

Cybersecurity in the context of the growing use of big data in the digital space

الأمن السيبراني في ظل تنامي توظيف البيانات الضخمة في الفضاء الرقمي

MOKHTARI Abderrazak¹

¹ Faculty of Political Science and International Relations, University of Algiers3

(Algeria), mokhtari.abderrazak @univ-alger3.dz

Received: 20/01 /2025

Accepted: 26/05/2025

Published: June /2025

الملخص:

تتناول هذه الدراسة التحديات التي تعترض مقتضيات تحقيق الأمن السيبراني في جزئياته المرتبطة بأمن خصوصية البيانات من خلال التطرق إلى مخاطر الجرائم السيبرانية التي تستهدف الأفراد والمؤسسات، لا سيما في خضم التطور المتسارع الذي تعرفه شبكات الحوسبة السحابية وتخزين المعلومات وتعميم الإنترنت. بما في ذلك تزايد الاعتماد على توظيف برمجيات القرصنة والحروب الإلكترونية التي تسهل إمكانية اختراق البيانات الضخمة الحساسة. وفي إطار هذه الرهانات، أصبح الأمن السيبراني في عصر العولمة الرقمية مهدداً، خاصة بعد ارتفاع معدلات الجرائم الإلكترونية التي أصبحت تمثل تهديدات أمنية جديدة، تتميز بالتعقيد والتشابك، وتستلزم على الدول تطوير آليات فعالة ووعي مجتمعي بغية مواجهة أخطارها.

الكلمات المفتاحية: الأمن السيبراني، الجرائم السيبرانية؛ البيانات الضخمة؛ التهديدات الأمنية الجديدة.

Abstract:

This study examines the challenges of cybersecurity in terms of data confidentiality and the risks of cybercrime targeting individuals and organizations. This is particularly the case in an environment where cloud computing networks and data storage are developing rapidly and the widespread use of the Internet. This includes a growing reliance on hacking and cyberwarfare software that facilitates the hacking of Sensitive big data. Against the backdrop of these challenges, cybersecurity in the age of digital globalization has come under threat, especially following the rise in cybercrime rates, which have become a new security threat characterized by complexity and entanglement, requiring states to develop effective mechanisms and societal awareness to address the dangers of cybercrime.

Key words: Cybersecurity; Cybercrime; big data; new security threats.

Introduction:

In the context of the ongoing evolution of the digital revolution, the predominance of information and communication technologies (ICT) in contemporary life, and the emergence of new security threats targeting digital societies in cyberspace, this transnational threat has transcended traditional concepts of state sovereignty.

Cybersecurity challenges have become a significant concern for governments, largely due to the complexities introduced by the technological revolution. The advent of artificial intelligence (AI) has further compounded this challenge, as it has become integral to the functioning of social networks, which are used to manage both public and private services and digital commercial marketing. Additionally, processing sensitive information related to the privacy of individuals and organizations has become a crucial area of focus.

The advent of new modes of communication in the virtual realm has not insulated these systems from the perils of cyber-attacks and data breaches. In its current state, cyberspace is susceptible to a multitude of cybercrimes, including extensive data destruction, which presents formidable security, legal, and technical challenges to nations, particularly those with inadequate data protection and security protocols.

Research problem: Cybersecurity faces significant challenges, primarily the increase in cybercrimes targeting digital identities and big data of internet users and institutions. This has given rise to a range of international concerns regarding the protection of operating systems from the risks of hacking and cyberattacks that target data security within the digital realm. In order to gain a deeper understanding of the various variables associated with cybersecurity, the following question will be addressed: In the context of the increasing digital reliance on big data, what are the challenges facing the achievement of cybersecurity?

Importance of the study: The scientific value of this research comes from the interpretation of the variables associated with the modern issues that research in the cognitive fields of cybersecurity, especially in its parts related to electronic data hacking and ways to protect individual and organizational digital identities. This poses new challenges to the digital sovereignty of states.

Objectives of this study: This research aims to elucidate the threats to data privacy in the digital space. To this end, an investigation is undertaken into the types of cybercrime and how they are deployed within cloud computing, thereby demonstrating the potential risks to users and organizations. Furthermore, the paper defines the nature of these crimes and the resulting issues related to digital society's security and economic dimensions.

Research methodology: The study takes a descriptive approach to examine aspects related to the phenomenon of cybercrime, focusing on the risks it poses. Additionally, it seeks to identify mechanisms to counter these threats to meet the cybersecurity requirements that have become an integral part of each country's national security concept.

1- Cybersecurity (concepts and dimensions)

This section will provide an overview of the fundamental concepts of cybersecurity and examine its various dimensions at different levels.

1.1- The concept of cybersecurity in the digital space

Cybersecurity is a scientific field related to the security of digital data technology, in terms of achieving high levels of security of databases in cloud computing, Internet communication networks, and information systems, relying on procedural techniques that provide protection from penetration and confront cyber threats, or minimize their negative effects ¹. In addition, it can be defined as activating a set of programs to prevent unauthorized access to data. Such a system aims to ensure the continuity of operating systems and to maintain the integrity of databases from threats that target cyberspace ².

The French Atomic Energy and Alternative Energies Authority has defined cybersecurity as: “The efficacy of the information system in enabling it to withstand events that arise in cyberspace and that are likely to jeopardize the integrity and confidentiality of data stored, processed, or transmitted, including the related services provided by these systems or that provide access to them”. Cybersecurity is not a static state, but a “state” that must be maintained through strong technical skills and real-time detection and response tools to get back to normal as quickly as possible after an attack ³.

From what has been presented above, it can be discerned that there are many definitions of the multifaceted and multidimensional concept of cybersecurity. Furthermore, it can be linked to government strategies aimed at achieving firewall immunity, which serves to prevent a multitude of electronic intrusions that threaten the country's information security, including the data of institutions, public utilities, and Internet users.

1.2- Cybersecurity Dimensions

1.2.1- Political dimensions

The political dimensions of cybersecurity are among the threats that destabilize the political life of countries especially since this digital space is an open space for raising political issues, where activists' ideas compete freely, both supporters and opponents, including those calling for chaos and coups, according to their ideologies and loyalties, which affects the balance of power within the same society.

Extremist networks and activists are using the digital space for politically motivated attacks to spread propaganda, attack the websites of their political enemies, steal money to fund their activities, or plan and coordinate their crimes. Based on the nature of the attack, politically motivated attacks can be categorized as creating protests against political systems, laws, and state policies ⁴.

Cyberspace has opened channels of communication that cross national borders for states and has enabled activists and organizations to become key players in political life at home and abroad. On the other hand, digital communication has become one of the most important channels regimes rely on in dealing with political affairs to target the largest segment of society to promote political issues or communicate information to the public. This is because cyberspace includes millions of interactors on social networks (Facebook, Twitter, YouTube, etc.), ⁵ as well as the extent of the impact that the spread of information on these platforms has, regardless of the level of the policies promoted within the digital space.

In this context, it is worth noting, for example, that leaks of confidential files and

serious breaches of state databases have often caused political and diplomatic crises ⁶. Such as the leaks of thousands of secret political documents through the website “WikiLeaks”, which negatively affected the stability of the political life of many countries and even the relations between the countries themselves ⁷.

1.2.2- Economic dimensions

In light of the digital revolution, cyberspace has become a broad field for economic transactions in the field of trade, industry, and major monetary transactions between companies, this reality has led to the emergence of a digital economy that requires attention to economic cybersecurity, as this field is vital for achieving development in countries with strong internet networks. This rapid digital development in the international environment is not immune to the risk of hackers disrupting development paths and hindering the future of economic relations between countries ⁸. Therefore, economic conflict between nations or financial greed of companies often leads to the use of cyberattacks, intending to obtain confidential data through cyber espionage, such as what happened in the United States in 2003, the “Titan Rain” cyber espionage case, where hackers penetrated NASA's computer network, and acquired sensitive data for flight planning programs and flight specifications ⁹.

The digital economy is closely related to cybersecurity due to the huge reliance on smart applications in the management of productive activity and the provision of economic services, through what their information systems provide in terms of using Internet networks to manage the cost of production, under favorable conditions that serve the paths of progress, Whether it is related to protecting the service provider or the Internet user ¹⁰.

The trend towards the digital economy has contributed to increased investments by financial institutions, which poses legislative and technical challenges to curb cybercrime, such as money laundering, or even the protection of intellectual property ¹¹. This trend has been accompanied by a rise in cybercrime, necessitating intensive international efforts to raise cybersecurity standards for the digital economy ¹². For example, statistics indicate that, in 2022, the proportion of people using the global Internet through mobile phones or computers was about 5.3 billion worldwide, equivalent to about %66.3 of the world's total population ¹³. The German economic statistics center Statista also showed retail e-commerce generated \$5.8 trillion in sales in 2023, and e-commerce revenue across social media platforms worldwide reached \$724 billion in 2022 ¹⁴.

1.2.3- Social dimensions

Cyberspace is characterized by its open features within Internet services via various social media networks that interact with digital identities that allow users to share ideas and information, including creating official pages, accounts, and groups interested in disseminating different themes and ideologies. Cyberspace is also a means for the development of societies, but it is not without dangers emanating from illicit content that harms society's values, contributing to a high proportion of cybercrime practices, particularly those related to pornography, drug trafficking, cyberterrorism, and extremist recruitment of issues affecting the internal stability of States ¹⁵.

The social dimensions in cyberspace are manifested through a social and cultural conflict between users (individuals or groups) over incompatible ideas, or power, including

the denial of control to others. Also, intercultural conflict manifests itself in the form of ethnic conflict through cyber conflicts that are instigated for cultural and ideological reasons ¹⁶, such as the Taiwan-China cyber conflict, the Sino-American cyber conflict, and the Palestinian cyber conflict with the Zionist entity.

1.2.4- Military dimensions

This sensitive dimension is related to defense institutions and their ability to secure Internet networks and databases, ensuring the safe movement of military information, especially cyber-attacks that may destroy the database, thus negatively affecting the state's national security. Former ITU Secretary-General “Hamadoun Tourih” says the catastrophic consequences that cyberwarfare attacks can cause in his presentation on cyber peace:” These attacks can happen without warning. Computers and mobile phones suddenly stop working; ATM screens and bank machines go dark; air, rail, and road traffic control systems are disrupted; and when the power goes out in hospitals, homes, shopping centers, and public buildings, communities are plunged into darkness and government authorities are unable to assess the extent of the damage, communicate with the rest of the world to report the disaster or protect their vulnerable citizens from the next attacks. This is the cruel ordeal of a society paralyzed by the instant loss of its digital networks by the devastation wrought by this new kind of cyber warfare” ¹⁷.

Within this framework, Cyber defense focuses on anticipating major threats that affect national life, as it is a digital sovereign activity, carried out by the defense establishment by the powers granted to it by law. It is also based on the set of resources placed under the responsibility of the state to defend its data systems in the cyber environment, especially attacks that would affect the state's military or economic potential or security. Since cyber defense aims to ensure the security of big data and the security of critical systems ¹⁸, it constitutes the cyber dimension of the country's national security.

2- Digital identity in cyberspace

This section examines the concept of digital identity in cyberspace, considering the characteristics that define it in the context of an increasing reliance on smart applications and social networks, as well as the growing use of big data in cloud computing.

2.1- Characteristics of digital identity

Digital identity is an essential component of a digital society and knowledge economy; it is the key to entering the digital world and conducting business, economic, or any kind of transaction and communication. Digital identity is consequently an interdisciplinary category, it is considered a contextual, dynamic, evolutionary, multi-dimensional, variant, and complicated subject ¹⁹. It is also described as a mercurial concept the law struggles to regulate. Digital identity is a complex technical and legal-political category that requires a holistic approach.²⁰

Digital identity represents a set of data that relates to Internet users, as it has become an essential part associated with our uses in the digital space, due to the dependence of societies on technology in all aspects of life, such as e-commerce, distance education, financial and administrative transactions, and others ²¹. Therefore, digital identity protection is an urgent

necessity to ensure the security and privacy of our data. Digital identity data generally includes the following information ²²:

- Personal information: This includes "Name, date of birth, address, and email address".
- Unique identifiers: usernames and multiple passwords for various digital accounts.
- Financial data: bank account numbers and credit card numbers.
- Online activities: browsing history, social media posts, and online purchases.
- Biometric identifiers: fingerprints, facial recognition, and voice recognition.

In the same context, we find that the feature that characterizes the digital identity in the virtual space takes multiple forms, which gives it a kind of variation, according to the type of data required in smart applications and related activities, as we illustrate this by showing some examples as follows ²³:

Social networking applications: "Facebook, TikTok, Instagram and others", where we note that these applications contain personal information such as names, dates of birth, addresses, phone numbers, and emails. These applications are characterized by the ability to post and share photos and videos that show an individual's activities, interests, and social relationships. These applications also reveal the user's behavioral patterns, locations, and activity times, making them a digital space with multiple layers of personal data.

Email accounts: such as Gmail, Outlook, and Hotmail, contain information about sent and received messages and attached files. These accounts can include sensitive data related to official professional jobs and assignments, financial accounts, personal information, and other private data. It should be noted here that email accounts are considered one of the most important data sources targeted by hacking networks in cyberspace.

Smart apps of financial services: The increasing prevalence of smart apps for online financial services has led to a corresponding increase in the data these apps contain. This data includes bank account details, credit card information, and transaction histories. However, this also makes these apps vulnerable to hacking attempts in the digital space, with the potential for financial gain for the perpetrators.

2.2- Big digital data

2.2.1-The concept of data: It represents all symbols, letters, texts, images, and videos created for use, dissemination, or storage based on electronic media and cloud computing systems. Data privacy is an expression of the sole right of the owner of the data that gives him the right to dispose of it or give permission to publish it to individuals or organizations within the spaces of the Internet ²⁴. Facebook, for example, offers its users various features that combine the option of making their data public or keeping it invisible or limited in visibility with algorithmic measures to protect data privacy. Leading companies in information technology and cloud computing have also started offering cloud storage services, such as Google Drive, iCloud, and One Drive, which are continuously updating their data security programs as it is a delicate responsibility that requires high technologies to secure the data of individuals and institutions (such as universities, hospitals, health, etc.) ²⁵.

The advent of Big Data represents a significant milestone in the evolution of information and communication systems. It signifies the emergence of a vast repository of

intricate data that surpasses the capacity of conventional software and hardware to accommodate, process, and disseminate ²⁶. Similarly, digital data is raw information before classification, organization, and processing techniques are applied. Data can be divided into three categories. The first category is structured data in the form of tables or databases. Secondly, unstructured data is the bulk obtained daily from various sources such as text, images, videos, messages, and website clicks. Thirdly, semi-structured data is a category that is not represented in the form of traditional tables or databases ²⁷.

2.2.2- As for the features of big data ²⁸:

-Volume: Refers to the amount of data generated from different sources that may reach a significant amount of data, which determines its size and value.

-Diversity: Refers to the extracted big data and includes structured data, which is the smaller proportion, unstructured data, which is the larger proportion, or semi-structured data, which is a combination of both types of data.

-Velocity: This means the frequency of data processing speed in a short time

-Heterogeneity: This can be defined as inconsistencies in data that can lead to difficulties in processing and effective data management.

The exponential growth in the amount of data produced daily on internet networks not only reflects users' activity but also represents a tremendous resource for artificial intelligence (AI), as data is the fuel that powers AI engines, used to train intelligent models and optimize performance and services. For example, Meta Platforms owns four of the largest social media platforms with massive amounts of big data, each with one billion monthly active users: "Facebook, WhatsApp, Instagram, and Messenger". while most top-ranked social networks with more than 100 million users are based in the United States, Chinese social networks such as TikTok, WeChat, or the video-sharing app Douyin have also gained global appeal to rival their American counterparts ²⁹.

In recent years, there has been an exponential growth in the amount of big data being generated every minute on the Internet, as highlighted by the Domo company infographic, which argues that this data is not just numbers, but the driving force behind improvements and innovations in the field of artificial intelligence ³⁰. Data will continue to grow exponentially, necessitating the development of new technologies to effectively manage this vast amount of information.

3- Transnational cyber crimes

This section examines the phenomenon of transnational cybercrime, analysing its defining characteristics and the threats it poses in the digital domain.

3.1- A conceptual introduction to cybercrime

Cybercrime is a term derived from the word "cyber", which refers to the computerized processing of data and is associated with the unlawful use of computer networks. The term "cyber" is therefore associated with all types of cybercrime, including cyber hacking, cyber terrorism, and cyber fraud ³¹. Cybercrime is one of the negative effects that appeared within the developments of the digital revolution, as it took a large share of studies to define its concept and the terms referring to it, such as cybercrime, cyber piracy, internet crimes,... etc ³². It can also be defined as, a criminal activity aimed at sabotaging and hacking computer

data, or any unauthorized use of information technology, to attack any legitimate interest, whether material or moral ³³.

Cybercrime is defined as crimes that target the information and communication system within Internet networks and cloud computing. The United Nations defines it as any behavior that includes electronic operations that harm the security of the information operating system and data processing ³⁴. The Organization for Economic Cooperation and Development (OECD) defines it as “any act of infringement of material or moral property resulting directly or indirectly from the unlawful use of data and software” ³⁵. In the same vein, the European Commission defines cybercrime in a broad sense as “any crime involving the use of computer technologies” ³⁶.

From the above, we can define cybercrime as any illegal software intrusion that causes material and technical losses in databases and Internet networks, targeting the cybersecurity of state institutions and users.

Cybercrime has a range of characteristics, which can be summarized as follows ³⁷:

Speed of execution: Cybercrime is distinguished by its rapid execution, necessitating minimal time for completion. This is achieved through the utilisation of virus programs that are specifically designed to circumvent cybersecurity measures, employing a combination of sophisticated programming languages and advanced protection techniques.

Transnational: Cybercrime is not constrained by national boundaries; it is not limited to a specific period. This is because cyberspace is a virtual digital society that extends beyond the geographical boundaries of states and whose data interacts within the domain of Internet networks. To perpetrate cybercrime from a remote location, hackers may engage in a range of activities, including the hacking of information databases that interact within Internet networks, the interception of financial transfers, the theft of confidential information, or the disruption of information systems.

Soft crimes: Cybercrime is not like traditional crimes that use the tools of direct violence such as robbery, murder, or terrorism, so it is a soft crime that takes place in cyberspace and aims to hack sensitive or personal data or take money from assets

Complex and difficult to follow: Cybercrime is difficult to prove and requires high technology to track and locate the perpetrators, unlike traditional crime, which can be traced through physical evidence such as fingerprints or physical evidence. In addition, cybercrime is characterized by ambiguity and transcends state borders. Therefore these crimes often lead to the dispersal of investigative efforts and international coordination to track them, whether in terms of their location, which can vary between more than one country ³⁸.

3.2- Nature of cybersecurity threats

3.2.1- Security and political cybercrimes:

It is related to espionage, hacking the electronic accounts of political figures or penetrating the confidential databases of official civil and military state institutions, and there are several examples of this, such as the hacking of the Pentagon's network of information systems and infiltration of control programs, which created a major emergency. In 2010, the advent of a wave of chaos in some Arab countries saw the exploitation of the Internet to disseminate confidential information and documents via the WikiLeaks platform. This

resulted in the exposure of scandals about the conduct of rulers and international political figures, with a particular focus on allegations of corruption, the misappropriation of national wealth, and security concerns. In 2016, emails sent by John Podesta, Hillary Clinton's campaign manager, were leaked ³⁹.

It can be said that over the past decade, there has been a notable surge in the prevalence of cyberattacks within cyberspace. In December 2020, the United States government became aware of an intrusion into the networks of nearly a dozen federal agencies, which was designated as the SolarWinds hack. In 2021, a ransomware attack on the Colonial Pipeline resulted in the shutdown of the pipeline, which provided approximately half of the East Coast's gas supply. Ransomware attacks on IT management group Kaseya also disrupted its big data. General Paul Nakasone, head of the National Security Agency and Cyber Command, said in an interview at NSA headquarters in Michigan: "2021, this is the inflection point for the nation in cyberspace, this is when cybersecurity became national security" ⁴⁰. The rapid development of digital technology has been accompanied by a dramatic rise in cyberattacks, which have become one of the most important national security threats to countries and political systems.

3.2.2- Economic cybercrimes:

hacking the networks of banking and stock exchange information systems to make illegal financial transfers, steal credit cards, or launder Bitcoins, as well as transfer financial balances from one bank to another by hacking their bank accounts through Internet networks that provide real-time electronic money transfer services between countries, transcending national borders and causing great financial losses to the economic and financial sectors of many countries ⁴¹. For example, in April 2003, many of the financial balances of customer accounts in 13 banks in Dubai were hacked, transferring funds from personal accounts to fictitious accounts created by Asian hackers ⁴².

Economic cybercrime is on an upward curve, as this phenomenon has increased significantly, according to the Business Software Alliance, an organization specialized in cyber studies and software market analysis, which is funded by major software companies such as Microsoft, and this is done through infringement of intellectual property rights such as data piracy and forgery, reproducing original programs and reselling them at prices much lower than the original price, causing financial losses to major companies ⁴³. In early 2103, for example, the GOZI virus was spread via cloud computing, infecting more than a million computers globally, giving a group of hackers access to bank account information in Europe and North America, enabling them to steal at least US\$50 million between 2005 and 2011. The case has been described as: "one of the most sophisticated financial hacking operations ever seen" ⁴⁴.

3.2.3- Social cybercrimes:

Social cybercrime is associated with targeting the normal life of Internet users in cyberspace by hacking their digital identity data in illegal ways and spying on their privacy, such as hacking email accounts and passwords to impersonate them and take important files and photos from their database, and "social engineering" is often used as a way to threaten and blackmail them morally and financially. Therefore, hacking social media users and acquiring their digital identity contributes to destroying the fabric of family relationships due

to the spread of false news, rumors, and defamation in online networks. In addition to the use of cybercrime in spreading the manifestations of moral decay and kidnapping minors ⁴⁵.

Social networks have become an attractive platform for cybercrime, as it is a virtual space where billions of people interact, exchange information and establish relationships. The sheer volume of personal data exchanged on these platforms makes them tempting targets for cybercriminals, especially with their continued growth and impact on our daily lives, which is accompanied by the growth of the dark side associated with them, posing a threat to individuals, organizations, and even national security. The lack of awareness and inadequate security measures implemented in social media networks to protect users' data drives cybercriminals to look for loopholes and weaknesses in the platforms' security to gain unauthorized access to users' accounts, putting personal information at risk. The rise of fake profiles has also contributed to hacking, spreading disinformation, and engaging in social engineering attacks against individuals and organizations ⁴⁶. The interconnected nature of social media makes it vulnerable to all kinds of threats that can harm personal and professional lives, and damage the reputations of users and organizations.

3.2.4- Cyber terrorism:

Cyberterrorism is a form of cyber warfare based on an extremist political and religious ideology that utilizes electronic technologies in cyberspace to intimidate societies and subjugate others by penetrating information systems. The United States Federal Bureau of Investigation defines it as: "Any intentional, politically motivated attack on information systems, programs or data, resulting in acts of violence against civilians, whether committed by a national group or invisible agents" ⁴⁷.

In light of the outcomes of the digital revolution, Internet networks have become a means of communication and an outlet for the activity of transnational terrorist organizations. Their activity has increasingly escalated through cyberspace, which has opened channels for funding and recruiting agents, as this technology has been exploited to achieve great damage beyond the concepts of traditional threats, as terrorist groups around the world have relied on Internet networks as a key element to support and achieve their goals and strengthen their activity in the virtual space ⁴⁸. Terrorist groups spread around the world have relied on Internet networks as a key element to support and achieve their goals and strengthen their activity in virtual space, which contributed to inflating the mental image of their size. Cyberterrorism threats have become a challenge to international peace and security since the events of September 11, 2001. In this period alone, more than five thousand websites and thousands of chat messages of terrorist groups have been counted ⁴⁹.

The most violent cyber-terrorist attacks are those that target the vital interests of the state, such as hacking the operation and distribution systems of water, energy and electricity, land, sea, and air transportation networks, nuclear power generators, and communication networks, all of which fall within the work of the e-government, as this type of cyber attack can paralyze and isolate the normal movement of the state, leading to chaos and violence within the society ⁵⁰.

4- The prerequisites for attaining cybersecurity and peace

Cybersecurity is one of the recent trends that the international community is still

working on crystallizing its regulatory and legislative frameworks as a common approach to achieving peace and security. It is also a result of the rapid development of Internet technologies and information systems, accompanied by the spread of cybercrime risks that affect cyberspace users (citizens, institutions, and states).

4.1- Cyber Governance

Cyber governance as presented by the United Nations Educational, Scientific and Cultural Organization (UNESCO) is defined as the optimal and secure use of an electronic application that facilitates services between the government sector, the private sector, and society. It is also the use of electronic technologies in public activities by strengthening relations between public authorities, civil society, and the electronic delivery of public services within the framework of e-government requirements ⁵¹.

As part of these challenges, cyber governance is looking for new ways to prevent information security breaches based on the five principles of cybersecurity (planning, proactivity, protection, prevention, and pitfalls. These five principles identify signs of intruders in the network, establish guidelines for protecting usernames and passwords, and match protection against physical access to IT facilities with the most effective security systems to deal with potential threats ⁵².

Securing databases from hacking is important to maintain digital service operations in the IT world in a sound, systematic, and sophisticated manner. For example, there are several recognized standards for information security management such as ISO 27001, which has proven to be effective in achieving high levels of security protection against the risks of cybercrime ⁵³.

From what has been presented, we can define e-governance as the product of the interactions of data traffic through Internet networks to provide a contemporary pattern of digital services in the conduct of human relations within state actors (states, international and regional organizations) and non-state actors (private institutions and society), ensure a safe environment in cyberspace, based on rights, duties, the rule of law, and accountability.

4.2- Enhancing community awareness within cybersecurity requirements

The United Nations and its partners are working to curb cybercrime through awareness programs on the dangers of hacking, as millions of Internet users around the world do not know the basics of operating system security, leaving their devices open to hacking.

Therefore, governments are working to implement cyber awareness programs for their citizens through awareness-raising announcements related to securing internet networks and promoting a culture of optimal use of social media networks. Most countries in Europe and the Americas have also developed awareness-raising strategies through annually scheduled campaigns such as Cybersecurity Awareness Month and Internet Safety Day ⁵⁴. In contrast, these campaigns are almost non-existent in most African countries.

Large-scale preventive campaigns aim to reach the largest possible number of Internet users, relying on various means to deliver their messages to the public, such as awareness posters in public places, sensitization programs broadcast on television or radio, or displayed on websites. These campaigns aim to raise awareness of safe Internet use, such as securing Wi-Fi networks, backing up files, protecting personal data, and protecting against malicious temptations. For example, the United States has also developed its national cybercrime

prevention campaign called “Stop.Think.Connect” The goal of this national campaign is to educate the public about the potential dangers of unsafe Internet use, raise awareness, train individuals on the applications available to protect their digital privacy, and provide them with an instruction manual for safe behavior in cyberspace⁵⁵.

Social media networks are also one of the most important methods employed in cybersecurity awareness campaigns, as they are the most widely used platforms by millions of individuals, and are characterized by high browsing of the information published in their space. Therefore, publishing advertising campaigns on social networking sites such as Facebook, YouTube, Instagram, and TikTok is one of the most effective means of raising awareness.

The involvement of civil society organizations in raising cyber awareness is a positive way for them to contribute to spreading the message about the risks of cybersecurity within the framework of their voluntary tasks. Where their programs must be integrated within the framework of governmental strategies and collaborative networks related to cybersecurity awareness activities. Especially cooperating organizations active in the technological fields achieve social and legal awareness related to cybercrime and activate conferences, to unify preventive efforts against the dangers of the digital space⁵⁶.

4.3- International efforts to reduce cybercrime

In this context, the United Nations, represented by the International Telecommunication Union (ITU), is intensifying international efforts to regulate cyberspace to create a safe environment that will facilitate the achievement of cyber peace and the reduction of the phenomenon of piracy. Based on joint international cooperation through international conferences and charters, for example, in 2000, the United Nations General Assembly adopted resolution 55/63 on combating the misuse of information technology, the most important points of which are as follows⁵⁷ :

- Adapt legal systems in line with the use of Information and communications technology, while emphasizing that cybercrime is a criminal offense and therefore punishable by law
- The international community must adapt its judicial laws to align with international texts and legislation about cybercrime in the criminal domain. Furthermore, there is a pressing need to modernise the legislative system to ensure its compatibility with the accelerated advancements in cyberspace.
- Professionals in the cyber field must receive specialized training to enhance their competence and electronic skills. Furthermore, it is crucial to rely on various specialized agencies to fight cybercrime.

Over the past two decades, the United Nations Organization has been adapting concepts and finding effective solutions and legal legislation in line with the evolution of cyberspace. Similar to the ratification of the regulations of the World Conference on International Telecommunications (WCIT) held in the United Arab Emirates in December 2012. in which the laws governing international telecommunications were reviewed and considered as a common and binding international treaty based on international coordination to ensure a safer digital environment based on cyber resilience to overcome cyber threats, cyber security to overcome cybercrime, and cyber peace to overcome cyber warfare⁵⁸.

Similarly, the Budapest Convention (2001) and the General Data Protection Regulation (2016) are legal frameworks designed to curb cybercrime. The Budapest Convention introduces a legislative framework to combat cybercrime by adopting the latest criminal law

standards based on important procedural rules regarding the temporary storage of data that may be used as evidence to prosecute criminal acts. The European General Data Protection Regulation (GDPR) has also established the legislative framework for properly handling information in a way that contributes to improving the data security framework, thereby reducing cybercrime. The Budapest Convention and GDPR is a binding international instrument on cybercrime that advocates for a common criminal policy aimed at protecting society from cyber intrusions and aims to combat threats to the confidentiality and integrity of operating systems, networks, and data ⁵⁹.

Conclusion

Cybersecurity is witnessing growing security challenges whose risks are significantly reflected in the security of countries, societies, and individuals, especially in light of the rapid development of artificial intelligence programs and the existence of hostile hacking networks spread globally, which take multiple faces (hackers, cyber terrorism), whose mission is to hack, extort and carry out cyber attacks targeting the vital sectors of countries and institutions and incur great material losses.

It must be said, then, that the fight against cybercrime is a joint international action that still requires greater efforts within the definition of a more cooperative international policy, given the global dimension that characterizes this type of transnational crime. It is a fast-growing phenomenon in cyberspace characterized by the rapid development of digital technologies, as well as the increasing use of the Internet in all daily activities of societies. The rise of this type of crime poses a fundamental challenge to governments in achieving optimal cybersecurity. It requires more flexible defensive and preventive measures than what we have discussed to counter the risks of data breaches.

Protecting digital privacy in the context of heavy reliance on big data presents difficulties related to the exponential use of data volume and the speed of its interactions within the broader scope of the transnational cyberspace, especially concerning the ability to control its sources, the speed of its transmission, and the increasing growth in its size. Therefore, it is necessary to develop states' cyber defence mechanisms in a manner consistent with the broader legal, regulatory, technical and technological frameworks for achieving cybersecurity requirements, and to enhance international cooperation in addressing the security challenges impeding cyber peace and stability.

Moreover, the swift advancements in information technology and international communication, coupled with the expanse of real-time interaction between data and the digital society in all daily activities of internet users, institutions, and governments, are driving the international community to enhance its legal framework in order to combat the growing threat of cyber-attacks, like protecting the international information network (Internet), defining responsibility, protecting privacy, and intellectual property rights.

The pressing need to employ digitalization services has imposed a new pattern in international competition, particularly the new dimensions created by information technology, both socially and economically. It is clear that information technology, communication

systems, and infrastructure have become essential needs for countries that aspire to achieve optimal levels in protecting their cybersecurity.

The challenges of protecting big data require continuous effort by implementing appropriate technical and programmatic preventive measures and taking advantage of available technological tools to ensure maximum reduction of the risk of digital hacking and protection of data from cyber attacks.

In this context, we present a set of recommendations represented in the following points:

- Increase preventive measures and work on adapting legal legislation in line with the rapid development in cyberspace, within the framework of the obligation to implement the outcomes of joint international coordination agreements to combat cybercrime.
- Use strong and complex passwords: It is recommended to use numbers, upper and lower case letters, and multiple symbols, without using the same password for other accounts and applications. Also, software and applications should be updated regularly to close security vulnerabilities and protect computer devices from malware.
- Intensify awareness campaigns on cybersecurity topics while uniting the efforts of the components of society (government, civil society, and private organizations active in technologies) to fight the phenomenon of cybercrime.
- Developing technical training programs for users to learn the basics of protecting operating systems and dealing with Internet networks to reduce cyber intrusions targeting individual and organizational data.
- It is imperative to install anti-virus software in order to protect personal data, and to refrain from opening links or downloading software from websites of unknown provenance.

Citations:

- 1-Mona Al-Ashqar Jabbour, Cybersecurity is the Obsession of the Age, League of Arab States: Arab Legal Research Center. 2016, p 45.
- 2-Omar Hamed Shoukry, The Fifth Domain: Cyberspace, Egyptian Institute for Studies, Oct 7, 2019, retrieved May 5, 2024, available at the link:<http://www.eipss-eg-org.cdn.ampproject.org>
- 3-Guillaume langin, L'enjeu de la cyber sécurité « La cyber parade s'organise », le magazine de la recherche impliquée, Commissariat à l'énergie atomique et aux énergies alternatives(CEA), Paris, Mars 2021, p 19, pp 1-36.
- 4- Robin A Gandhi, William Sousan, Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political, Technology and Society Magazine, February 2011, 30(1), p 29. pp 28 - 38
- 5-Mona Al-Ashqar Jabour, Op Cit, p 30.
- 6-Noureddine Flak, Cyber threats through blue space and their impact on the national security of countries, People's Daily, December 8, 2021, retrieved May 10, 2024, available at the link:
<http://www.ech-chaab.com/ar%.html>
- 7-Mona Al-Ashqar Jabour, Op Cit, p 30.
- 8- Noureddine Flak, Op Cit.
- 9- Robin A Gandhi, William Sousan, op cit, p 32.
- 10 - Chabrow E, Susan Collins,” one of the bill’s sponsors, said in a Senate speech. “The threat is not just to our national security, but also to our economic well-being”, Govinfosecurity, December 14, 2012, retrieved June 6, 2024, available at the link:
http://www.govinfosecurity.com/articles.php?art_id=4506&opg=1
- 11- Chabrow E, Susan Collins, op cit.
- 12- Muhammad Mukhtar, Can countries avoid the dangers of electronic attacks? Events Trends Magazine, Abu Dhabi, Issue 6, January 2015, p 6.
- 13-Jamal Kassem Hassan, Arab States Electronic Commerce Statistics "10th Meeting of the Technical Committee of the Arab Statistics Initiative", Arab Monetary Fund, Abu Dhabi, Nov 9, 2023, p5. pp 1-15.
- 14- Sky News Arabia, global e-commerce fictional sales in 2023, News Arabia, February 7, 2024, retrieved September 20, 2024, available at the link:<https://www.skynewsarabia.com/business/169>.
- 15-Mona Al-Ashqar Jabour, Op Cit, p 29.
- 16- K. Avruch, “Cross-cultural conflict”(Conflict Resolution), in Encyclopedia of Life Support Systems (EOLSS). Oxford, U.K: Eolss, 2002, p 25.
- 17- Hamdon tourih, cyberspace and the threat of cyberwarfare. Switzerland: International Telecommunication Union, 2011, p 6.
- 18-Bertrand Warusfel, Cyberdefense “digital dimension of national security”, Hal open science, ISTE, Paris, Dec 15, 2023, retrieved September 1, 2024, available at the link:
<https://hal.science/hal-04347116>
- 19-Margarita Robles-Carrillo, Digital identity: an approach to its nature, concept, and functionalities, International Journal of Law and Information Technology, Volume 32, Issue 1, September 18, 2024, p 3. pp 1-21.
- 20- Umar Mir et al., ‘AI-enabled Digital Identity – inputs for stakeholders and policymakers’, Journal of Science and Technology Policy Management, February 2021, retrieved September 1, 2024 , available at the link:

<https://www.emerald.com/insight/content/doi/10.1108/JSTPM-09-2020-0134/full/html?skipTracking=true>

21- Ali Abulhasan, digital identity: what is it and how can it be protected?, Covenant News Website, May 27, 2024, retrieved June 6, 2024, available at the link:

<https://www.alahednews.com.lb/article.php?id=69857&cid=181>

22- Charlotte Bowyer, What is digital identity?, Onfido Company, January 12, 2024, retrieved June 4, 2024, available at the link:<https://onfido.com/blog/digital-identity/>

23- Ali Abulhasan, Op Cit.

24- Ali Sayyid, data privacy.. Its Importance and Ways of Protecting It, Covenant News Website, Feb 6, 2023, retrieved June 6, 2024, available at the link:

<https://www.alahednews.com.lb/article.php?id=50473&cid=181>

25- Ali Sayyid, Op Cit.

26- Chen, C. P., & Zhang, C.-Y, Data-intensive applications, challenges, techniques and technologies: A survey on Big Data. Information sciences,2014, p 314.

27- Adnan Mustafa al-Barr, Big Data and Application Areas, Blog Site, December 1, 2018, Retrieved September 10, 2024, available at the link:<https://www.awforum.org/index.php/ar>

28-Al-Hassan Sha 'aban Ahmed, Big Data: What It Is and Its Significance and Elements, Arab International Journal of Knowledge Management, vol. 1, No. 2, April 20, 2018, p. 115. pp. 99-148.

29-Ali Abu al-Hassan, The Data Does not Sleep: the importance of data for artificial intelligence and Arab content on the Internet, Covenant news website, June 1, 2024, Retrieved Sept 6, 2024, available at the following

link:<https://www.alahednews.com.lb/article.php?id=70087&cid=181>

30-Ali Abu al-Hassan, Op Cit.

31- Romain Boos, The fight against cybercrime with regard to State action, Doctoral thesis, faculty of law and economic sciences, University of Lorraine, France, 2016, p 25.

32-Youssef Saghir, Crime Committed via the Intranet, Master's Thesis in International Business Law ,Faculty of Law and Political Sciences, University of Tizi Ouzou, 2010, p 9.

33-Miftah Boubacar Al-Mutradi, "Cybercrime and Overcoming Its Challenges." A research paper within the activities of the Third Scientific Conference of Presidents of Supreme Courts in Arab Countries. Sudan, September 25, 2012, p. 3.

34-Hisham Mohamed Rostom, "Information Crimes: Principles of Technical Criminal Investigation." A research paper presented within the activities of the scientific conference on: (Law, Computers and the Internet). United Arab Emirates: Emirates Center for Strategic Studies and Research, November 2004, p. 40.

35-Brigitte Pereira. The fight against cybercrime: from the abundance of the norm to its perfectibility, International Journal of Economic Law, Paris, 3 t. XXX,2016, p398. pp 387 - 409.

36- Romain Boos, Op Cit, p 26.

37- Dhiab Musa Al-Badaina, National Security in the Information Age, Naif Arab University for Security Sciences, Riyadh,2011, pp. 92-93.

38- Hamdoun Tourih, Cybersecurity Guide for Developing Countries, International Telecommunication Union, Switzerland,2007, p. 47.

39- Fouad Gamal, Information Crimes, Arab Arbitrators, November 28, 2017, Retrieved Sept 3, 2024, available at the link:<https://almohakmoonalarab.ahlamontada.com/t91-topic>

- 40- Maggie Miller and Lara Seligman, The U.S. is getting hacked. So the Pentagon is overhauling its approach to cyber, politico, dec 9,2023, retrieved June 3, 2024, available at the link:
<https://www.politico.com/news/2023/09/12/pentagon-cyber-command-private-companies-00115206>
- 41- Sabah Kazez, The impact of cybercrimes on the security and stability of countries, Al-Naqid Journal for Political Studies, Vol 2, N 2, October 2018, p 131. Pages 119-144
- 42- Ali Adnan Al-Feel, cybercrime, Zein Legal Publications, Damascus,2011, p 96.
- 43- Mona Al-Ashqar Jabour,Op Cit, p. 85.
- 44- United Nations Crime Office, comprehensive study on cybercrime, United Nations, New York,2013, p 29.
- 45- Reham Abdel Rahman Rashad, The Impact of Cyber Terrorism on Changing the Concept of Power in International Relations, Case Study: The Islamic State Organization, Arab Democratic Center, January 10, 2017, retrieved June 3, 2024, available at the link: <http://democraticac.de/?p=345>
- 46- UniSense Advisory, Cybercrimes On Social Media: The Ultimate Guide, medium, Dec 19, 2023, retrieved June 20, 2024, available at the link:
<https://medium.com/@unisenseadvisory/cybercrimes-on-social-media-the-ultimate-guide-06b329e1e11f>
- 47- Mona Al-Ashqar Jabour,Op Cit, p. 86.
- 48-Muhammad Madian, cybercrime, and national security challenges, Egyptian Publishing and Distribution, Egypt,2019, p 43.
- 49- Iman Al-Hiyari, The Concept of Electronic Warfare, Mawdoo3 website, December 22, 2016, retrieved June 7, 2024, available at the link:<http://mawdoo3.com>
- 50-Muhammad Madian,Op Cit, p 44.
- 51- United Nations Crime Office, comprehensive study on cybercrime, United Nations, New York, 2013, p 329.
- 52-Heru Susanto, Information Security Management Systeme, Apple Academic Press, Canada, 2018, p 217.
- 53- Heru Susanto, Op cit, 240.
- 54- International Telecommunication Union, Securing Information and Communications Networks: Best Practices for Building a Culture of Cybersecurity, Union Publications, Switzerland, 2017, p 13.
- 55- Cameron Coutu, The prevention of cybercrime, Master's degree in criminology, University of Montreal, School of criminology, August 2019, p 42.
- 56-Muhammad Al-Alfi, The Role of Civil Society in Combating Manifestations of Criminal Aggression via the Internet, Al-Minshawi Center for Studies and Research, February 8, 2015, retrieved June 10, 2024, available at the link: <http://www.minshawi.com/other/alfi.htm>
- 57- United Nations Crime Office, Op cit, p 330.
- 58- International Telecommunication Union, Op cit, p 13.
- 59- DavidWicki-Birchler, The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? , International Cybersecurity Law Review, Switzerland, 1(2) ,September 2020, p 70. pp 63-72