Migration Letters

Volume: 20, No: S12 (2023), pp. 1787-1798

ISSN: 1741-8984 (Print) ISSN: 1741-8992 (Online)

www.migrationletters.com

Digital Governance And Risk Reduction Of Cybercrime: A Theoretical Study

Dr: Abbes Midoune[1] , Dr: Youcefi alaeddine[2] , Pr: Ounnoughi Nabil[3]

Abstract:

This study aims to highlight the role of digital governance in mitigating the severity of cybercrime risks. The study adopts a descriptive-analytical approach to understand the concept and objectives of digital governance. It also examines various theoretical perspectives on the concept of cybercrime. Furthermore, the study explores the requirements of digital transformation. Finally, the study focuses on the role of digital governance as a mechanism for successfully reducing the spread of cybercrime risks.

The study has yielded several results, among which international cooperation in the field of information security and the availability of necessary conditions to ensure safe and proper use of information and communication technology stand out. These conditions are instrumental in avoiding the threats posed by cybercrime.

Keywords: *Governance, Digital Governance, Cybercrime.*

Introduction:

The rapid global developments and changes have posed significant challenges in the field of information and communication technology, becoming the foundation relied upon in various sectors of daily life. This rapid advancement has been accompanied by a global trend towards harnessing the benefits arising from the use of digital tec[1]hnology to achieve economic growth, increased productivity, efficiency, enhanced services, and cost reduction.

In parallel with these trends, and with the increasing reliance on modern technology and communication through the growing use of internet-connected applications, electronic and digital media, new patterns of crimes have emerged. These crimes result from the malicious exploitation of technology, giving rise to a new phenomenon previously unknown, known as cybercrime. These crimes encompass various types, ranging from attacks on electronic systems to breaches of information security, as well as fraud and electronic forgery.

Consequently, it has become imperative to adopt policies and strategies that contribute to reducing these crimes, involving both public and private sectors, and engaging the community. The risks associated with information technology are substantial, necessitating the use of security systems to protect against such crimes. This has compelled both advanced and developing societies to seek effective mechanisms for preventing these types of crimes. This involves exploring new approaches that keep up with these evolving dynamics, establishing legal frameworks and agencies to safeguard data, providing guidance to companies and institutions, and establishing official channels to train skilled engineers and technicians. These trained professionals ensure the

[1]University Batna 1, Algeria.
[2]University Center of Barika, Algeria.
[3]University Center of Barika, Algeria.

implementation of digital governance strategies across various sectors while maintaining data security and confidentiality.

Algeria is among the countries that have prioritized enhancing cybersecurity and combating cybercrime amidst digital transformations and the contemporary information revolution. This is done to decode and confront this type of crime, mitigating potential damages and losses.

In light of the above, the importance of utilizing digital governance as a mechanism and approach to curb this type of crime becomes evident. This relies on a set of procedures and measures that work towards early detection, containment, and identification of the sources of these crimes before they occur.

From this perspective, the research paper introduces the following problem:

To what extent can digital governance serve as an effective mechanism for addressing cybercrime?
This attempt to answer that will follow these elements:

- **Different contents of digital governance.**
- **Cognitive frameworks of cybercrime.**
- **Reflections of implementing digital governance on the risks of cybercrime.**

1. Study Methodology:

Such studies require diversity in the use of methodologies to allow for the study and analysis of the subject. Given the nature of our topic, we adopted the descriptive-analytical methodology. We chose to utilize this methodology to describe and present all aspects related to the variables we aim to study the relationship between, namely digital governance and cybercrime. Additionally, we used this method to analyze and interpret certain relationships connecting different parts of the subject.

First - Various Aspects of Digital Governance:

1. Concept of Digital Governance:

Before delving into the concept of digital governance, it's necessary to clarify the concept of governance itself, which is a relatively recent concept in the scholarly arena.

-The topic of governance faced challenges in defining and establishing a precise conception. Therefore, multiple definitions exist. Among these is the World Bank's definition in its well-known 1989 report, which emphasizes that governance is "the manner in which power is exercised in the management of a country's economic and social resources for development."[1]

- The United Nations Development Program (UNDP) defines it as: "The exercise of economic, political, and administrative authority to manage a nation's affairs at all levels."[2]

---

[1] Robert Cameron Orr, **Winning the Peace: An American Strategy for Post-conflict Reconstruction**, Washington, D.C: Center for Strategic & International Studies, 2004, p59.

[2] Robert Cameron Orr, Winning the Peace: An American Strategy for Post-conflict Reconstruction, Washington, D.C: Center for Strategic & International Studies, 2004, p59.

- Governance can be defined as the tools, relationships, and methods related to governing, encompassing the array of relationships between the government and citizens, whether as a comprehensive structure of political, social, and economic institutions.[1]

- The International Finance Corporation defines governance as: "The system by which companies are directed and controlled." The Organization for Economic Cooperation and Development (OECD) defines it as: "The set of relationships between the company's management, its board, its shareholders, and other stakeholders."[2]

- And some define it as: the set of rules and regulations that govern the functioning of organizations, ensure effective management control, regulate the relationship between organizations and various stakeholders, and aim to achieve transparency, fairness, and anti-corruption efforts.

With the multiplicity of definitions of governance ،the characteristics of governance are multiplied according to what was stated in it or defined by the United Nations Development Program in has 8 major characteristics. It is participatory ، consensus oriented ،accountable ،transparent ،responsive ،effective and efficient ، equitable and inclusive and follows the rule of law ،which are shown in the following figure (01):

Figure No. (01) Characteristics of governance



Source: Youssef Azrawal, Righteous Governance in Algeria, Egypt: Al-Wafa Legal Library, 2016, p. 54.

In light of the previous definitions, digital governance can be understood as an extension of governance, serving as a tool to implement these practices through electronic means. This involves utilizing modern technology to enhance effectiveness, speed,

[1] Salima Ben Hussein, Governance: A Study of the Concept, Journal of Legal and Political Sciences, University of Shahid Hamma Lakhdar El Oued, Algeria, Issue 10, 2015, p. 183.

[2] Zainab Yahyawi, Electronic Governance: An Introduction to Quality Public Service, Journal of Intellectual Excellence for Social and Human Sciences, Al-Tarf University, Algeria, Issue 08, 2021, p. 64.

transparency in the performance of governmental activities, and the dissemination of information to the public and other institutions.

Meanwhile, according to UNESCO, digital governance is defined as: the use of information and communication technology in the public sector to improve service delivery, encourage citizen participation in decision-making, and make the government more accountable, transparent, and efficient.[1]

Backus defines it as the application of electronic means in interactions between the government and citizens, government and organizations, as well as various internal governmental processes, to enhance democracy, governance, and other functions.

On the other hand, Heeks defines digital governance as the use of information and communication technology to support governance.[2]

Therefore, it can be said that digital governance is the utilization of modern technologies, information, and communication technology to achieve the goals and principles of governance. This involves transforming institutional information content into digital content that supports the information technology infrastructure.

2. Justifications for Transition to Digital Governance:

The most important justifications for transitioning to digital governance can be summarized as follows:[3]

- Increasing pressures on governments to efficiently meet the needs and desires of citizens, especially with growing populations and living standards.
- Escalating complexities faced by individuals dealing with various government service sectors, primarily bureaucratic procedures, routines, and slow service delivery.
- Technological advancement and the rapid information revolution, along with a strong determination to apply them to enhance governmental performance.
- Enhancing citizen involvement in monitoring, accountability, and decision-making processes.
- Reducing the cost of governmental procedures.
- Transparency in procedures.
- Improving the quality of services provided through digital governance.

3. Significance and Objectives of Digital Governance:

The significance and objectives of digital governance can be summarized as follows:

Importance of Digital Governance: The importance of digital governance lies in the following points:[4]

- The existence of laws and frameworks governing the design and launch of electronic services.
- Uniformity in building e-government systems within governmental institutions.
- Limiting deviations of administrations and institutions from general guiding plans issued by the authority responsible for managing digital governance.
- Ability to provide high-quality services and measure the extent of their acceptance by the target audience.
- Achieving the highest levels of efficiency, transparency, and accountability by integrating and harmonizing government services provided by all entities.

---

[1] Souad Moghadam, Requirements for Activating Electronic Governance in Modern Administrative Organizations, Concepts and Application Mechanism, Journal of Intellectual Excellence for Social and Human Sciences, Al-Tarf University, Algeria, Issue 08, 2021, p. 32.

[2] Heeks Rebuilding, e-governance for Development Aframe work for National and Donor Action i- Government Working Paper Series, 2001, N12, p02.

[3] Muqaddam Souad, previous reference, pp. 34, 35.

[4] Rania Tanah, Safia Boumsbah, previous reference, p. 58.

- Facilitating oversight and supervision over institutions' performance through defining frameworks for internal control.
- Adopting digital governance methods saves effort, time, and resources for all parties involved.
- Fostering an advanced society that keeps pace with the digital age and deals with various new technological data.

Objectives of Digital Governance: Digital governance aims to achieve a set of objectives, which can be summarized as follows:[1]

- Facilitating and enhancing the internal workings of institutions through interaction encouragement, improved decision-making processes, and citizen participation.
- Efficiently managing public services for the benefit of employees, both public and private, and citizens.
- Providing better information and delivering higher-quality services.
- Achieving transparency to reduce and mitigate corruption.
- Enhancing credibility and political responsibilities.
- Promoting democratic practices through participation, consultation, and information exchange with citizens, institutions, and governmental administrations.
- Delivering public services faster and more efficiently.

4. Requirements for Achieving Digital Governance:

The transition to digital governance is a complex and gradual process that takes considerable time. Successfully achieving this process requires meeting a set of conditions, which can be summarized as follows:[2]

Administrative Support: The conviction, interest, and backing of top management in applying information technology within organizations are crucial factors that contribute to the success of implementing digital governance.

Communication Infrastructure and IT Resources: The success of digital governance requires supportive information technology. This, in turn, necessitates the availability of communication infrastructure and financial budgets provided by the government.

Legislation: To effectively implement digital governance, it is essential to legislate its processes, specify its requirements, allow for inter-institutional collaboration, and emphasize privacy and information security.

Human Resources: As governments increasingly transition to providing services electronically, there's a growing need for specialized human resources in information technology. This places the public sector in a competitive challenge to acquire these resources.

Security and Privacy: Security encompasses measures, policies, and technical standards used to prevent unauthorized access to networks, tampering with their contents, or stealing and managing information within their systems. Privacy involves maintaining the

[1] Yassi Elham, Culture as a Key to the Success of Electronic Governance, Al-Manhal Economic Journal, Volume 03, Issue 02, 2020, p. 334.

[2] Tilly Maryam, Electronic governance as a mechanism for improving the quality of health services -with reference to the Algerian experience, Journal of Social Responsibility Governance and Sustainable Development, Volume 03, Issue 02, 2021, pp. 60, 61.

confidentiality of individuals' information stored in digital governance systems and preventing unauthorized access by others.

Secondly - Conceptual Framework of Cybercrime:

1. Concept of Cybercrime:

Cybercrime has gone through various terminologies over time, starting with terms like "misuse of computers," "computer fraud," "cybercrimes," "high-tech crimes," "hacks," "internet crimes," and finally "cybercrimes." Cybercrime refers to all activities with criminal intent in the cyberspace, targeting three categories: individuals, commercial and non-commercial organizations, and governments. It is also defined as any intentional criminal act, regardless of its connection to information technology, resulting in losses for victims or gains for perpetrators. The United Nations defines cybercrime as all unlawful activities that utilize electronic operations to target the security of information systems and the data they handle. Algerian legislation defines cybercrime as "crimes affecting computer processing systems specified in the Penal Code and any other crimes that are committed or facilitated through an information system or communication system."

2. Causes of Cybercrime Spread:

The main reasons behind the spread of cybercrimes include:
Material Motives: The desire to achieve wealth is a major driving factor behind committing cybercrimes. Some individuals are motivated to rapidly acquire wealth by providing unauthorized access to critical information that others seek.
Revenge Motives: Revenge is a significant motivator for committing cybercrimes. Individuals who possess extensive knowledge about an organization or company might resort to cybercrimes as a form of revenge due to personal grievances, such as being terminated from employment or facing discrimination and non-promotion.
Personal Motives: Often, cybercriminals are driven by a desire to prove themselves, asserting superiority over information technology, and portraying themselves as intelligent and worthy of admiration, rather than as criminals who deserve prosecution. These individuals are primarily driven by curiosity rather than financial gain and do not have malicious intentions.
Desire for Learning: Some individuals engage in cybercrimes to learn more about rapidly evolving technology and to explore forbidden areas of the internet. They prefer to remain anonymous for as long as possible to continue learning about hacking prohibited websites and computer security techniques.
Political Motives: These motives involve defending specific ideologies or viewpoints, leading to cyberterrorism and criminal acts against political opponents.
Threat and Competition: This motive emerges from external pressures and threats in areas such as business and private sectors. Espionage and competition might compel individuals to engage in cybercrimes in an attempt to discover competitors' secrets.

In addition to the above, researchers **Serkan Savaş & Süleyman Karataş** point out that today there are problems that the information law cannot fully solve, which **have exacerbated the spread of Cybercrime**. The main ones include the following: [1]

- ✓ Problems in commercializing electronic data.
- ✓ Responsibility of search engines and problems in internet law.

---

[1]- For further information, please refer to:
- Serkan Savaş & Süleyman Karataş, "Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance", **International Cybersecurity Law Review**, N°2, Int. Cybersecure, June 2022, p p 09, 10.
- Murat Volkan Dulger, "Regulations in the Council of Europe and European Union Regulations Against the Spread of Child Pornography Through the Interne", **Journal of the Istanbul Bar Association**, Istanbul, no 4, 2004, pp1485–1496.

- ✓ Problems with the formation of the internet censorship network.
- ✓ Increase in crimes committed through social media.
- ✓ New generation peer bullying—the increase in cyberbullying.
- ✓ Failing to protect personal information in the digital environment.
- ✓ Violation of privacy and unauthorized access.
- ✓ There is no consensus on the definition and content of cybercrime، and classic criminal law is inadequate.
- ✓ With the widespread use of the internet، the common legal understanding determined by physical borders between countries is insufficient.
- ✓ There is no consensus on ethical rules in the digital world regarding intellectual property، user privacy، and information integrity.
- ✓ The technical، application، and legislative infrastructure of the e-signature is insufficient.
- ✓ Failure as yet to develop forensic informatics as an independent scientific discipline.
- ✓ The inability to prevent offenders from using computer systems for crimes such as money laundering and financing of terrorism through technology and the internet.
- ✓ Failing to prevent international cyber operations that cause all manner of rights violations.

3. Characteristics of cybercrime:

Cybercrime is characterized by a set of characteristics, including the following:[1]

Crimes committed by means of electronic devices such as computers and cell phones: the two tools that enable the criminal to enter the Internet to carry out the crime.

Cybercrime is a cross-border crime: information crime is a form of cross-border crime, so the crime survey is no longer local, but has become global, as the agent is not physically present at the crime scene, so the perpetrator can carry out his crime by entering the memory of the computer located in another country, this act is to meet a third person who is in another country.

Difficulty detecting and proving cybercrime: These crimes are characterized by the difficulty of detection and proof, because the offender does not leave traces of his criminality. In his right.

Rapidly executed crimes: the speed of committing the crime may be within a fraction of a second, and may not require preparation before execution.

Soft crimes: They are crimes that do not practice violence, and do not require the slightest muscular effort, unlike some traditional crimes.

4. The nature and forms of cybercrimes:

Cybercrimes are classified into two parts: the first section targets computers and information networks such as viruses, and the other section targets internet users and cyberspace pioneers, including individuals, economic institutions, and government ministries, including cyberbullying, phishing, social engineering, and other forms, which are as follows:[2]

Viruses: They are malicious computer programs that transmit between computers in several ways, and multiply depending on other files. There are several types of viruses, some of which start at a specific time or incident, and some that are composed of multiple parts, and some that change their characteristics periodically, and some that are hidden until Anti-virus software, which causes great damage to the information environment and may destroy all files on storage media, or replace information with meaningless ones.

---

[1] Rawan bint Atiyatullah, journalist, cybercrimes, comprehensive multidisciplinary electronic magazine, issue 24, 2020, p. 11.

[2] Tiwari, S, Bhalla A, & Rawat, Cyber-Crime and Security, International journal of advanced research in. computer Science and Software engineering, 2016, P47.

Cyberbullying: Cyberbullying is one of the most prevalent forms of cybercrime, especially among school students at all educational levels, and it takes many forms, including: abuse and threats of harm, slander, slander and contempt, sending immoral pictures and videos, stealing and hacking personal accounts, broadcasting hate speech Defamation, intimidation, blackmail...

Social engineering: This form of cybercrime has become popular recently due to the widespread and rapid spread of social networks. Social engineering aims to focus on hacking minds instead of focusing on computers and information networks.

Defamation: It means defaming a person in cyberspace by publishing incorrect information with the aim of offending and degrading him. Defamation includes publishing pictures of the targeted person via social media or via e-mail after modifying them by digital design programs to serve the goals of the attacker.

Hacking: It is the process of entering into information systems by experienced people, usually programmers who are not allowed to enter those systems in order to break the security barriers surrounding them.

Phishing: It is considered one of the easiest cybercrimes for cybercriminals, and it only requires them to create a website and send messages via e-mail, to appear as if they were sent from companies known to the victims, and in this way, they can obtain some bank account details, credit card numbers or some Personal details.

Grooming or enhancement: This type of cybercrime means an adult interested in sexual exploitation of children tries to establish a friendship with a child or adolescent under eighteen years of age, and the attacker pretends at the beginning of contact that he is young and shares the same interests with the child he communicates with, so that the relationship develops Between them until he gains the confidence of the child to push him to send sexual images, and the matter may develop into direct sexual encounters between the two parties.

Although new studies have been carried out in the field of Information and communication technology to overcome these problems، these studies have many theoretical، technical، and structural deficiencies. Cyber domains cover issues in all areas of civil society، military، social security، politics، economy، culture، technological development، security، and mobile technologies. For the management of all these different kinds of challenges، comprehensive rules must be found; written standards must be set and generally accepted. All New actors (government، private sector، citizen، civil society organizations) should be involved in these processes and all employees in public and private institutions should grasp the importance of governance concepts. The elimination of Cybercrime risks is possible with the implementation of a strategy effective It is based on the concept of digital governance. Although the area covered by the concept of digital governance is Developing digital services in all government institutions، the most important component of this concept is Human resource. Users should distinguish between security and insecurity in cyberspace and have technology literacy. Whether they are professional (business) users or personal users، all individuals are important for to activate the various criteria of digital governance (transparency، accountability، efficiency and effectiveness، dedication of the law، Participation...).

Third: The implications of the application of digital governance on the risks of cybercrime:

The role of digital governance in reducing the risks of cyber-attacks can be observed through four main axes:[1]

Axis One: Digital governance is based on three pillars, the first of which is: the basic dimensions of implementing digital transformation, which include the financial and administrative structure of the activities, operations, and departments of the institution, the engineering of operational processes to identify the processes that add value and exclude the processes that do not add value, and determine the form and quality of the final outputs, and the formulation and adoption of reverse feedback components, while the second pillar deals with the requirements and components of the success of digital governance in terms of (domination of the concept of effective digital management, availability of adequate and appropriate financial budget, selection of best digital practices, and building and adopting indicators for evaluating digital performance), and finally, the third pillar includes the axes of security and privacy in terms of (ensuring the confidentiality of data and information, formulating and adopting standards of digital safety and accuracy, ease of data and information exchange through digital and government platforms).

Axis Two: It deals with the implications of the application of digital governance on the success of digital transformation strategies, through the promotion of the use of new technologies and techniques such as (artificial intelligence systems, big data analysis, computing technologies...), as well as the changes in creating added value for activities, operations, and individuals, structural changes and electronic infrastructure, enhanced financial aspects in terms of the availability of liquidity needed to implement digital transformation strategies, equip the electronic infrastructure, train individuals, purchase devices and software, and launch digital platforms, and finally, cybersecurity requires the existence of effective local and international partnerships, supported by advanced mechanisms for sharing information; so that it can develop and improve continuously, and share best practices, investigative information, and necessary measures. In addition to its high importance in keeping pace with threats, reducing risks. And reaching the desired degree of cooperation, and strengthening partnerships, and building channels for sharing information within and outside institutions, contribute to sharing information related to cybersecurity.

Axis Three: The success of digital governance contributes to achieving many advantages, especially the speed of providing products and services and the relative decrease in costs, ensuring the quality of operations and services provided to citizens, strengthening control and accountability processes for employees and officials by regulatory and supervisory authorities, as well as enhancing levels of disclosure and transparency through the provision of timely and suitable information through digital platforms for decision-makers.

Axis Four: This axis includes controls and standards for enhancing cybersecurity, as the success of the application of digital governance depends on the standards and controls that institutions adopt and implement them properly, the most important of which are: network security management standards, management of tangible and intangible assets, mechanisms for protecting systems and information processing devices, event management methodology and monitoring of the risks of cyber-attacks, and data and information protection and encryption models, which ensure the quality of government operations, products, and services and the reduction of cybercrime attacks.

---

[1] Look:

- Muhammad Fawzi Amin Al-Bardan, Muhammad Musa Ali Shehata, "Digitization Strategies to Reduce the Risk of Cyberattacks in the Egyptian Environment," a presentation presented during the Third International Conference on Digitization and Quality Assurance of Higher Education, Egypt: Sadat City University, October 2-3, 2012, pp. 14, 15.
- National Cybersecurity Authority, National Cybersecurity Strategy, Kingdom of Saudi Arabia, December 2020, p. 29.

Security, efficiency, and accountability are institutional context standards, according to Dr. Ali Mohammed Al-Khouri in his book "Digital Government: Concepts and Practices." He believes that digital identity systems can meet essential requirements in digital governance projects in the institutional context Organization Context. Here are some of them:[1]

Digital signature and encryption services: Security and reliability are essential aspects for building trust in digital government platforms. Digital identity systems play a central role as a component in the public basic infrastructure for securing transactions by providing advanced technologies such as "encryption and digital signature." With the existence of such advanced government systems, they can be used by service providers from government institutions and business sectors without having to incur additional costs and duplicate projects to build a different infrastructure to confirm identity and secure digital transactions.

Control of access points to electronic systems: this includes updating access control systems to computers, networks, files, and other sensitive data. Digital identity systems can be relied upon as a way to unify identification mechanisms and grant access permissions to networks and information systems.

Control of access points to physical systems: this includes updating access control systems to government buildings, facilities, and physical assets. Here too, modern systems such as digital identity and smart identity card can be used as a reliable and trusted mechanism, especially in the field of employing the advanced features of these systems such as biometric fingerprints and encryption infrastructure.

Based on these sample tasks، the scope and framework of policies digital governance that should be implemented in order to mitigate the risks of cybercrime can be drawn. **The digital governance policies to be determined should be within the following scope:** [2]

It must be generally valid: The determined policies must be valid for all institutions, individuals, and devices in cyber environments. Since all individuals, institutions, and devices are included in the elements that make up cyber environments, the policies that bring them together should have general validity.

It must be adaptable: The policies determined should be adaptable to the issues in the sub-domain of cyber environments (e.g., CS، cloud computing، IoT، etc.). The number of components in cyber environments is continuously increasing and therefore new subset areas are constantly being formed. In this rapidly developing digital world، instead of frequently updating the policies.

It must be participatory: It is necessary to provide participants representing all of the public، private sector، and individual users to the policies to be determined.

It must be inclusive: The policies determined should be policies that cover all institutions، organizations، and users—and not a single group.

It must be binding: Digital governance procedures and policies must be binding against all elements using cyber environments and must be able to impose sanctions. Sanctions are also needed for the determined policies to be accepted and binding. Just as certain sanctions are applied to ensure the applicability of real-life rules، similarly، sanctions will be needed to carry out policies in cyber environments. For this reason، while the studies are carried out، not only the rules should be established، but also the sanctions to be applied to adhere to them should be planned. These sanctions can range from limiting access to real-life fines and prison sentences. For this، national and international patrols can be established. Real-life security forces can be adapted to digital environments and

---

[1] Ali Muhammad Al-Khoury, Digital Government: Concepts and Practices, Egypt: Arab Administrative Development Organization, 2021, pp. 210, 212.

[2] For further information, please refer to:

- Serkan Savaş & Süleyman Karataş, **Op. Cit**., p p 29,30.
- Serkan SAVAŞ, Nurettin TOPALOGLU, Osman GULER, "Determination of Preferences: A Questionnaire Application", Journal of Information Technologies, vol. 8, no 2, Gazi University, Turkey, 2015, p 51.

the framework of existing teams can be expanded. In fact، artificial intelligence and machine learning algorithms can be used for these processes.

The scope of the framework to be determined for digital governance can be expanded to cover the basic elements above، and the content of each scope item can be determined with more precise lines.

Conclusion:

Confronting the repercussions of cybercrime is one of the most difficult challenges that requires concerted efforts, especially since the use of this technology is constantly increasing in managing various security, economic and military affairs, which requires cooperation between countries in the field of information security and confronting the risks of cybercrime.

On this basis, Algeria, like other developing countries, has become forced to enter into technology-based digital governance in various areas and fields, and therefore it has become necessary to provide the necessary conditions to ensure the safe and proper use of information and communication technology, in order to avoid the risks and threats of cybercrime that could have effect on various economic, social, political, cultural, religious and even individual dimensions.

The most important recommendations that we can provide to reduce the effects of cybercrime are the following points:

- It is necessary to establish rapid procedural rules commensurate with the speed of cybercrime in order to facilitate the provision of evidence and identify and prove its perpetrators.
- Working to manage the risks of cyber-attacks in a systematic manner aimed at protecting information and technical assets, in accordance with regulatory policies and procedures and legislative requirements.
- The need for the management of institutions to maximize the benefit of digital governance in building databases and digital platforms that contribute to processing, analyzing and managing data well as a guarantee to reduce the risks of cyber-attacks.
- Increase investment in electronic infrastructure by devoting financial and human capabilities to address this phenomenon.
- Intensifying training and training courses and benefiting from the experiences and expertise of developed countries to combat various manifestations of cybercrime.

List of sources and references:

- Robert Cameron Orr, Winning the Peace: An American Strategy for Post-conflict Reconstruction, Washington, D.C: Center for Strategic & International Studies, 2004.
- Robert Cameron Orr, Winning the Peace: An American Strategy for Post-conflict Reconstruction, Washington, D.C: Center for Strategic & International Studies, 2004.
- Salima Ben Hussein, Governance: A Study of the Concept, Journal of Legal and Political Sciences, University of Shahid Hamma Lakhdar El Oued, Algeria, Issue 10, 2015.
- Zainab Yahyawi, Electronic Governance: An Introduction to Quality Public Service, Journal of Intellectual Excellence for Social and Human Sciences, Al-Tarf University, Algeria, Issue 08, 2021.
- Souad Moghadam, Requirements for Activating Electronic Governance in Modern Administrative Organizations, Concepts and Application Mechanism, Journal of Intellectual Excellence for Social and Human Sciences, Al-Tarf University, Algeria, Issue 08, 2021.
- Heeks Rebuilding, e-governance for Development Aframe work for National and Donor Action i- Government Working Paper Series, N12, 2001.
- Yassi Elham, Culture as a Key to the Success of Electronic Governance, Al-Manhal Economic Journal, Volume 03, Issue 02, 2020.
- Tilly Maryam, Electronic governance as a mechanism for improving the quality of health services -with reference to the Algerian experience, Journal of Social Responsibility Governance and Sustainable Development, Volume 03, Issue 02, 2021.

- Serkan Savaş & Süleyman Karataş, "Cyber governance studies in ensuring cybersecurity: an overview of cybersecurity governance", International Cybersecurity Law Review, N°2, Int. Cybersecure, June 2022.
- Murat Volkan Dulger, "Regulations in the Council of Europe and European Union Regulations Against the Spread of Child Pornography Through the Interne", Journal of the Istanbul Bar Association, Istanbul, no 4, 2004.
- Rawan bint Atiyatullah, journalist, cybercrimes, comprehensive multidisciplinary electronic magazine, issue 24, 2020.
- Tiwari, S, Bhalla A, & Rawat, Cyber-Crime and Security, International journal of advanced research in. computer Science and Software engineering, 2016.
- Muhammad Fawzi Amin Al-Bardan, Muhammad Musa Ali Shehata, “Digitization Strategies to Reduce the Risk of Cyberattacks in the Egyptian Environment,” a presentation presented during the Third International Conference on Digitization and Quality Assurance of Higher Education, Egypt: Sadat City University, October 2-3, 2012.
- National Cybersecurity Authority, National Cybersecurity Strategy, Kingdom of Saudi Arabia, December 2020.
- Ali Muhammad Al-Khoury, Digital Government: Concepts and Practices, Egypt: Arab Administrative Development Organization, 2021.
- Serkan SAVAŞ, Nurettin TOPALOGLU, Osman GULER, "Determination of Preferences: A Questionnaire Application", Journal of Information Technologies, vol. 8, no 2, Gazi University, Turkey, 2015.