un pouvoir de direction selon les règles suivantes :

a. Pouvoir de représenter la personne morale.

b. Pouvoir de prendre des décisions au nom de la personne morale.

c. Pouvoir d'exercer le contrôle au sein de la personne morale.

2. Outre les cas prévus au paragraphe 1, chaque partie doit prendre les mesures nécessaires pour s'assurer que la personne morale puisse être tenue responsable si la surveillance ou le contrôle par une personne physique mentionnée au paragraphe 1 font défaut, permettant ainsi la commission des infractions mentionnées au paragraphe 1 pour le compte de la personne morale par une personne physique agissant sous son autorité.

3. Conformément aux principes juridiques de la partie, la responsabilité de la personne morale peut être pénale, civile ou administrative.

4. Cette responsabilité doit être sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

La convention ayant établi la responsabilité pénale de la personne morale, conformément à la tendance juridique actuelle qui reconnaît la responsabilité des personnes morales, il convient de remplir quatre conditions pour établir la responsabilité de la personne morale : l'infraction commise doit être l'une des infractions mentionnées dans la convention, l'infraction doit avoir été commise pour le bénéfice de la personne morale, la personne ayant commis l'infraction doit exercer un pouvoir de direction, incluant les partenaires, et le terme « personne exerçant un pouvoir de direction » désigne une personne physique occupant une position élevée dans l'institution, comme un directeur, et la personne exerçant un pouvoir de direction doit agir en vertu d'un pouvoir tel que la prise de décisions ou l'exercice du contrôle, prouvant que la personne physique mentionnée a agi dans le cadre de ses pouvoirs, engageant ainsi la responsabilité de la personne morale.

A.3 Dispositions relatives à la cybercriminalité transfrontalière

Premièrement : La coopération internationale

L'article 23 de la convention stipule les dispositions générales relatives à la coopération internationale. Le texte de cet article précise que les parties doivent coopérer entre elles conformément aux dispositions de ce chapitre en appliquant les principes internationaux de coopération dans les affaires pénales, ainsi que les conventions basées sur des législations similaires ou équivalentes et les lois locales, dans toute la mesure du possible, aux fins de recherche, d'enquête, ou de procédures pénales relatives aux infractions pénales liées aux systèmes et données informatiques, ou pour recueillir des preuves électroniques d'une infraction pénale (La référence du rapport explicatif à la Convention, pp. 44-46).

La note explicative de cette convention indique que cet article établit trois principes généraux régissant la coopération internationale :

Premier principe : Cet article oblige les parties à coopérer entre elles aussi largement

que possible. Ce principe impose aux parties de s'entraider largement et de minimiser autant que possible les obstacles susceptibles de ralentir le flux rapide des informations et des preuves au niveau international.

Deuxième principe : L'article définit l'étendue de l'obligation de coopération, stipulant que cette coopération doit couvrir tous les infractions pénales liées aux systèmes et données informatiques, tels que mentionnées à l'article 14, paragraphe 2, points a et b de la convention.

Troisième principe : Cette coopération doit être mise en œuvre conformément aux dispositions de ce chapitre, en appliquant les principes internationaux de coopération dans les affaires pénales, ainsi que les conventions basées sur des législations similaires ou équivalentes et la loi locale.

Cette dernière clause relative à la loi locale crée un principe général selon lequel les conditions du troisième chapitre n'annulent pas les conditions des documents internationaux relatifs à l'entraide judiciaire et aux conventions d'extradition équivalentes entre les parties concernant ces documents, et détaillées davantage dans l'analyse de l'article 27 ci-dessous, ou les conditions de la loi locale concernant la coopération internationale.

Ce principe est clairement soutenu par les articles (24) relatifs à l'extradition, (25) relatifs aux principes généraux de l'entraide mutuelle, (26) relatifs aux informations automatiques, (27) relatifs aux procédures spéciales de demandes d'entraide en l'absence de conventions internationales applicables, (28) relatifs à la confidentialité et aux restrictions d'utilisation, (31) relatifs à l'entraide pour l'accès aux données informatiques stockées sur un ordinateur, (33) relatifs à l'entraide pour la collecte en temps réel des données de trafic, et (34) relatifs à l'entraide pour l'interception des données de contenu.

Deuxièmement : Extradition des criminels :

L'article 24 de la convention stipule que :

1. Cet article s'applique à l'échange de criminels entre les parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente convention, à condition qu'elles soient passibles, en vertu de la loi des deux parties, d'une peine privative de liberté d'au moins un an, ou d'une peine plus sévère.

Si l'application d'une peine minimale différente est nécessaire, sur la base d'un accord d'extradition en vigueur entre deux parties ou plus, y compris la Convention européenne d'extradition, ou tout autre accord prévu dans des législations similaires ou analogues, la peine prévue dans cette convention s'applique.

2. Les infractions pénales décrites au paragraphe 1 du présent article doivent être considérées comme des infractions justifiant l'extradition dans tout accord conclu entre ou par les parties. Les parties doivent s'engager à inclure ces infractions comme des infractions justifiant l'extradition dans tout accord d'extradition conclu entre elles ou par elles.

3. Si une partie exige que l'extradition soit conditionnée par l'existence d'un accord

pour recevoir une demande d'extradition d'une autre partie avec laquelle elle n'a pas d'accord d'extradition, cette convention (Convention de Budapest) peut être considérée comme une base légale pour l'extradition de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4. Les parties qui n'exigent pas que l'extradition soit conditionnée par l'existence d'un accord reconnaîtront que les infractions pénales mentionnées au paragraphe 1 du présent article sont des infractions justifiant l'extradition entre elles.

5. L'extradition est soumise aux conditions prévues par la législation interne de la partie requise ou par les accords d'extradition en vigueur, y compris les motifs pour lesquels la partie requise peut refuser l'extradition.

6. Si l'extradition est refusée pour une infraction pénale mentionnée au paragraphe 1 du présent article uniquement en raison de la nationalité de la personne demandée, ou parce que la partie requise considère qu'elle a compétence sur cette infraction, la partie requise soumet l'affaire, à la demande de la partie requérante, à ses autorités compétentes pour enquête, en tenant compte du délai approprié pour envoyer le résultat final de l'affaire à la partie requérante. Ces autorités doivent prendre leur décision et mener leurs enquêtes et procédures pénales de la même manière que pour toute autre infraction de même nature dans la législation de cette partie.

7. Chaque partie doit informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature, de la ratification, de l'acceptation ou de l'approbation de l'adhésion à la présente convention , du nom et de l'adresse de chaque autorité responsable de l'envoi ou de la réception des demandes d'extradition, ou de l'arrestation provisoire en l'absence d'un accord particulier à cet effet.

8. Le Secrétaire Général du Conseil de l'Europe doit créer et tenir à jour un registre des autorités concernées par les parties. Chaque partie doit s'assurer en permanence de l'exactitude des informations figurant dans ce registre.

Il ressort de l'examen du paragraphe 1 de l'article (24) susmentionné que l'obligation d'extradition ne s'applique qu'aux infractions définies conformément aux articles (2) à (11) de la convention, qui sont punissables dans la législation des deux parties par une peine privative de liberté d'une durée maximale d'au moins un an, ou par une peine plus sévère. L'État requis peut refuser la demande d'extradition sur la base des motifs prévus par sa législation, qu'il soit membre de la convention ou non, et selon les principes et procédures prévus par la convention, à condition que le principe de double incrimination soit respecté. Le refus doit être accompagné d'une note expliquant les raisons et les fondements sur lesquels repose cette décision.

Troisièmement : Assistance judiciaire mutuelle :

Nous aborderons ici deux articles de la convention, à savoir l'article 25 portant sur les dispositions générales régissant l'entraide judiciaire mutuelle, et l'article 26 sur les informations automatiques, c'est-à-dire celles qui sont fournies spontanément.

L'article 25 de la convention stipule que :

1. Chaque partie doit fournir aux autres parties une assistance judiciaire mutuelle dans

toute la mesure possible aux fins d'enquêtes ou de procédures concernant des infractions pénales liées aux systèmes et données informatiques ou aux fins de la collecte de preuves électroniques des infractions pénales.

2. Chaque partie doit également adopter les mesures législatives et autres qu'elLe juge nécessaires pour remplir les obligations énoncées aux articles (27 à 35).

3. En cas d'urgence, chaque partie peut présenter une demande d'assistance mutuelle ou des communications par des moyens de communication rapides tels que le fax ou le courrier électronique, ces moyens offrant des garanties suffisantes de sécurité et d'authentification (y compris le chiffrement si nécessaire), avec une confirmation officielle ultérieure lorsque cela est requis par l'État destinataire de la demande. L'État destinataire de la demande doit accepter et répondre à la demande par tout moyen de communication rapide.

4. Sauf disposition contraire expresse dans les articles du présent chapitre, l'entraide mutuelle est soumise aux conditions définies par la législation interne de la partie destinataire de la demande ou par les accords d'assistance mutuelle applicables, y compris les motifs pour lesquels la partie destinataire peut refuser la coopération. La partie destinataire ne doit pas exercer son droit de refuser l'entraide judiciaire mutuelle pour les infractions énoncées aux articles (2 à 11) de la convention, uniquement si la demande est liée à une infraction de nature financière.

5. Lorsqu'il est permis, conformément aux dispositions du présent chapitre, à la partie destinataire de la demande de soumettre l'entraide mutuelle à l'existence d'une double incrimination (conjointe), cette condition est considérée comme remplie si le comportement constitutif de l'infraction dans la demande présentée à la partie requise est qualifié d'infraction pénale en vertu de sa législation interne, que cette législation interne le classe ou non dans la même catégorie d'infractions et qu'il soit incriminé ou non dans les mêmes termes que la législation de la partie requise.

L'obligation d'assistance doit être assurée dans toute la mesure du possible, de sorte que l'entraide mutuelle doit être, en principe, exhaustive ou étendue, et les obstacles doivent être réduits au minimum. De même, l'obligation de coopération prévue à l'article (23) s'applique en principe à la fois aux infractions pénales liées aux systèmes et données informatiques et à la collecte de preuves électroniques liées à une infraction pénale. Il est devenu nécessaire d'imposer l'obligation de coopération pour cette large catégorie d'infractions en raison de la nécessité de disposer de mécanismes de coopération internationale dans ces deux domaines. Cependant, les articles (34) et (35) permettent aux parties de modifier la portée de ces mesures.

L'article (26), paragraphe (1), de la convention stipule qu'une partie peut, dans les limites de sa législation nationale et sans demande préalable, envoyer à une autre partie des informations obtenues dans le cadre de ses enquêtes, si elle estime que ces informations peuvent aider la partie destinataire à clarifier ou à mener des investigations ou enquêtes relatives à des infractions pénales visées par ce traité, ou lorsque ces infractions pourraient donner lieu à une demande d'assistance par cette partie conformément à ce chapitre.

Il convient de noter que l'article (25) découle des conditions énoncées dans des conventions antérieures du Conseil de l'Europe, comme l'article (10) de la convention relative au blanchiment d'argent. En effet, il arrive souvent qu'une partie dispose d'informations importantes et pense que les communiquer pourrait être bénéfique pour des recherches, des enquêtes ou des procédures en cours, dont la partie concernée n'est pas encore informée. Dans de tels cas, aucune demande d'assistance n'est déposée, ce qui permet au premier paragraphe de l'article (26) d'autoriser l'État détenant l'information à contacter directement l'autre État concerné sans attendre de recevoir une demande préalable.

Il est utile d'inclure cette disposition, car, selon la législation nationale de certains pays, une telle clarification positive est nécessaire pour permettre l'acceptation de l'assistance mutuelle en l'absence d'une demande. Une partie n'est pas tenue de fournir les informations à l'autre partie de manière automatique, mais elle dispose de la liberté d'agir en fonction des circonstances particulières de l'affaire en question. De plus, la divulgation spontanée des informations n'empêche pas la partie qui les envoie de poursuivre ses propres recherches ou de lancer des enquêtes sur les faits révélés. Le paragraphe (2) de l'article (26) prévoit qu'il peut arriver, dans certains cas, que la partie détenant des informations sensibles ne les envoie que sous condition de confidentialité ou à condition qu'elles soient utilisées selon certaines restrictions. Ainsi, la confidentialité devient un facteur important dans les affaires où les intérêts de l'État fournissant les informations pourraient être compromis par la divulgation de ces informations.

Quatrièmement : Création d'un Réseau d'Urgence Permanent pour Activer l'Entraide Mutuelle

Nous traiterons ici une seule disposition de la convention, à savoir l'article 35, concernant la création d'un réseau d'urgence permanent pour activer l'entraide mutuelle, appelé le réseau 24/7. Ce réseau fonctionne 24 heures sur 24, 7 jours sur 7, afin de garantir la fourniture d'une assistance immédiate pour les enquêtes relatives aux infractions pénales liées aux systèmes et données informatiques, ou pour collecter des preuves électroniques concernant une infraction pénale. Cette assistance doit inclure la facilitation ou l'application pratique directe des procédures suivantes (Rapport explicatif de la Convention p. 185) :

- Fourniture de conseils techniques.

- Conservation des données conformément aux articles (29 et 30).

- Collecte de preuves et fourniture d'informations à caractère juridique, ainsi que localisation des suspects.

En outre, l'article stipule les points suivants :

1. Le point de contact d'une partie doit être capable de communiquer rapidement avec le point de contact d'une autre partie.

2. Si le point de contact désigné par une partie ne dépend pas de l'autorité ou des autorités de cette partie responsables de l'entraide internationale ou de l'extradition, il doit être capable de coopérer rapidement avec cette autorité ou ces autorités.

3. Chaque partie doit disposer d'un personnel formé et équipé pour faciliter le fonctionnement du réseau.

La création de ce réseau est l'une des mesures les plus importantes prévues par cette convention, car il garantit non seulement les moyens les plus efficaces pour faire face aux problèmes de la criminalité informatique, mais aussi pour surmonter les défis majeurs posés par l'ère de l'information aux autorités chargées de l'application de la loi.

Le point de contact vise soit à faciliter la mise en œuvre rapide des fonctions du réseau, soit à appliquer directement plusieurs mesures, y compris la fourniture de conseils techniques, la conservation des données, la collecte de preuves et la localisation des suspects.

B- Convention Arabe sur la Lutte contre les Crimes de Technologies de l'information

Cette Convention est considérée comme l'une des plus importantes conventions arabes dans le domaine de la lutte contre la criminalité technologique, visant à la prévenir, à enquêter à son sujet et à poursuivre ses auteurs (Batikh, p. 22).

La Convention Arabe sur la Lutte Contre les Crimes de Technologie de l'Information a été adoptée au Caire le 21 décembre 2010, et l'Égypte a accepté d'y adhérer conformément à la décision du Président de la République n° 276 de l'année 2014, en date du 19 août 2014, publiée au Journal Officiel n° 46 du 13 novembre 2014 p. 65. Cette convention vise à renforcer la coopération entre les pays arabes dans le domaine de la lutte contre les crimes de technologie de l'information afin de prévenir les dangers de ces crimes, de préserver la sécurité des pays arabes, leurs intérêts, et la sûreté de leurs sociétés et de leurs citoyens. La convention impose également à chaque État partie de criminaliser les actes énoncés dans les articles du chapitre II de cette convention, intitulé «Incrimination»(Abdel Azim, 2016, p. 166).

Cette convention est l'une des plus importantes conventions arabes dans le domaine de la lutte contre la criminalité technologique, visant à prévenir, enquêter et poursuivre les auteurs de crimes (Battikh, p. 22) tels que les atteintes à l'intégrité des données, les abus des moyens technologiques, la falsification, la fraude, la pornographie, les atteintes à la vie privée, ainsi que les crimes liés au terrorisme commis via les technologies de l'information, comme la diffusion et la promotion des idées de groupes terroristes, le financement des opérations terroristes, et la publication des méthodes de fabrication des explosifs. Elle traite également de la criminalité organisée, comme le blanchiment d'argent, la promotion des drogues, la traite des êtres humains, des organes humains et des armes (Abdel Sadek, 2018, p. 5).

La convention arabe se compose de quarante-trois articles, obligeant les États parties à introduire certaines modifications pour criminaliser les crimes de technologie de l'information, à savoir les actes de piratage, l'interception illégale, les atteintes à l'intégrité des données, les atteintes à la vie privée, les atteintes à la propriété intellectuelle, l'abus des moyens technologiques, la falsification, la fraude, les crimes liés au terrorisme, le blanchiment d'argent, les drogues, la traite des êtres humains, des organes humains, des armes, les atteintes aux valeurs religieuses ou à l'ordre public, les menaces et

l'extorsion, le commerce des antiquités et des œuvres d'art, et l'utilisation illégale des outils de crédit et des documents électroniques (El-Kady, 2011, pp. 50, 70).

Les chapitres III et IV de la convention arabe précisent le champ d'application des dispositions procédurales et de la coopération juridique et judiciaire en matière d'extradition des criminels, d'entraide mutuelle entre les États, ainsi que de l'assistance relative aux autorités d'enquête, tout en insistant sur la nécessité pour chaque État partie d'adopter dans son droit interne des législations et des procédures pour faire face à la cybercriminalité.

Cette convention a eu un impact sur le plan législatif arabe, de nombreux pays arabes ayant suivi cette évolution technologique dans le domaine de l'information et s'efforçant de lutter contre les crimes électroniques qui en résultent, en édictant un certain nombre de législations spécifiques, en s'appuyant et en se basant sur ce qui est prévu par la convention mentionnée.

Deuxième partie

Les Efforts égyptiens dans le Domaine de la Cybersécurité

L'Égypte a connu un mouvement fort dans le domaine de la sécurité de l'information et des réseaux, parallèlement à l'intérêt international croissant pour la sécurité de l'information, à la lumière des violations de la sécurité des infrastructures, des réseaux et des informations dans certains pays de la région à la suite des développements technologiques rapides.

Ainsi, l'Égypte a cherché à construire et à établir un système moderne capable de protéger le cyberespace égyptien («Histoire d'une patrie», 2023, pp. 275, 267, et 277)..

Le Conseil supérieur de la cybersécurité a été créé, ainsi que le Centre égyptien de réponse aux urgences informatiques (CERT). En outre, un centre de réponse aux urgences informatiques pour le secteur financier, affilié à la Banque centrale, a été mis en place. L'Égypte a également publié la stratégie nationale de cybersécurité 2017-2021, suivie par la stratégie nationale de cybersécurité 2023-2027, que nous aborderons ci-dessus.

Nous examinerons les efforts égyptiens dans le domaine de la cybersécurité en six points, comme suit :

1- Le Conseil Supérieur de la Cybersécurité
2- Le Centre Égyptien de Réponse aux Urgences Informatiques (EG-CERT)
3- Le Centre de Réponse aux Urgences Informatiques du Secteur Financier
4- La Stratégie Nationale de Cybersécurité de la République Arabe d'Égypte 2017-2021
5- La Stratégie Nationale de Cybersécurité de la République Arabe d'Égypte 2023-2027
6- Évaluation des efforts égyptiens dans le domaine de la cybersécurité

1- Le Conseil Supérieur de la Cybersécurité

Le Conseil supérieur de la cybersécurité en Égypte a été formé par une décision de l'ancien Premier ministre, l'ingénieur Ibrahim Mahlab, n° 2259 en décembre 2014. Ce conseil vise à protéger les informations et les données des différentes entités, en se concentrant sur les départements d'information et de communication des ministères et des diverses entités, et en s'assurant de la disponibilité des financements nécessaires pour garantir la mise en œuvre du système de cybersécurité, tout en veillant à la clarté du cadre législatif le concernant ([7]).

Le conseil est composé du ministre des Communications et de la Technologie de l'information, qui en est le président, ainsi que de représentants des ministères suivants : Défense, Affaires étrangères, Intérieur, Pétrole et Ressources minérales, Électricité, Santé, Ressources en eau et Irrigation, Approvisionnement, Communications, Service de renseignement général, Banque centrale, et trois membres experts. Ensuite, la décision du Premier ministre n° 1630 de l'année 2016 a défini les compétences et les tâches du conseil, ainsi que ses horaires de travail. La décision du Premier ministre n° 994 de l'année 2017 a attribué au ministre des Communications la responsabilité de fixer les règles de protection et de suivre le conseil dans la mise en œuvre de ses décisions.

Le Conseil supérieur de la cybersécurité est responsable de l'élaboration d'une Stratégie nationale de lutte contre les cybermenaces et les cyberattaques, ainsi que de superviser sa mise en œuvre et sa mise à jour. Ses tâches comprennent également :

- La détermination des infrastructures critiques de communication et d'information dans tous les secteurs de l'État, ainsi que la mise en place de cadres pour leur évaluation et leur suivi sécuritaire dans les différents secteurs.
- L'adoption de cadres, de stratégies et de politiques pour sécuriser les infrastructures critiques de communication et d'information pour tous les secteurs de l'État.
- L'élaboration de plans et de programmes pour développer l'industrie de la cybersécurité et former les cadres nécessaires pour faire face aux défis et aux risques cybernétiques, ainsi que la mise en place d'un cadre pour la recherche scientifique et le développement dans le domaine de la cybersécurité.
- La coopération et la coordination régionales et internationales avec les entités concernées dans le domaine de la cybersécurité et de la protection des infrastructures critiques de communication et d'information, ainsi que la formulation de recommandations pour toute intervention législative nécessaire à la sécurisation.
- L'établissement de normes contraignantes pour toutes les entités, au minimum, pour sécuriser les infrastructures critiques de communication et d'information, et les obliger à élaborer des plans d'urgence.

(7) https://www.escc.gov.eg.

- La mise en place de mécanismes de suivi des risques et de suivi périodique des cyberattaques, et la répartition des rôles au niveau national.
- L'établissement et l'activation de normes et de mécanismes pour déterminer les interdépendances entre les éléments des infrastructures critiques et ceux qui en ont la charge, ainsi que ce qui est en dehors, afin d'éviter les effets en cascade.
- L'approbation des spécifications de cybersécurité standard pour les systèmes dans les différents secteurs, ainsi que l'ajout de critères de qualité cybernétique.
- L'approbation du descriptif d'évaluation de la sécurité pour les opérateurs des infrastructures critiques de communication et d'information.
- La mise en place d'un mécanisme de suivi de la sécurité et de la protection des sites gouvernementaux officiels sur Internet.

Le Conseil suprême de la cybersécurité vise à renforcer la sécurité cybernétique en Égypte et à protéger les infrastructures critiques, tant publiques que privées, contre les cyberattaques potentielles. Le conseil a pris plusieurs décisions réglementaires pour atteindre cet objectif :

a – Création d'un centre de surveillance, d'analyse et de réponse aux incidents cybernétiques, développement des capacités nationales en matière de cybersécurité et renforcement de la coopération internationale dans ce domaine.

b – Publication de la première stratégie nationale de cybersécurité 2017-2021, qui a abordé les risques et les défis cybernétiques, identifié les secteurs vitaux ciblés, analysé les éléments essentiels de la gravité des menaces, puis défini l'objectif stratégique et les piliers de l'approche pour faire face aux dangers, ainsi que le mécanisme de mise en œuvre.

c – Publication de la stratégie nationale de cybersécurité 2023-2027. Cette stratégie vise à fournir un environnement sécurisé pour divers secteurs, unifiant les visions nationales dans le but de créer un cyberespace égyptien sûr et résilient face aux menaces et attaques cybernétiques, tout en favorisant la croissance et la prospérité économique.

d – Organisation et parrainage de nombreuses conférences dans le domaine de la cybersécurité et de la sécurité de l'information pour développer un mécanisme efficace afin de faire face aux menaces. La plus récente de ces conférences est la troisième édition du Caisec 24 sur la sécurité de l'information et la cybersécurité.

2- Le Centre Égyptien de Réponse aux Urgences Informatiques (CERT)

Le ministère des Communications et des Technologies de l'information a adopté l'initiative de créer un conseil supérieur pour la protection des infrastructures de communication et des technologies de l'information. Ce conseil est composé de seize spécialistes qui fournissent un soutien technique 24 heures sur 24 afin de protéger les infrastructures critiques d'information. Depuis 2012, le centre offre son soutien à diverses entités dans les secteurs des technologies de l'information et des communications, des services bancaires et gouvernementaux pour les aider à faire face aux cybermenaces, y compris les attaques par déni de service.

La mission du Centre égyptien de réponse aux urgences Internet et informatiques est de fournir un système d'alerte précoce contre les logiciels malveillants et les cyberattaques de grande envergure visant les infrastructures critiques d'information égyptiennes. Actuellement, le centre travaille à l'expansion et au développement de ses laboratoires dans les quatre principales divisions opérationnelles, avec des plans pour des laboratoires supplémentaires de cybersécurité dans le domaine de la téléphonie mobile et de la cybersécurité des systèmes de contrôle industriels.

Parmi les objectifs du centre figurent également la mise en place d'un cadre législatif approprié pour la cybersécurité, l'élaboration d'un cadre réglementaire pour la création d'un système national de cybersécurité et de centres de réponse aux urgences, et l'établissement de l'infrastructure nécessaire pour garantir la confiance dans les transactions électroniques et la protection de l'identité numérique, comme l'infrastructure à clé publique et les bureaux de crédit en collaboration avec le secteur privé. Le centre recueille également des informations sur les incidents de sécurité, les analyse, coordonne et assure la médiation entre toutes les parties concernées pour résoudre ces incidents.

Le centre se compose de cinq divisions ; à savoir : la gestion des cyberincidents et de la continuité des activités, la surveillance des cyberattaques et l'alerte précoce, l'analyse des vulnérabilités et les tests de pénétration, ainsi que la division de la protection des infrastructures d'information critiques et des plans d'urgence, et la division de la sensibilisation à la cybersécurité et du développement des affaires.

La division de la protection des infrastructures d'information critiques et des plans d'urgence se concentre sur la protection de l'information dans les secteurs critiques de l'État. Elle étudie les besoins de certains secteurs et le niveau d'application des normes et procédures de cybersécurité dans ceux-ci.

La direction de la sensibilisation à la cybersécurité est chargée de renforcer la culture et la sensibilisation à la cybersécurité et à la sécurité de l'information, et de mieux comprendre les risques d'Internet ainsi que les menaces et les attaques électroniques. Cette division vise à sensibiliser les ministères et les institutions gouvernementales ayant des infrastructures critiques en organisant des campagnes de sensibilisation par le biais de cours de sensibilisation, de formations, d'ateliers, de bulletins d'information, de guides, de vidéos éducatives et en participant à des événements scolaires et universitaires ([8]).

3- Le Centre de Réponse aux Urgences Informatiques du Secteur Financier de la Banque Centrale

Le Centre de Réponse aux Urgences Informatiques du Secteur Financier se spécialise dans la gestion des cyberincidents et des urgences Internet au sein du secteur financier et bancaire. Cela inclut la prédiction précoce des incidents de sécurité, leur gestion, l'atténuation de leurs effets et la prévention de leur récurrence. Ce centre s'appuie sur un système technologique innovant de surveillance et de détection des incidents de sécurité, ainsi que sur l'analyse des preuves numériques et des vulnérabilités des cybercrimes dans le secteur financier, afin d'en identifier les causes et d'éviter leur répétition à l'avenir. De plus, il traite les logiciels malveillants et effectue l'ingénierie inverse.

(8) https://egcert.eg/ar

Les tâches et la stratégie du Centre de Réponse aux Urgences Informatiques pour le secteur financier et bancaire sont les suivantes :

1- Assurer une réponse aux urgences de sécurité des technologies de l'information et des communications en soutien aux organismes gouvernementaux, aux infrastructures nationales critiques et au public, à travers des initiatives légalement reconnues, fiables, autorisées et coordonnées au niveau national.

2- Promouvoir la sécurité et la protection en diffusant des informations importantes telles que les alertes précoces, les avertissements et les conseils de sécurité, et en soutenant les meilleures pratiques de sécurité.

3- Soutenir et maintenir ces initiatives en adoptant des technologies et des techniques avancées, en établissant des méthodologies, et en menant des recherches sur l'analyse des menaces et leur atténuation.

Cette stratégie du Centre de réponse aux urgences informatiques pour le secteur financier et bancaire, affilié à la Banque centrale, fonctionne selon la priorité de protection des technologies de l'information et de la communication du pays à travers :

1. L'adoption de toutes les initiatives nécessaires pour le Centre égyptien de réponse aux incidents informatiques « CERT ».

2. La sécurisation des informations sensibles par la coopération régionale avec les partenariats internationaux multilatéraux contre les cybermenaces.

3. La collecte d'informations sur les menaces d'origine internationale et mondiale grâce à ses installations technologiques.

4. La coordination avec l'Union internationale et les centres de réponse aux urgences informatiques accrédités dans d'autres pays ainsi qu'avec toute organisation concernée par la sécurité des technologies de l'information et de la communication.

Le Centre de Réponse aux Urgences Informatiques du Secteur Financier de la Banque Centrale d'Égypte a réussi à obtenir l'accréditation et l'adhésion au Forum Mondial des Équipes de Réponse aux Incidents et Sécurités (FIRST) après avoir rempli toutes les exigences techniques et organisationnelles en un court laps de temps, devenant ainsi le premier centre sectoriel de ce type reconnu internationalement en République Arabe d'Égypte.

Cela s'inscrit dans la stratégie de la Banque Centrale visant à construire un cadre intégré pour renforcer la cybersécurité dans le secteur financier et bancaire, et couronne les efforts du Centre de Réponse aux Urgences Informatiques au cours des quatre dernières années, veillant à suivre et à se conformer aux normes et spécifications de sécurité internationales, ce qui a grandement facilité la réussite de toutes les vérifications et audits effectués par les experts de l'organisation internationale (FIRST) au cours des quatre derniers mois.

L'accréditation et l'adhésion au forum (FIRST) visent à renforcer la coopération et la

coordination pour prévenir et atténuer les cyberincidents, à y répondre rapidement, et à améliorer l'échange d'informations entre les membres et la communauté dans son ensemble, permettant de traiter et de répondre plus efficacement aux cyberincidents. Cela contribue également à maximiser et développer les capacités techniques des centres et équipes de réponse en les informant des pratiques les plus récentes dans ce domaine, ainsi qu'à permettre l'échange instantané d'informations de sécurité sur les cyberincidents, renforçant ainsi leur capacité à gérer et à réduire les attaques et menaces de sécurité, tout en encourageant des réponses rapides et des mesures proactives.

Ce forum facilite également la collaboration et les partenariats stratégiques entre les pays et les institutions mondiales, en renforçant la communication entre les équipes de réponse aux incidents de différents pays grâce à l'échange d'expertise technologique et de renseignement de sécurité. Il permet également aux membres d'assister à des séminaires spécialisés rassemblant des experts en cybersécurité, ainsi qu'à des formations et des conférences pratiques, en plus de participer à la conférence mondiale annuelle sur la réponse aux cyberincidents. De plus, il offre l'accès aux dernières méthodes et publications sur la cybersécurité et les services web, ainsi que la possibilité de rejoindre des forums et discussions en ligne entre les membres.

Tout cela est en accord avec la stratégie de la Banque Centrale Égyptienne visant à renforcer la participation du Centre de Réponse aux Urgences Informatiques du Secteur Financier dans la mise en œuvre efficace de la stratégie nationale de cybersécurité, tout en améliorant la capacité des institutions et entités du pays à répondre rapidement et à coopérer pour prévenir les cyber incidents.

4- La Stratégie Nationale de Cybersécurité de la République Arabe d'Égypte 2017-2021

L'Égypte s'est intéressée au domaine de la cybersécurité dès ses débuts et a cherché à diriger la scène arabe et africaine dans les indicateurs internationaux. Elle a été parmi les premiers pays à chercher à améliorer continuellement et à créer une expérience pionnière au Moyen-Orient.

En matière de gouvernance de la cybersécurité au niveau national, l'Égypte a publié la Stratégie nationale de cybersécurité 2017-2021 en réponse aux tendances mondiales modernes et aux exigences de la constitution égyptienne de 2014. **L'article 31 de la constitution** stipule que la sécurité du cyberespace fait partie intégrante de l'économie nationale et de la sécurité nationale, et que l'État doit prendre les mesures nécessaires pour la préserver, conformément à la loi.

Axes de la Stratégie Nationale de Cybersécurité

1. Objectif de la stratégie

La stratégie nationale de cybersécurité de l'Égypte vise à faire face aux risques cybernétiques, à renforcer la confiance dans l'infrastructure des télécommunications et des informations, ainsi que dans leurs applications et services dans divers secteurs vitaux, et à les sécuriser afin de créer un environnement numérique sûr et fiable pour la société égyptienne dans son ensemble. L'objectif principal est de surveiller et de faire face aux risques, de renforcer la confiance et la sécurité dans les secteurs vitaux et leurs

transactions, et de créer un environnement numérique sûr et fiable.

2. Secteurs vitaux ciblés

La stratégie a identifié plusieurs secteurs ciblés, prioritaires en matière de protection, d'amélioration de l'efficacité et de la préparation, notamment :

a- Les Secteurs des télécommunications et des technologies de l'information : incluant les réseaux de télécommunications filaires et sans fil, les câbles marins et terrestres, les tours de télécommunications, les satellites de communication, et les fournisseurs de services de télécommunications et d'Internet.

b- Le Secteur des services financiers : incluant les réseaux et sites bancaires, les transactions bancaires, les paiements électroniques, la bourse, les sociétés de courtage en valeurs mobilières, et les réseaux de services financiers postaux.

c- Le Secteur de l'énergie : incluant les systèmes et réseaux de contrôle et de production et de distribution de l'électricité, du pétrole et du gaz, les centrales hydroélectriques du Haut barrage, les centrales nucléaires, etc.

d- Le Secteur des transports : incluant les transports terrestres, maritimes, aériens et fluviaux, et tous les systèmes et centres de contrôle des trains, métros, réseaux routiers, et systèmes de contrôle de la navigation aérienne et maritime.

e- Le Secteur de la santé : incluant les services d'ambulance d'urgence, les réseaux de secours et d'ambulance, les banques de sang, les systèmes et réseaux hospitaliers, et les réseaux et sites de fourniture de soins de santé.

f- Secteur des services gouvernementaux : incluant le portail et les sites du gouvernement électronique, les sites des entités et institutions gouvernementales, les bases de données et informations nationales, en particulier la base de données des numéros d'identification nationaux et les réseaux et sites qui y sont connectés.

3. Mécanismes pour faire face aux risques

a. Soutien politique et institutionnel stratégique et exécutif :

Il s'agit de la prise de conscience de la gravité des cybermenaces et la nécessité de les traiter comme une priorité avec le plus grand sérieux. Il est essentiel de se préparer à l'avance, y compris les plans stratégiques et exécutifs, des plans d'urgence, des mécanismes de coordination occasionnels, ainsi que la préparation du personnel et des équipements techniques et logistiques.

b. Cadre législatif :

Établir un cadre législatif adéquat pour la sécurité du cyberespace, la lutte contre les cybercrimes, la protection de la vie privée, la protection de l'identité numérique et la sécurité de l'information. Cela doit se faire en collaboration avec les parties concernées et les experts du secteur privé et des institutions de la société civile, en s'inspirant des expériences et des programmes internationaux pertinents. Il est également nécessaire de former des spécialistes pour l'application de la loi dans les institutions judiciaires et policières.

c. Mise en place d'un cadre réglementaire pour la protection de la sécurité du cyberespace

:

Créer un système national pour sécuriser les infrastructures de communication et de technologie de l'information, ainsi que les systèmes et bases de données nationaux, les portails de services gouvernementaux et les sites internet gouvernementaux.

d. Préparation et activation des équipes de préparation et de réponse aux urgences informatiques et aux réseaux dans les secteurs vitaux au niveau national :

Ces équipes sont responsables de la surveillance de la sécurité des réseaux de communication et d'information nationaux et des ordinateurs qui y sont connectés, et de la gestion de toute menace ou attaque cybernétique. Elles sont également chargées de sensibiliser et de se préparer à faire face à ces menaces.

e. Encourager, soutenir et développer la recherche scientifique et le développement :

Soutenir la collaboration entre les institutions de recherche et les entreprises nationales dans des domaines tels que l'analyse des logiciels malveillants avancés, l'analyse des preuves numériques, la protection et la sécurisation des systèmes de contrôle industriels, le développement d'appareils et de systèmes de sécurité des réseaux, le cryptage et la signature électronique, la protection des infrastructures de communication et de technologie de l'information, la protection des ordinateurs en nuage et des grandes bases de données, ainsi que les technologies d'intelligence artificielle et l'Internet des objets.

f. Développement des ressources humaines et des expertises nécessaires pour activer le système de sécurité cybernétique dans différents secteurs : en collaboration et en partenariat avec le secteur privé, les universités et les institutions de la société civile.

g. Coopération internationale avec les pays amis et les organisations internationales et régionales concernées, échange d'expériences et coordination des positions dans le domaine de la sécurité du cyberespace et de la lutte contre les cybercrimes, car ces crimes ne sont pas limités par les frontières géographiques ou politiques.

h. Élaboration et mise en œuvre de plans et de campagnes de sensibilisation communautaire à l'importance de la sécurité du cyberespace :

Protéger les services électroniques pour les individus et les institutions contre les risques et les défis qu'ils peuvent rencontrer, ainsi que protéger la vie privée et lancer des programmes de protection des enfants et des jeunes sur Internet.

4. Principaux programmes de la Stratégie pour la période 2017-2021:

a. Programme de développement du cadre législatif approprié pour la sécurité du cyberespace, la lutte contre les crimes cybernétiques, et la protection de la vie privée et de l'identité numérique, avec la participation des parties prenantes et des experts des secteurs public, privé, académique et des institutions de la société civile. Ce programme comprend :

- La promulgation de la loi n° 175 de 2018 sur la lutte contre les crimes liés aux technologies de l'information.
- La promulgation de la loi n° 151 de 2020 sur la protection des données personnelles.

L'achèvement du cadre législatif est en cours.

b. Programme de développement d'un système national intégré pour la protection de la sécurité du cyberespace, visant à sécuriser l'infrastructure des communications et des technologies de l'information, à préparer et activer des équipes de réponse aux urgences dans les secteurs vitaux au niveau national («L'Égypte et la Cybersécurité» publié par l'Autorité Générale pour l'information).

c. Programme de protection de l'identité numérique, incluant l'activation du programme de citoyenneté numérique, la mise en place des infrastructures nécessaires pour renforcer la confiance dans les transactions électroniques en général et dans les services gouvernementaux en particulier ainsi que l'activation de la signature électronique.

d. Programme de sensibilisation communautaire aux opportunités et avantages offerts par les services électroniques pour les individus, les institutions et les entités gouvernementales, à l'importance de la cybersécurité pour protéger ces services contre les risques et défis possibles. Ce programme comprend l'organisation de célébrations et de campagnes annuelles à l'échelle nationale, de conférences, de séminaires et d'ateliers spécialisés dans divers secteurs.

e. Programme de soutien à la recherche scientifique et de développement de l'industrie de la cybersécurité qui encourage les programmes et projets de coopération entre les entités de recherche et les entreprises nationales, notamment dans le domaine de l'analyse des logiciels malveillants avancés , l'analyse des preuves numériques, la protection et sécurisation des systèmes de contrôle industriels, le développement de dispositifs et systèmes de sécurisation des systèmes et réseaux, la cryptographie et signature électronique, la protection des infrastructures de télécommunications et des technologies de l'information, la sécurisation de l'informatique en nuage et des grandes bases de données et les technologies de l'intelligence artificielle et de l'internet des objets.

f. Programme de formation des ressources humaines et des compétences nécessaires pour activer le système de cybersécurité dans divers secteurs grâce à la collaboration et partenariat entre les entités gouvernementales, le secteur privé et les universités (Ali, 2020 p. 168).

5- La Stratégie Nationale de Cybersécurité de la République Arabe d'Égypte 2023-2027

Au cours de la première semaine de février 2024, le Conseil suprême de la cybersécurité a annoncé le lancement de la Stratégie Nationale de cybersécurité pour la période 2023-2027. Cette stratégie vise à offrir un environnement sécurisé pour divers secteurs et à unifier la vision nationale afin de créer un cyberespace égyptien sécurisé et résilient face aux cybermenaces et cyberattaques, tout en favorisant la croissance et la prospérité économiques.

Cette stratégie constitue une feuille de route globale comprenant des projets nationaux visant à établir des cadres et des réglementations afin de faire face aux cyberincidents et cybermenaces croissants. Elle cherche également à créer des opportunités sur le marché égyptien en formant des ressources humaines qualifiées et en établissant une industrie

nationale efficace et influente contribuant à l'augmentation du produit intérieur brut de l'État égyptien. Enfin, elle vise à instaurer une culture de cybersécurité pour sensibiliser toutes les catégories de la société, réduisant ainsi les risques de cybercriminalité.

La stratégie comprend six domaines principaux :

1. La mise en place d'un cadre législatif intégré.
2. Le changement de la culture sociétale concernant la cybersécurité.
3. Le renforcement des partenariats nationaux.
4. La construction de cyberdéfenses robustes et résilientes.
5. La promotion de la recherche scientifique, de l'innovation et de la croissance.
6. Le renforcement de la coopération internationale.

La stratégie est divisée en neuf parties, dont les points essentiels sont résumés ci-dessous :

Premièrement : La cybersécurité en Égypte

Cette partie introduit la stratégie en soulignant son importance et en présentant les conclusions de l'analyse SWOT (forces, faiblesses, opportunités, menaces). Elle décrit également les sources utilisées pour élaborer la stratégie, telles que les experts et les universitaires concernés, ainsi que les meilleures pratiques mondiales basées sur l'expérience des pays leaders en cybersécurité.

Deuxièmement : Les fondements et les axes de la stratégie

Cette partie présente la vision, la mission et le cadre législatif constitutionnel de la stratégie. Elle détaille les programmes et les axes de la stratégie, qui comprennent la mise en place d'un cadre législatif intégré, le changement de la culture sociétale concernant la cybersécurité, le renforcement du partenariat national, la construction de cyberdéfenses résilientes, la promotion de la recherche scientifique et de l'innovation, et le renforcement de la coopération internationale.

Troisièmement : La mise en place d'un cadre législatif intégré

Cette partie examine la structure législative actuelle. Le législateur vise à travailler sur deux axes principaux et parallèles : la criminalisation des actes et des auteurs (réalisée par la loi n° 175 de 2018 sur la lutte contre les crimes liés à la technologie de l'information) et l'imposition de normes et de standards (partiellement réalisée par la loi n° 151 de 2020 sur la protection des données personnelles et son règlement d'exécution). Un projet de loi sur la cybersécurité est en cours d'élaboration et devrait être publié prochainement.

Quatrièmement : Le renforcement du partenariat national

Cette partie traite des efforts de gouvernance du système de cybersécurité en Égypte par la coordination entre les entités gouvernementales, les entreprises privées travaillant dans le domaine de la cybersécurité et les institutions éducatives, en conjonction avec la création d'une base de données centrale pour le marché de la cybersécurité afin de faciliter l'échange d'informations et d'expertise dans le domaine de la cybersécurité pour

soutenir le système décisionnel, l'établissement d'accords de coopération bilatérale avec les propriétaires et opérateurs d'unités d'infrastructures critiques assurant l'atteinte des plus hauts niveaux de cybersécurité, et enfin la création d'un fonds pour le développement de l'industrie de la cybersécurité afin de garantir un financement continu nécessaire aux projets de cybersécurité.

Cinquièmement : La Construction de cyberdéfenses robustes et résilientes

Cette partie décrit cinq types de programmes ciblant différents secteurs : les programmes visant l'intégration avec des projets nationaux, ceux visant les infrastructures critiques, ceux destinés aux unités et institutions du secteur privé, ceux établissant des normes et politiques de sécurité, et enfin, ceux améliorant le niveau de service.

Sixièmement : Le renforcement de la coopération internationale

La coopération internationale en cybersécurité est cruciale car la cybercriminalité est une menace transfrontalière et oblige les États et les organisations à se donner la main pour y faire face. Cette partie inclut le développement d'une stratégie égyptienne pour la coopération internationale en cybersécurité, l'établissement des principes et orientations de la cyberdiplomatie égyptienne, en se concentrant sur les axes de leadership et d'innovation, en assurant la prévention, la détection et la réponse aux cybermenaces au fur et à mesure qu'elles surviennent, et la poursuite des auteurs.

Septièmement : Changer la culture sociétale concernant la cybersécurité

Cette partie aborde les divers efforts visant à changer la culture de la société en matière de cybersécurité, ce qui revêt une importance capitale, car de larges secteurs de la population ne connaissent même pas les principes de base de la cybersécurité. Cela conduit à tomber dans les pièges des cyberattaques. Dans le but de changer cette culture, plusieurs activités sont prévues pour cibler différents groupes. Cela comprend la création d'une plateforme de sensibilisation à la cybersécurité de manière simplifiée via des moyens audiovisuels, ainsi que le ciblage des enfants à travers des jeux éducatifs conçus pour transmettre les informations nécessaires de manière simple et attrayante pour les enfants. De plus, les élèves de tous niveaux seront ciblés par l'intégration de programmes éducatifs sur la cybersécurité et par des campagnes de sensibilisation dans les écoles. Il y aura également des campagnes de sensibilisation générale visant divers segments de la société, ainsi que des programmes de formation spécialisés pour préparer des professionnels compétents capables de rivaliser dans le domaine de la cybersécurité.

Huitièmement : Promouvoir la recherche scientifique, l'innovation et la croissance

Cette partie traite des efforts pour encourager la recherche scientifique et renforcer l'innovation et la croissance, des efforts essentiels et indispensables compte tenu de l'évolution continue des technologies, des moyens et des méthodes utilisés dans les cyberattaques. Par conséquent, il est nécessaire de suivre cette évolution en développant des technologies défensives et en créant les technologies nécessaires pour améliorer la sécurité du cyberespace. Les efforts dans le domaine de la promotion de la recherche scientifique incluent le soutien aux incubateurs de petites entreprises et l'encouragement des investissements, tant nationaux qu'étrangers, afin d'augmenter le nombre de

prestataires de services dans le domaine de la cybersécurité. Cela inclut également le renforcement de la disponibilité de personnel qualifié pour fournir des services de cybersécurité, ce qui, à son tour, augmente le nombre de services dans ce domaine. Enfin, il est essentiel de renforcer la coopération avec les universités, les centres de recherche et les entreprises des secteurs public et privé pour soutenir la recherche et le développement.

Neuvièmement : Indicateurs de performance

Cette partie est cruciale car les indicateurs de performance permettent de suivre la mise en œuvre de la stratégie et de mesurer les progrès. Les indicateurs comprennent des mesures quantitatives et qualitatives, y compris des indicateurs globaux, des indicateurs de talents nationaux, des indicateurs de croissance et d'innovation, des indicateurs de partenariat national, et des indicateurs de sensibilisation.

6- Évaluation des efforts égyptiens dans le domaine de la cybersécurité

Tout accord dans la communauté internationale implique toujours un engagement, ce qui a conduit cette communauté à établir des mécanismes pour mesurer la performance, l'engagement et le niveau de progrès sur une certaine période. De nombreux indicateurs internationaux et mondiaux ont ainsi vu le jour, parmi lesquels le Global Cybersecurity Index (GCI), un indice publié par le Centre mondial de cybersécurité de l'Union internationale des télécommunications (UIT), qui analyse la performance des pays sur 80 sous-indicateurs, et le National Cyber Security Index (NCSI), un indice publié par le Centre national de cybersécurité en Estonie (NCSC). Il est donc pertinent de présenter l'évaluation des efforts de cybersécurité de l'État égyptien à la lumière de ces deux indices. L'Égypte a occupé la vingt-troisième place mondiale dans l'indice de mesure de la préparation des pays en matière de cybersécurité publié par l'Union internationale des télécommunications en 2020, tandis qu'elle s'est classée soixantième au niveau mondial dans le National Cyber Security Index de l'Estonie (NCSC) en novembre 2021.

L'Égypte a réalisé des succès dans le domaine de la cybersécurité, résumés comme suit :

- Participation à la Conférence de Budapest sur le cyberespace en octobre 2012 en Hongrie.

- Participation à l'atelier régional arabe sur la protection des enfants en ligne organisé par l'Union internationale des télécommunications sur les aspects juridiques de la protection des enfants en ligne dans la région arabe en juin 2012.

- Formation du Comité national pour la protection des enfants en ligne en mars 2013.

- Le Centre égyptien de réponse aux urgences informatiques «CERT» a été classé troisième selon l'indice mondial de cybersécurité de l'Union internationale des télécommunications en octobre 2013.

- Le centre a également obtenu une place au comité directeur de l'équipe de réponse aux urgences informatiques de l'Organisation de la coopération islamique en novembre 2013.

- En novembre 2016, le centre et l'Autorité nationale de régulation des télécommunications ont accueilli la cinquième conférence régionale sur la cybersécurité et le Forum régional

FIRST pour la région arabe et africaine.

- Le centre égyptien de réponse aux urgences informatiques «CERT» a participé au forum régional de l'Union internationale des télécommunications en novembre 2017 et à un atelier pour évaluer la préparation à la réponse aux urgences informatiques pour la région arabe et africaine.

- L'Égypte a organisé l'exposition et la conférence sur la sécurité de l'information et la cybersécurité «CAISEC'22» les 13 et 14 juin 2022, sous le thème «La cybersécurité en temps de crise», avec le parrainage et le soutien de divers ministères. L'événement s'est répété en 2024, avec la participation de nombreuses entités gouvernementales, du secteur privé et de diverses entités internationales.

- L'Égypte a été élue à la présidence du Conseil supérieur des télécommunications et des technologies de l'information de l'Union africaine pour une période de deux ans, ainsi qu'à la présidence du bureau exécutif du Conseil des ministres arabes des télécommunications et des technologies de l'information pour une période de deux ans.

- L'Égypte a présidé la 24ème session du Conseil des ministres arabes des télécommunications et des technologies de l'information.

- L'Égypte a été élue membre du Conseil d'administration de l'Union internationale des télécommunications pour l'Afrique et membre du Comité des règlements des radiocommunications de l'Union en 2023.

Résultats et Propositions

Premièrement : Du point de vue institutionnel

1. Étendre l'émission de stratégies sectorielles au niveau de toutes les institutions de l'État et s'y conformer, étant donné que les actifs numériques sont des actifs sensibles de l'État.

2. Définir un plan de travail avec des responsabilités et des tâches clairement définies et chronométrées, ainsi que déterminer les ressources et les sources (numériques) selon les principes de disponibilité, d'intégrité et de transparence.

3. Fournir plus de transparence dans la publication de la stratégie et de ses étapes de mise en œuvre pour atteindre ses objectifs, et mettre en place un mécanisme pour activer le rôle du Conseil supérieur de la cybersécurité dans l'élaboration des plans sectoriels, la surveillance de la mise en œuvre de la stratégie et le respect de celle-ci.

4. Travailler à l'émission d'un guide de cybersécurité pour chaque entité et institution gouvernementale, le publier et le diffuser sous la supervision et le suivi du Conseil supérieur de la cybersécurité.

5. Aligner la mise en œuvre de la stratégie avec l'approche de l'État dans toutes les autres stratégies adoptées par le gouvernement, telles que la stratégie d'intelligence artificielle, la stratégie de lutte contre la corruption, la stratégie climatique, les plans de développement durable et le plan économique.

6. Inclure un représentant de l'autorité législative nationale, ainsi que des comités de réforme législative affiliés à la présidence du Conseil des ministres, et les entités

concernées par la gouvernance législative dans la composition du Conseil supérieur de la cybersécurité, pour garantir la mise à jour continue et permanente des lois régissant afin de suivre l'évolution rapide dans le domaine de la protection du cyberespace et des cyberattaques, conformément à ce qui est prévu dans le troisième pilier de la stratégie : «Construire un cadre législatif intégré».

7. Représenter les entités de recherche scientifique concernées par ce sujet au sein du Conseil supérieur de la cybersécurité, ainsi que les experts ayant le grade de consultant ou équivalent, conformément à ce qui est prévu dans le neuvième pilier de la stratégie : «Programmes de promotion de la recherche scientifique et de renforcement de l'innovation et de la croissance».

Deuxièmement : Du point de vue législatif et judiciaire

1. Œuvrer à l'achèvement du modèle optimal du cadre législatif – conformément au troisième pilier de la stratégie : «Construire un cadre législatif intégré» – ainsi que du cadre institutionnel et organisationnel capable de protéger les ressources numériques et d'assurer la cybersécurité, en renforçant les législations existantes par la rédaction de lois et de réglementations efficaces et complètes pour traiter les cybercrimes et protéger les individus et les institutions.

2. Effectuer une modification législative de la loi n° 175 de 2018 sur la lutte contre les crimes liés aux technologies de l'information, en supprimant la possibilité de conciliation dans les crimes électroniques et en alourdissant les peines jusqu'à une peine de crime, si l'acte criminel est lié à la sécurité et à l'économie nationale ou réalisé dans un but terroriste général.

3. Effectuer une modification législative de la loi sur la régulation des télécommunications pour créer une administration indépendante d'experts en technologies de l'information, rattachée à la direction des experts du ministère de la Justice et faisant partie de la structure du bureau des experts du ministère de la Justice.

4. Bien que le législateur égyptien ait bien fait en confiant aux tribunaux économiques la résolution de tous les litiges et crimes de cybersécurité, nous proposons que les procès soient tenus à huis clos dans certains cas pour encourager les victimes de cybercrimes à les signaler sans craindre de subir une atteinte à leur réputation.

Troisièmement : Du point de vue de la sensibilisation, de l'éducation et de la formation descompétences

1. Encourager les médias sous toutes leurs formes – visuels, audibles, écrits, et numériques sur Internet et les réseaux sociaux – à adopter des campagnes de sensibilisation adaptées aux différentes cultures, tranches d'âge, spécialisations, niveaux d'éducation et de connaissances.

2. Renforcer la sensibilisation à la sécurité, en éduquant les individus et les institutions sur l'importance de la cybersécurité et les méthodes de prévention et de défense de base. Des campagnes de sensibilisation et des formations devraient être organisées en vue de renforcer les connaissances et les compétences en matière de cybersécurité.

3. Promouvoir la culture de la cybersécurité dans l'enseignement primaire, secondaire

et universitaire en adoptant des programmes éducatifs à différents niveaux scolaires pour sensibiliser les étudiants de tous âges, afin de créer une génération consciente de l'importance de la cybersécurité et capable de relever les défis.

4. Accentuer l'innovation, la recherche et le développement :

a. Il est essentiel de soutenir l'innovation, la recherche et le développement dans le domaine de la cybersécurité pour faire face aux menaces évolutives et futures. Il est également important d'investir dans le développement de nouvelles technologies et outils pour la détection, la prévention et la réponse aux cybercrimes.

b. Investir dans l'élément humain dans ce domaine en formant des cadres efficaces et en affinant leurs compétences de manière continue afin de faire face aux défis et risques émergents, ainsi qu'en les préparant à la gestion et au traitement des crises.

Quatrièmement : En matière de coopération internationale et de suivi des indicateurs de performance

1. En matière de coopération internationale et d'accords internationaux comme source d'engagement national :

a. Il doit y avoir une coopération efficace entre les pays dans la lutte contre les cybercrimes. Il est nécessaire d'échanger des informations, des expériences, de partager les meilleures pratiques et de coopérer dans le domaine des enquêtes criminelles cybernétiques pour faire face aux menaces communes.

b. Renforcer les partenariats avec des institutions publiques et privées, locales, régionales et internationales. Il est crucial d'encourager la coopération entre le secteur public, le secteur privé et le milieu académique pour lutter contre les cybercrimes. Les informations et les expériences peuvent être échangées, et la coopération peut se faire dans le développement de solutions technologiques et de stratégies efficaces dans le cadre de la promotion de l'innovation et de la recherche scientifique.

2. En matière de suivi des indicateurs de performance :

a. Adopter les résultats internationaux des plans d'action et des meilleures pratiques dans l'élaboration de la stratégie, en adoptant un modèle optimal, en le construisant et en le personnalisant selon la vision égyptienne et les défis spécifiques, d'autant plus que le guide de l'Union internationale des télécommunications dans ce domaine est constamment mis à jour et amélioré.

b. Suivre les indicateurs mondiaux et adopter leurs méthodologies d'évaluation pour atteindre des positions avancées, voire viser la première place.

c. Œuvrer à la mise en place de mécanismes d'audit et de révision dans l'application des politiques et stratégies de cybersécurité en vue d'atteindre la capacité de mesurer la performance, puis appliquer les normes mondiales et les mesures internationales pertinentes.

■ Bibliographie:

Premièrement: Références arabes * :

- Batikh, Hatem (2021). L'évolution de la politique législative dans le domaine de la lutte contre les crimes liés aux technologies de l'information, étude analytique comparative, Revue des études juridiques et économiques, Université de Sadate, vol. 5, n°1, août 2021.

- Wazir, Abdelazim (2009). Explication du droit pénal, Partie générale Volume 1 : La théorie générale du crime, Dar Al-Nahda Al-Arabiya.

- Al-Awadi, Aws, (2016). « La Cybersécurité », Centre d'études et de planification Al-Bayan p.5.

- L'Autorité générale de l'information (s.n.). Rapport de l'Autorité générale de l'information de la République arabe d'Égypte.

- Gaafar, Hatem, El-Kady, Haitham et Labib, Mohammed (2023). « Cadres stratégiques et juridiques de la cybersécurité », recherche présentée à l'Académie Egyptienne de lutte contre la corruption, édition 2023

- Al-Hussein, Hassan,(2022). « Les Fondements de la cybersécurité », édition, Syrie.

- Akwes, Khaled, (2018). « La Cybersécurité dans la convention arabe sur la lutte contre les crimes liés aux Technologies de l'Information », pp. 303 à 306.

- Présidence du Conseil des ministres égyptien, (2023). « Histoire d'une patrie »

*Les références arabes sont classées dans les recherches selon l'ordre alphabétique arabe

- Abdel Sadek, Adel (2018). « Cyberattaques, nouveaux modèles et défis pour la sécurité mondiale », Centre Arabe de recherche sur le cyberespace.

- Al-Otaibi, Abdel Rahman et Mirghani, Al-Mourshidi (2020). « Le rôle de la Cybersécurité dans la réalisation de la Vision 2030 » , Université arabe Naïve des Sciences de la sécurité.

- Al-Amarat , Fares et Al-Hammamsa, Ibrahim, (2022). « Concept de cybersécurité et défis de l'époque », première édition.

- Suleiman, Qataf et Buqrin, Abdel Halim, (2022). Faculté de droit et de Sciences Politiques - Université Ammar Theligi Agouat, Algérie , « Faire face à la cybercriminalité à la lumière des conventions internationales ».

- Al-Tayeb, Mostafa, (8 août, 2019). « Introduction à la cybersécurité, aux réseaux et aux systèmes d'exploitation. Blog scientifique. »

- Al-Samhani, Mona, (2020). « Exigences pour atteindre la cybersécurité des Systèmes d'information de Gestion », Journal de recherche de la Faculté d'Éducation, Université Mansoura, N ° 11.

- Al Khalifa , Mai (2023) : « Le rôle de la transformation numérique dans la réalisation de la cybersécurité: une étude appliquée sur le ministère de la Justice de l'État du Qatar, Journal de la recherche administrative, numéro1, Qatar.

- Ahmed, Hilali, (2011). « Convention de Budapest sur la lutte contre la cybercriminalité », Dar Al-Nahda El-Arabia, huitième édition.

- Hilali Ahmed, (1997). « Inspection des systèmes informatiques et garanties des informations accusées », Dar Al-Nahda Al-Arabiya, édition initiale, Le Caire.

Deuxièmement: Articles et Sites Web sur Internet (en arabe):

- Portail Arabe de Planification du Développement de la CESAO.

- Le journal Al-Yom Al-Sabia daté du 14 janvier 2015 article sur la lutte contre le cyberterrorisme.

- Le site Web du Ministère égyptien des communications et des Technologies de l'Information.

- Le centre des médias de l'Autorité égyptienne pour l'information.

- Journal Al-Masdar du 18 décembre 2014.

- Al-Rais, Suzi: Définition de la stratégie.

- Enquête sur l'administration en ligne 2022 : L'avenir de l'administration numérique.

- Publication du cadre de gouvernance des stratégies de cybersécurité publié par l'American Institute of standards and technology.

- Le site officiel du Centre National Saoudien d'Orientation sur la Cybersécurité.

- Le site du journal Al-Yom Al-Sabia.

- L'État de l'Égypte selon le rapport 2021 de l'Indice National de cybersécurité.

- Rapport du Centre national d'Information.

Troisièmement: Références et Sites Web sur Internet en anglais:

- Draft Explanatory Memorandum to the Draft convention on cybercime", (2001, February 14), Strasbourg.

- Final activity report", (2001, May 25). Strasbourg .

- Cambridge Dictionary, *available online* via the link https://dictionary.cambridge.org/dictionary/english/cyber; on 03/03/2024.

- Recommendation X.1205 (04/08) Overview of cybersecurity, available in different languages including the Arabic language, *available at*https://www.itu.int/rec/T-REC-X.1205-200804-I; on 03/03/2024.

- National Institute of Standards and Technology (NIST).

- Cybersecurity. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity; on 03/03/2024.

- Green, James, (2016). Cyber Warfare: A Multidisciplinary Analysis, Routledge.

- Middleton, Bruce (2017). A History of Cyber Security Attacks 1980 to Present, Routledge.
- IBM (2023). Cost of a Data Breach Report, Retrieved from https://www.ibm.com/reports/data-breach; on 03/03/2024.
- Statista. Estimated cost of cybercrime worldwide 2017-2028, Retrieved from, https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide; on 03/03/2024.
- Benson, Vladlena and Mcalane, John (2020). Emerging Cyber Threats and Cognitive Vulnerabilities, Academic Press.
- Kala, Emiles (2023). The Impact of Cyber Security on Business: How to Protect Your Business, by Open Journal of Safety Science and Technology, 13(2), Retrieved from, https://www.scirp.org/journal/paperinformation?paperid=126109; on 03/03/2024.
- Maurer , Tim and Nelson, Arthur; (2021). The Global Cyber Threat: Cyber threats to the financial system are growing, and the global community must cooperate to protect it; by a report issued by the International Monetary Fund, Retrieved from, https://www.imf.org/external/pubs/ft/fandd/2021/03/pdf/global-cyber-threat-to-financial-systems-maurer.pdf; on 03/03/2024.
- National Institute of Standards and Technology (NIST). Cyber Framework. Retrieved from, https://www.nist.gov/cyberframework on 03/03/2024.
- Council of Europe, (2001). Explanatory Report to the Convention on Cybercrime: Budapest, Retrieved from, https://rm.coe.int/16800cce5b; on 03/03/2024.
- ESCC: Le site officiel du Centre Égyptien de Réponse aux Urgences Informatiques Retrieved from, https://www.escc.gov.eg/ on 03/03/2024.
- EG-CERT. Retrieved from, https://egcert.eg/ar /on 03/03/2024.
- Gate.ahram. Retrieved from, https://gate.ahram.org.eg/News/3187514.aspx on 03/03/2024.

- UN-ESCWA. Retrieved from, https://andp.unescwa.org/sites/default/files/2021-11/AR_National_Cybersecurity_Strategy_2017_2021.pdf on 03/03/2024.
- International Telecommunication Union (ITU). Global Cybersecurity Index. Retrieved from, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx on 03/03/2024.
- NCSI. Retrieved from, https://ncsi.ega.ee/ on 03/03/2024.
- UN-ESCWA. Retrieved from, https://andp.unescwa.org/sites/default/files/2021-11/AR_National_Cybersecurity_Strategy_2017_2021.pdf on 03/03/2024.
- International Telecommunication Union (ITU). Retrieved from, http://www.itu.int/md/S06-PP-C-0024-en. on 03/03/2024.
- Bayan Center. Retrieved from, www.bayancenter.org on 03/03/2024.
- Oolom. Retrieved from, https://www.oolom.com/6124/ on 03/03/2024.

Quatrièmement : Références en langue française :

Kowalski, Melanie, (2002), «Cybercriminalité: enjeux, sources de données et faisabilité de recueillir des données auprès de la police, Centre canadien de la statistique juridique, No 85-558-XIF.