Ministry of Higher Education and Scientific Research

Higher National School of Management
Kolea

وزارة التعليم العالي و البحث العلمي

المدرسة الوطنية العليا للمناجمنت
القليعة

DISSERTATION

Fulfillment of the requirements for the Professional Master's Degree in Electronic Government

Theme:

The Role of Cybersecurity in e-government services

Case study: Research center of the information and technical information (CERIST)

Prepared by

Mr. BENAISSA Islam

Supervised by

Dr. MOHAMMED ELHADJ Leila

Members of jury

President: Dr.Adnani Khawla

Examiner: Dr.Bokreta Naoual

2023/2024

ABSTRACT

In the digital era, e-government services, which leverage electronic means to deliver public services, are increasingly vital for enhancing efficiency, transparency, and accessibility in governmental operations. However, these services also pose significant cybersecurity challenges due to the sensitive nature of the data involved. This study examines the crucial significance of cybersecurity in the context of e-government services, with a specific focus on a case study of the Research Centre for Scientific and Technical Information (CERIST) in Algeria, The dissertation explores the current dynamics of cybersecurity in e-government, highlighting the risks, threats, and strategic measures necessary to safeguard these digital infrastructures. Through a qualitative approach that includes document analysis and semi-structured interviews with key stakeholders, this research identifies the existing cybersecurity practices at CERIST and proposes improvements to ensure the security and resilience of e-government services. The findings underscore the importance of robust cybersecurity measures, comprehensive legal frameworks, and continuous stakeholder collaboration to protect against cyber threats and maintain public trust in digital government services.

Key words: Cybersecurity, E-government services, Digital infrastructure, Data protection, CERIST, Cyber threats, Legal frameworks, Information security.

الملخص

في العصر الرقمي، أصبحت خدمات الحكومة الإلكترونية، التي تعتمد على الوسائل الإلكترونية لتقديم الخدمات العامة، ذات أهمية متزايدة لتعزيز الكفاءة والشفافية وإمكانية الوصول في العمليات الحكومية. ومع ذلك، تواجه هذه الخدمات أيضًا تحديات كبيرة في مجال الأمن السيبراني بسبب الطبيعة الحساسة للبيانات المتضمنة. تتضمن هذه الدراسة الأهمية الحاسمة للأمن السيبراني في سياق خدمات الحكومة الإلكترونية، مع التركيز بشكل خاص على دراسة حالة المركز الوطني للبحث في المعلومات العلمية والتقنية (CERIST) في الجزائر. تستكشف الأطروحة الديناميكيات الحالية للأمن السيبراني في الحكومة الإلكترونية، مسلطة الضوء على المخاطر والتهديدات والتدابير الاستراتيجية اللازمة لحماية هذه البنية التحتية الرقمية. من خلال نهج نوعي يتضمن تحليل الوثائق والمقابلات شبه المنظمة مع الأطراف المعنية الرئيسية، تحدد هذه البحث الممارسات الحالية للأمن السيبراني في CERIST وتقترح تحسينات لضمان أمن ومرونة خدمات الحكومة الإلكترونية. تؤكد النتائج على أهمية التدابير القوية للأمن السيبراني، والأطر القانونية الشاملة، والتعاون المستمر بين الأطراف المعنية لحماية ضد التهديدات السيبرانية والحفاظ على ثقة الجمهور في الخدمات الحكومية الرقمية.

الكلمات المفتاحية: الأمن السيبراني، خدمات الحكومة الإلكترونية، البنية التحتية الرقمية، حماية البيانات، CERIST, التهديدات السيبرانية، الأطر القانونية، أمن المعلومات.

RESUMÉ

À l'ère numérique, les services de gouvernement électronique, qui utilisent des moyens électroniques pour fournir des services publics, sont de plus en plus essentiels pour améliorer l'efficacité, la transparence et l'accessibilité des opérations gouvernementales. Cependant, ces services posent également des défis importants en matière de cybersécurité en raison de la nature sensible des données impliquées. Cette étude examine l'importance cruciale de la cybersécurité dans le contexte des services de gouvernement électronique, en se concentrant spécifiquement sur une étude de cas du Centre de Recherche sur l'Information Scientifique et Technique (CERIST) en Algérie. La thèse explore la dynamique actuelle de la cybersécurité dans le gouvernement électronique, en mettant en évidence les risques, les menaces et les mesures stratégiques nécessaires pour protéger ces infrastructures numériques. Grâce à une approche qualitative comprenant l'analyse de documents et des entretiens semi-structurés avec les principales parties prenantes, cette recherche identifie les pratiques de cybersécurité existantes au CERIST et propose des améliorations pour garantir la sécurité et la résilience des services de gouvernement électronique. Les résultats soulignent l'importance de mesures robustes de cybersécurité, de cadres juridiques complets et de la collaboration continue entre les parties prenantes pour se protéger contre les menaces cybernétiques et maintenir la confiance du public dans les services gouvernementaux numériques.

Mots-clés : Cybersécurité Services de gouvernement électronique, Infrastructure numérique, Protection des données, CERIST, Menaces cybernétiques, Cadres juridiques, Sécurité de l'information.

ACKNOWLEDGMENTS

I would like to start by expressing my deepest gratitude to Allah, the Almighty, for His boundless blessings and guidance throughout this journey. His unwavering support and grace have been fundamental in the successful completion of this thesis.

I am deeply indebted to my Mom, Dad, and siblings for their unconditional love, encouragement, and steadfast belief in my abilities. Their unwavering support and sacrifices have provided me with immense strength and motivation throughout this journey.

I would like to extend my heartfelt appreciation to my beloved family for their unwavering love, encouragement, and continuous support. Their words of wisdom and steadfast faith in me have been a guiding light throughout this journey.

I am profoundly grateful to my supervisor, Dr. ***MOHAMMED ELHADJ Leila***, for her invaluable guidance, support, feedback, and mentorship, I am deeply appreciative of the time and effort you have invested in my work and in me.

I am grateful to ***Pr. MOKHTARI Lazhar*** and my internship supervisor, ***Ms. BOUDER Hadjira***, for giving me the chance to carry out my research in the most favorable conditions. I cherished the dynamic and challenging environment you established for me.

A particular thank you to my close friends of Red Tribe Abdelhak, Lyes, Dhiaa elhak, Redha who supported me mentally and emotionally as I worked on my dissertation. This process has been less intimidating and more fulfilling thanks to their support, encouragement, and camaraderie. I am truly thankful for your unwavering support and friendship.

To my friends Minet Allah, Oussama, Nazih, abdessamed, Mohammed, Hakim, Lyes, Aymen, Imad, Achour, Moncef, Boudi, Ayoub, Brahim Chaima Words cannot express the depth of my gratitude for you.

Finally, I would want to express my gratitude to all of our friends, family, instructors, and staff at the National High School of Management who have supported us, whether directly or indirectly.

Last but not least, I wanna thank me for believing in me I wanna thank me for doing all this hard work I wanna thank me for having no days off, I wanna thank me for, for never quitting.

Table of Contents

LISTE OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

E-government: electronic government

CERIST: Research Centre for Scientific and Technical Information

ICT: Information and Communication Technologies

EGDI: E-Government Development index

EPI: E-participation Index

CISCO: Computer Information System Company

EGMMs: e-government maturity models

GDPR: General data protection regulation

HIPPA: Health Insurance Portability and Accountability

AI: Artificial intelligence

ML: Machine learning

DDos & Dos: Distributed denial-of-service and denial-of-service

DNS: Domain Name System

ARN: Algerian Research Network

CIS: Center for internet security

FISMA: Federal Information Security Management

ITIL: Information Technology Infrastructure Library

EDPB: European data protection board

INTRODUCTION

Introduction

E-government, usually known as the use of electronic methods by governments to provide public services, is becoming more prevalent in the digital era. E-government is a revolutionary method of managing public administration that utilises technology to simplify procedures, improve the provision of services, and promote increased interaction between governments and citizens. The use of e-government holds the potential for a multitude of advantages, such as enhanced efficacy, openness, and availability of governmental services. (Heeks, 2006)

An inherent benefit of e-government is its capacity to enhance the efficiency of governmental procedures. E-government can achieve considerable time and resource savings by digitising information and automating operations. This enhanced efficiency not only reduces operational expenses but also expedites the provision of services, granting citizens quicker and more convenient access to public services. (Jaeger & Bertot, 2010)

E-government has the important advantage of transparency. Digital platforms can enhance transparency by providing easy access to information for the general public. This level of transparency serves as a means to prevent corruption, enhance accountability, and foster confidence between governments and their constituents. Online portals can offer immediate reports on government spending, enabling citizens to oversee the use of public cash. (Bertot, Jaeger, & Grimes, 2010)

E-government projects significantly improve accessibility as well. Digital services have the capacity to extend their reach to a wider demographic, encompassing individuals residing in distant or underserved regions who may otherwise encounter restricted availability to government offices. Online platforms offer round-the-clock availability to services, eliminating constraints associated with time and place. This inclusivity guarantees that a greater number of residents can reap the advantages of government programmes and services. (West, E-Government and the Transformation of Service Delivery and Citizen Attitudes, 2004)

As these services increasingly depend on digital infrastructure, the importance of strong cybersecurity measures becomes crucial. Securing e-government systems is crucial not only for safeguarding sensitive data but also for upholding public confidence and ensuring the uninterrupted functioning of vital services. E-government cybersecurity encompasses safeguarding digital resources against a range of hazards, such as cyber assaults, data breaches,

and other malevolent actions. Due to the sensitive nature of the information managed by government systems, such as personal data, financial records, and national security information, it is crucial to prioritise strong cybersecurity measures. (Anderson & Moore, 27-29)

Implementing cybersecurity measures is crucial to protect the confidentiality, integrity, and availability of e-government services. Confidentiality entails safeguarding sensitive information from unauthorised access. Integrity maintains the accuracy and integrity of data, preventing any unauthorised tampering. Availability, on the other hand, ensures that services are consistently accessible and operational as required. An infringement in any of these domains can result in significant ramifications, encompassing identity theft and monetary detriment, as well as the disturbance of essential public services and erosion of public confidence. (Pfleeger, 2002)

Furthermore, the incorporation of cybersecurity into e-government systems extends beyond the mere implementation of technical remedies. It also entails the creation of extensive laws, legal structures, and optimal methods that regulate the safeguarding of digital assets. These frameworks need to be flexible in order to adapt to changing threats and technology, thus ensuring the long-term security of e-government systems. (Dunleavy, Margetts, Bastow, & Tinkler, 2006)

Cybersecurity plays a diverse role in e-government, involving the creation of secure infrastructures, the adoption of protective measures, and the ongoing monitoring and updating of security procedures. It additionally entails cooperation among diverse stakeholders, such as government agencies, corporate sector allies, and individuals, in order to establish a robust cyber environment. (NASCIO, 2016)

To summarise, the implementation of e-government provides substantial advantages in terms of effectiveness, openness, and availability. However, it also introduces fresh obstacles concerning cybersecurity. Tackling these obstacles is essential for the effective execution and long-term viability of e-government projects. This thesis seeks to investigate the present dynamics of cybersecurity in e-government and provide methods to improve the security and resilience of digital public services. (Weerakkody & Dhillon, 2008)

Research problem and questions

To address the problem statement effectively, this thesis is guided by the following research questions. These questions are designed to explore the various dimensions of cybersecurity in e-government services and provide a comprehensive understanding of the challenges and solutions in this domain:

What role does cybersecurity play in influencing the overall effectiveness and trustworthiness of e-government services?

Problem Statement

The rapid expansion of e-government services has outpaced the development of corresponding cybersecurity measures, leading to vulnerabilities that can be exploited by cyber attackers. This gap poses a significant risk to the security and functionality of e-government systems. Therefore, it is essential to investigate the current state of cybersecurity in e-government and identify strategies to enhance it.

Research Questions

1. What are the primary cybersecurity challenges faced by e-government systems?
2. How can cybersecurity measures be effectively integrated into e-government architectures?
3. What roles do various stakeholders play in ensuring the cybersecurity of e-government services?

Significance of the study

This study is significant because it focuses on the crucial role of cybersecurity in the effective implementation and long-term viability of e-government services. The project seeks to improve

the security, efficiency, and dependability of digital public services by examining cybersecurity concerns and integration techniques. Implementing strong cybersecurity protections is crucial for safeguarding sensitive information, such as personal data and financial records, in order to prevent identity theft and financial fraud.

Furthermore, this study aims to provide policymakers and IT professionals with valuable insights on the most effective methods and structures for incorporating cybersecurity measures into e-government systems. The research will assist in creating thorough cybersecurity policies and regulatory frameworks that protect digital infrastructure by offering practical suggestions. Another important result is the improvement of public confidence through the implementation of secure e-government services. When citizens have confidence that their data is safeguarded, they are more inclined to use digital platforms.

Ultimately, this work enhances the existing scholarly understanding of cybersecurity and its relationship to e-government. By tackling emerging cyber dangers and fostering interdisciplinary collaboration, it facilitates the advancement of robust e-government systems. This research is of great significance not only for governments and policymakers, but also for scholars and students who have a keen interest in the domains of cybersecurity and digital governance.

Methodology

This study utilises a qualitative research design to investigate the intricacies of cybersecurity in e-government services. A qualitative approach is used due to its capacity to offer comprehensive insights into the experiences, perceptions, and practices of different stakeholders engaged in e-government cybersecurity. The research will utilise case studies, interviews, and content analysis to collect extensive data on the subject. This methodology enables a comprehensive analysis of the particular cybersecurity obstacles and the tactics utilised to tackle them in various e-government scenarios. (Creswell J. W., 2014)

The main focus of this research will be on the research centre of scientifical technical information (CERIST) in Algeria. The organisational history of CERIST and its involvement in e-government services offer a pertinent framework for examining cybersecurity concerns and

solutions. The case study will entail a comprehensive analysis of CERIST's cybersecurity policies, practices, and incidents. This contextual emphasis enables a detailed comprehension of how cybersecurity is controlled in a particular organisational and national environment, providing significant insights that can be applied to other e-government systems. (Yin, 2017)

The data will be gathered through a blend of semi-structured interviews, document analysis, and direct observation. Key stakeholders at CERIST, such as IT experts, policymakers, and employees involved in cybersecurity, will be interviewed using a semi-structured approach. The interviews will offer direct and personal narratives on the difficulties and tactics associated with cybersecurity. The process of document analysis will entail the examination of CERIST's internal policies, incident reports, and cybersecurity frameworks. Observing directly will provide valuable understanding of the day-to-day procedures and operational elements of cybersecurity at CERIST. The utilisation of several data sources in this triangulation process guarantees a thorough and dependable comprehension of the research subject. (Merriam & Tisdell, 2015)

Thematic analysis will be conducted on the collected data to discover recurring patterns and themes pertaining to cybersecurity problems and practices in e-government. Thematic analysis entails the process of categorising the data and organising the codes into themes that accurately represent the main topics and approaches discovered throughout the investigation. This approach enables a comprehensive analysis of the qualitative data, emphasising the subtle and nuanced experiences and viewpoints of the respondents. The results obtained from the thematic analysis will be utilised to formulate suggestions for enhancing cybersecurity in e-government systems. (Braun & Clarke, 2006)

Structure of the dissertation

The dissertation is organised in the following manner to methodically investigate the significance of cybersecurity in e-government services:

Chapter one offers an extensive examination of existing literature and presents a conceptual framework in depth. The text begins by examining fundamental ideas such as e-government and cybersecurity, establishing the basis for comprehending their interaction. The literature review analyses prior studies on the development of e-government and the influence of cybersecurity on its implementation and efficacy. This chapter conducts a synthesis of existing studies to identify areas where current knowledge is lacking and to build the theoretical foundation for the investigation. Furthermore, it establishes precise definitions for key terms and topics that will be utilized consistently throughout the dissertation, guaranteeing clarity and coherence.

Chapter two provides an overview of the case study background by presenting a detailed account of the organizational history and missions of the Scientific and Technical Information Research Center (CERIST). The context is essential for comprehending the particular setting in which the research is carried out. The chapter subsequently introduces the methodological framework employed in the study, elucidating the qualitative research design and the justification for selecting CERIST as the case study. The text outlines the data gathering techniques employed, such as semi-structured interviews, document analysis, and direct observation. It elucidates how these procedures enhance the overall comprehension of the study inquiries.

Chapter three provides an analysis of the results obtained from the case study and includes a detailed examination of the consequences of these findings. The text outlines the main cybersecurity challenges found at CERIST and the solutions implemented to tackle them. The data are examined to emphasise recurring patterns and themes, offering valuable insights into the efficacy of existing cybersecurity solutions. The discussion part provides an analysis of these findings within the wider context of e-government services, examining their relationship to current literature and theoretical frameworks. This chapter additionally examines the practical consequences of the discoveries for policymakers and practitioners in the realm of e-government and cybersecurity.

The thesis finishes by providing a concise overview of the study conducted, highlighting its significant contributions, acknowledging its shortcomings, and proposing potential areas for

further research. This section provides a concise summary of the main ideas presented in the dissertation, highlighting the importance of the findings and their possible influence on the field of e-government. Furthermore, it recognises the constraints of the research, such as the exclusive emphasis on CERIST, which could impact the applicability of the findings. Ultimately, the conclusion recommends specific topics for future investigation, outlining how later studies might expand upon the findings to enhance the comprehension of cybersecurity in e-government services.

This thesis seeks to enhance the existing knowledge in the field of public administration and information security by analysing the significance of cybersecurity in e-government services using a systematic and meticulous methodology. The systematic style guarantees a thorough examination of the subject, covering both theoretical principles and practical uses. This eventually improves the comprehension and execution of cybersecurity measures in e-government systems.

CHAPTER 1: THEORETICAL FRAMEWORK

The first chapter offers an extensive examination of existing literature and presents a conceptual framework in depth. The text begins by examining fundamental ideas such as e-government and cybersecurity, establishing the basis for comprehending their interaction. The literature review analyses prior studies on the development of e-government and the influence of cybersecurity on its implementation and efficacy. This chapter conducts a synthesis of existing studies to identify areas where current knowledge is lacking and to build the theoretical foundation for the investigation. Furthermore, it establishes precise definitions for key terms and topics that will be utilized consistently throughout the dissertation, guaranteeing clarity and coherence.

Section 1. Literature Review

The growing integration of digital technology into governmental activities has transformed the landscape of public administration, giving rise to the notion of e-government. However, this digital transformation brings with it the ever-present threat of cybersecurity breaches, which pose serious challenges to the integrity, confidentiality, and availability of government information systems. Understanding the intricate connection between cybersecurity and e-government is critical for policymakers, practitioners, and academics alike, as it affects the efficiency, security, and dependability of digital government efforts.

The purpose of this literature review is to give a complete examination of existing research on cybersecurity in the context of e-government. This review aims to elucidate the current state of knowledge regarding the role of cybersecurity in e-government services by synthesizing and analyzing a diverse array of academic articles, reports, and policy documents, with an emphasis on the case study at the Scientific and Technical Information Research Center (CERIST) in Algeria.

The literature review is divided into three major areas. First, we examine the evolution of e-government, tracking its historical course and distinguishing its many forms and frameworks. Second, we examine the diverse landscape of cybersecurity in e-government, including common risks, mitigation techniques, and the role of policies and regulations. Finally, we address the theoretical viewpoints and conceptual frameworks that support the relationship between cybersecurity and e-government, establishing the groundwork for the remaining parts of this thesis.

Through this extensive examination of the literature, we want to discover gaps, discrepancies, and emerging patterns in the current body of knowledge, providing the framework for the empirical inquiry that will follow. We hope that by contextualizing our research within the larger scholarly debate on cybersecurity and e-government, we may contribute to a better understanding of this complex and dynamic topic, eventually guiding policy and practice in digital governance.

1.1 Understanding E-Government

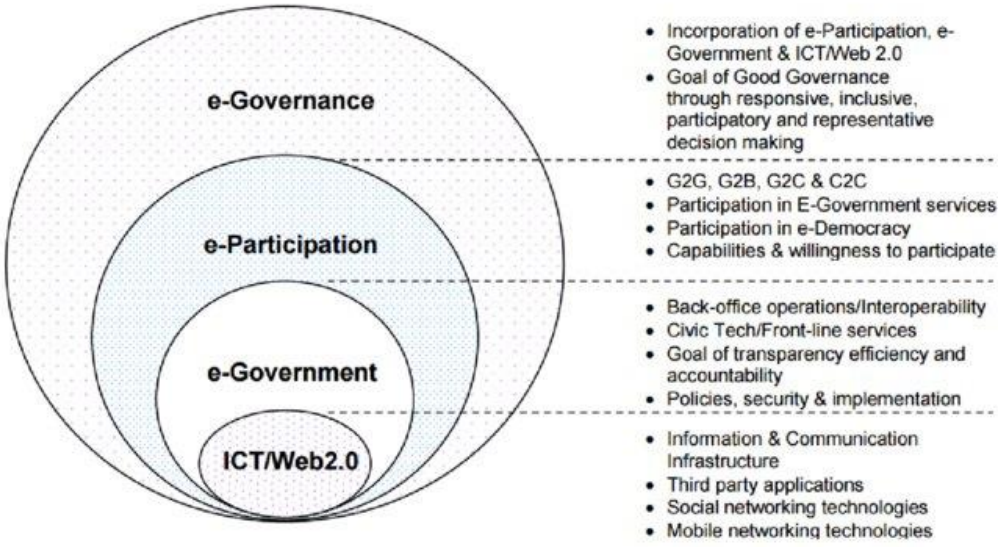
E-government is an abbreviation for electronic government, which refers to the framework of employing information systems and technology communications to deliver services to citizens inside the government. E-government involves a wide range of factors, including the use of the Internet and equipment such as computers to help the government provide different services to residents.

Adopting an e-government model can improve service efficiency and convenience while offering various options to various stakeholders. When an e-government system is operating efficiently, citizens can obtain government services directly, bypassing multiple intermediaries. It becomes the responsibility of the government to guarantee the security of these systems and, by extension, the security of the entire paradigm of service delivery to the populace. A foundational element of any e-government system is cybersecurity. (Alrubaiq & Alharbi , 2021)

E-government refers to the use of an internet-enabled platform to deliver government services to citizens and other residents of a nation. E-government services are routinely subjected to both qualitative and quantitative analysis, and the level of consumer participation and satisfaction serves as a barometer for success. Awareness, competence, social acceptance, sophistication, and service provision all lead to service adoption and engagement. Previous research on this topic has shown that a lower rate of adoption and satisfaction was caused by a lack of initiatives to raise awareness, foster trust, and offer sufficient training. The rapidly advancing technologies and improved infrastructure have the potential to drastically alter the situation, even quickly. (Basahel & Mohammad , 2017)

The use of ICTs in governmental activities is frequently associated with the concept of e-Government. eGovernment, as defined by the Organization for Economic Cooperation and Development (OECD, 2004), is the use of ICTs, especially the Internet, to improve governance procedures. 'Enhanced governance' is essentially about improving the provision of administrative services at first. There is hence a goal to improve the policymaking process by incorporating ICTs. The principal objective of integrating information technology is to optimize process efficiency, whereas the integration of communication technologies seeks to augment government accessibility. This strategy can increase public participation, which will boost effectiveness and raise the standard of governance procedures as a whole. (Islam & Mohammad , 2012)

Figure 1: Evolutionary E-Governance 2.0 Model



Source: (Huffman, 2017)

1.2 The Evolution of E-government

The emergence of e-government marks a significant shift in public administration, with technology used to improve government services and connections with citizens. Key findings obtained from many sources outline the growth of e-government as follows:

The word "evolution" connotes a dynamic process of advancement and change in e-government that includes modifications to tactics, tools, and models of governance. The authors' goal in performing a systematic literature review is to offer a thorough overview of the major developments, obstacles, and trends in e-government practice and research. The systematic method assures a complete and rigorous evaluation, with specific criteria for choosing and interpreting relevant material. (Oliveira & Martins, 2020) This technique improves the reliability and validity of the findings, allowing for a more impartial evaluation of e-government progress. The paper may discuss different aspects of e-government evolution, such as its development throughout history, stages of maturity, adoption patterns, and implications for governance, society, and the economy. It may also draw attention to new problems and potential paths for e-government practice and study. (Wang & Xiao, J, 2019)

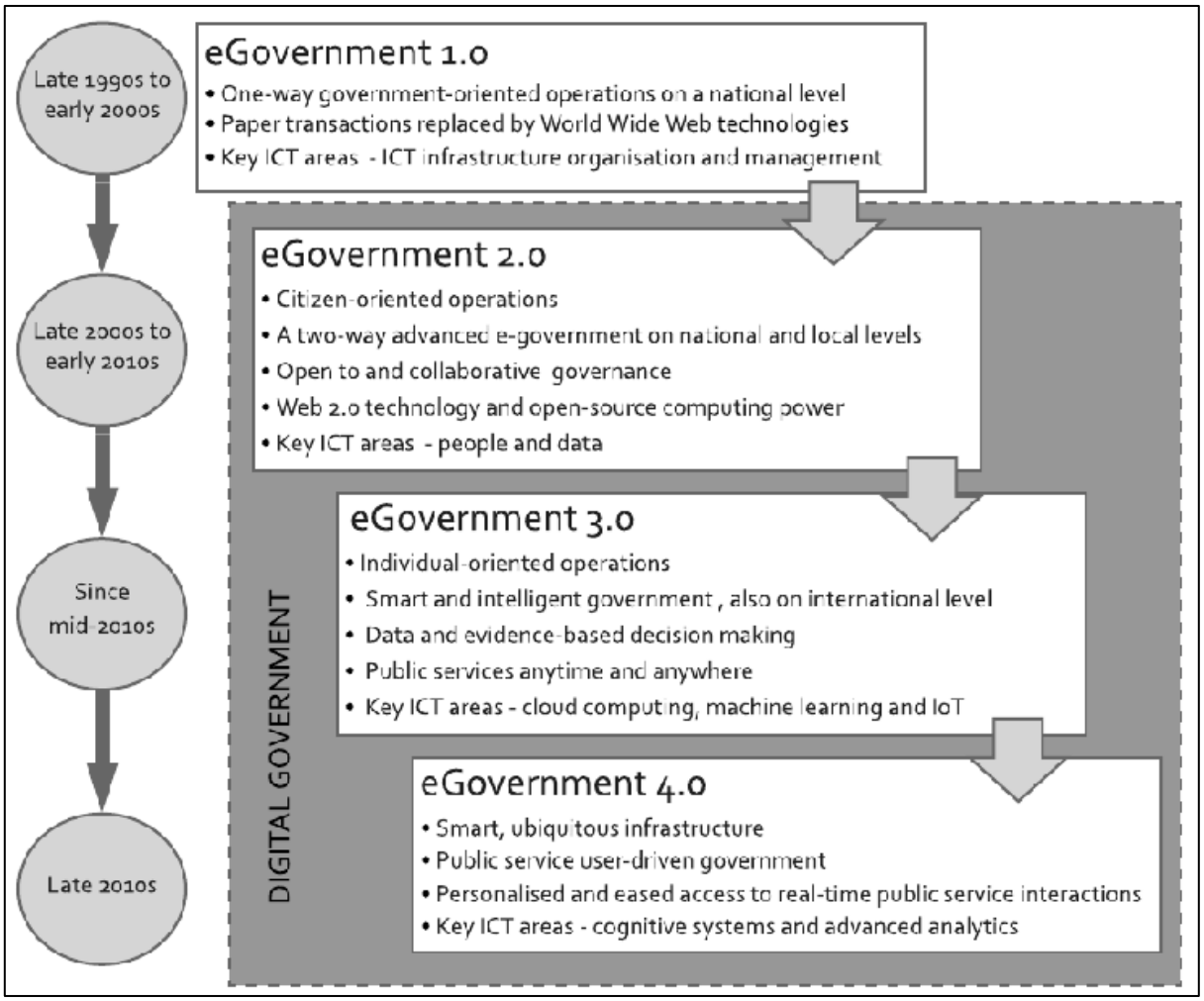
The phrase "e-Government" first appeared in the late 1990s, while the usage of computers in government predates this era. Over time, the literature on IT in government has developed, with a current emphasis on external applications, notably citizen services. E-Government began as a practitioner field, bringing together experts to address developing Internet-related issues. Initiatives such as the National Performance Review in the United States have highlighted the critical role of e-government in public services. (Horan & Åke, 2005)

E-government has evolved into a formal study sector with scientific inquiry, resulting in the formation of specialist conferences and publications. The field has expanded tremendously, generating discussion about its substance and placement in relation to other disciplines. Governments worldwide have embraced e-government projects to improve delivery of services and efficiency. Strategic plans like South Korea's national ICT Plan and Cyber Korea 21 represent concentrated attempts to digitize governance and promote a knowledge-based society. Promoting interministerial collaboration in e-government is critical to improving service delivery and information sharing. Initiatives such as e-government roadmaps and Electronic Government Acts promote system integration and e-participation. Some governments advocate

for a 'digital by default' policy, which prioritizes online service availability while assuring access for all sectors of society. However, obstacles remain in properly implementing these regulations to promote inclusiveness and efficiency in service delivery. (Horan & Åke, 2005)

The growth of e-government exemplifies a trend toward digital governance, emphasizing efficiency, transparency, and citizen-centric delivery of services via technology innovation and strategic planning attempts. (Horan & Åke, 2005)

Figure 2: the evolution of e-government



Source: (Barcevičius)

E-government, or the use of information and communication technologies (ICTs) to improve government operations and service delivery, has evolved significantly over the last several decades. Scholars have conducted substantial research on this progression, including historical context, technical breakthroughs, obstacles, and global viewpoints.

Historical Context and Emergence of e-government:

E-government appeared in the end of the 20th century, aligning with the internet and ICT breakthroughs. (West, E-Government and the Transformation of Service Delivery and Citizen Attitudes, 2004) The early conversations focused on using technology to improve government services and connections with citizens. Over time, the notion expanded beyond simply information broadcast to interactive and transactional platforms, indicating a move toward citizen-centric service delivery. (Heeks, Implementing and Managing E-Government: An International Text, 2006)

Technological Advancements and Impact on e-government:

Technological breakthroughs have significantly influenced the growth of e-government. discuss how innovations like mobile platforms and social media have revolutionized government-citizen relations, making them more accessible and engaging. These improvements have aided the move to more user-centric e-government models, resulting in increased efficiency and effectiveness. (Dwivedi, Pan, Sharif, & Weerakkody, 2009)

Challenges and Barriers in e-government implementation:

Despite the potential benefits, implementing e-government programs is not without obstacles. Highlight key success factors and constraints, such as infrastructure, cybersecurity, and the digital divide. Addressing these problems is critical to ensuring the effective adoption and sustainability of e-government projects. (Alshibly & Irani, , 2020)

Global Perspectives and Case Studies:

A globally view of e-government evolution gives useful insights into various strategies for implementation and lessons learnt from different nations. Case studies from diverse locations provide real examples of successful e-government efforts, demonstrating best practices and

novel approaches to digital administration. (The United Nations Department of Economic and Social Affairs (UNDESA), 2020)

The study of e-government has advanced significantly, with researchers attempting to comprehend its dynamics, effect, and future prospects. A recent review looked at the state of e-government research, offering information on its developmental history and new tendencies.

The study analysed a corpus of 21,320 papers connected to e-government research and discovered a surprising volume of scholarly production, indicating the growing interest and relevance of digital governance. Notably, these publications received a high citation count of 263,179, demonstrating the significance and relevance of e-government research in academic debate. (Ramzy & Ibrahim, Bahaa, 2024)

The data revealed a continuous yearly increase of 21.50% in e-government research, indicating a continued momentum and growing scholarly interest in the topic. Regression analysis also predicted a modest rise in research results in the following years, showing a continuous focus on investigating various facets of e-government. (Ramzy & Ibrahim, Bahaa, 2024)

Although conference papers have traditionally been important for sharing e-government research, researchers discovered that articles had a higher effect than conference proceedings. This emphasizes how crucial scholarly publications with high standards are for influencing the conversation and expanding our understanding of e-government. (Ramzy & Ibrahim, Bahaa, 2024)

Also, the survey highlighted the University of Albany (SUNY) as a key institution for e-government research, both in terms of output and effect. Its contributions highlight the university's critical role in encouraging innovation and research in the discipline. (Ramzy & Ibrahim, Bahaa, 2024)

In addition, the analysis revealed specific nations positioned to become significant actors in e-government research, indicating a worldwide dispersion of studies and interests. Furthermore, numerous emergent issues were recognized as prospective focal points for future research

initiatives, highlighting the dynamic character of the e-government sector and shifting academic agendas. (Ramzy & Ibrahim, Bahaa, 2024)

Table 1: Regional rankings (EGDI - 2018)

		Classement	EGDI	OSI	TII	HCI
2008 (readiness)	EGDI	121	0.3515	0.2241	0.1230	0.7114
	EPI	152	0.0227			
2010	EGDI	131	0.3181	0.0984	0.1248	0.7377
	EPI	157	0.0143			
2012	EGDI	132	0.3608	0.2549	0.1812	0.6463
	EPI	124	0.0526			
2014	EGDI	136	3106	0.0787	0.1989	0.6543
	EPI	172	0.0784			
2016	EGDI	150	0.2999	0.0652	0.1934	0.6412
	EPI	167	0.1186			
2018	EGDI	130	0.4227	0.3056	0.1138	0.3562
	EPI	165	0.2022			

Source: (Mezhouda, 2019)

1.3 Understanding Cybersecurity

The expression "Cyber" originated from "Cybernetic," which refers to the principle of communication and regulation feedback control utilizing computers. Cybersecurity refers to technology, methods, and practices used to protect networks, computer hardware, software, programs, information, and data against unwanted access, damage, or assaults. In essence, cybersecurity involves proactive techniques for protecting information against theft, compromise, or harmful use. It necessitates the ability to recognize risks and harmful programs that threaten data and information security. (Goutam, 2021)

Cybersecurity is the activity of safeguarding internet-connected systems, including hardware, software, and data, against cyberthreats. It is used by consumers and businesses to prevent unwanted access to data centers and other digital systems. (Alexander S. Gillis, 2024)

A good cybersecurity plan may offer a strong defense against harmful assaults that attempt to access, change, delete, destroy, or extort a company's or user's systems and private data. Cybersecurity can also help avoid attacks that aim to disable or impair the operations of a system or device. (Alexander S. Gillis, 2024)

An effective cybersecurity strategy should include many layers of defense across all potential access points and attack surfaces. This comprises a layer that protects data, software, hardware, and network connections. Furthermore, all personnel in a business who have access to any of these endpoints should be taught in the correct compliance and security procedures. Organizations also employ solutions like unified threat management systems to provide another layer of security against attacks. These technologies can identify, isolate, and remediate possible problems while also notifying users if further action is required. (Alexander S. Gillis, 2024)

Cyberattacks may disrupt or paralyze their victims in a variety of ways, therefore developing a robust cybersecurity plan is a critical component of any firm. Companies should also have a plan for disaster recovery in place in order to swiftly recover in the case of a successful cyberattack. (Alexander S. Gillis, 2024)

Cybersecurity is the activity of defending networks, programs, and systems from digital threats. These assaults are often intended to access, change, or delete sensitive information; extract funds from users via ransomware; or disrupt routine corporate activities. Cybersecurity includes technology, techniques, and strategies for protecting data, computer systems, and networks from threats. It is critical for protecting all forms of data against theft and loss, as well as preventing data breaches, identity theft, and financial losses. Cybersecurity concerns have become a genuine hazard as cybercrime has increased and people rely more on technology in their everyday lives. To solve these difficulties, enterprises must put in place effective cybersecurity measures, such as application security, network security, endpoint safety, security of data, and access and identity management. A single threat management system may also assist automate interconnections across chosen Cisco Security products and speed essential recognition, investigation, and remediation. In the context of e-governance, cybersecurity is critical for

securing sensitive information while also assuring the integrity and efficiency of government services. Governments must develop a comprehensive cybersecurity strategy in order to successfully handle security threats. This strategy should include methods to preserve information confidentiality, availability, and integrity inside e-government systems. (Kelley, 2023)

1.4 The Impact of Cybersecurity on E-Government: A Review of Existing Literature:

The extant literature on cybersecurity in e-government emphasizes the vital significance of safeguarding government services in today's digital environment. It underlines the need of deploying effective cybersecurity measures to defend against cyber-attacks, improve the delivery of services, and promote trust among users. (Anderson J. , 2018)

To deal with these issues, experts have developed a variety of frameworks aimed at empowering government institutions to efficiently provide safe e-government services. These frameworks intend to enhance awareness about the relevance of safety services in e-governance among varied stakeholders, including academia, policymakers, practitioners, and the general public. (Smith & Johnson, 2019)

Plus, the literature highlights the insertion of safety services into eGMMs in order to align the strategic goals of e-government services with security measures. This integration is critical for addressing security risks completely and preserving the security, confidentiality, and accessibility of critical information assets. (Patel & Lee, 2020)

Research efforts have focused on finding weaknesses in the cybersecurity framework within e-government operations, measuring the resilience of the cybersecurity framework, and comparing the efficacy of cybersecurity frameworks across different nations' e-government services. (Wang & Chen, 2021)

Cybersecurity in e-government has received a lot of attention because of the growing dependence on digital technology to offer government services and manage sensitive data.

A thorough examination of the available literature gives insight on the complex difficulties, emerging methods, technical breakthroughs, human variables, and global views related with cybersecurity in e-government.

1.4.1 Challenges in Cybersecurity:

Cybersecurity in e-government faces a myriad of challenges. (Disterer, 2018) exposes the inherent weaknesses in government systems caused by complicated infrastructures and older technology. Furthermore, the rise of sophisticated cyber-attacks creates an ongoing danger to the integrity and confidentiality of government data. Compliance with legal frameworks, such as GDPR and HIPAA, hampers cybersecurity operations, especially for government entities that handle sensitive information. (Bertino & Islam, 2019).

1.4.2 Strategies and Approaches:

To address these issues, academics presented a variety of tactics and approaches. (Bertino & Islam, 2019) encourage the use of risk-based cybersecurity frameworks, which prioritize resources based on the potential impact of cyber threats. likewise, the deployment of sophisticated encryption techniques, such as homomorphic encryption and quantum-resistant cryptography, can strengthen data security safeguards. (Stylianou, Skouloudis, Georgiadou, & Malesios, 2020). Multi-factor authentication solutions add an extra layer of protection, lowering the danger of unwanted access to government systems.

1.4.3 Role of Technology:

Technological advancements play a pivotal role in enhancing cybersecurity in e-government. (Stylianou, Skouloudis, Georgiadou, & Malesios, 2020) explore the potential of emerging technologies, such as AI and ML, in threat detection and incident response. AI-powered cybersecurity solutions can analyse vast amounts of data in real-time, identifying patterns indicative of cyber-attacks and enabling proactive mitigation measures. Blockchain technology, with its decentralized and immutable ledger, holds promise for securing government transactions and data exchanges (Stylianou, Skouloudis, Georgiadou, & Malesios, 2020).

1.4.4 Human Factors and Training:

Human factors are another important part of cybersecurity resilience in e-government. Emphasize the value of training and awareness initiatives for government staff. Effective cybersecurity training efforts teach employees how to spot phishing attempts, recognize social engineering strategies, and follow security best practices. Furthermore, building an environment of cybersecurity understanding creates accountability among employees, minimizing the possibility of insider attacks. (Awad, Atef, & El-Zayat, 2019)

Section 2. Conceptual framework

In the world of e-government, cybersecurity integration is critical for protecting digital assets and maintaining efficient administration. This conceptual framework brings together aspects of cybersecurity and e-government to give a thorough understanding of their interactions. It recognizes the complex character of cybersecurity in e-government, which includes technical, managerial, and policy elements. The paradigm emphasizes the interconnectivity of cybersecurity and e-government governance, which influences making decisions, resilience, and accountability. By taking contextual aspects into account, this framework aims to provide insights into successful solutions for improving the resilience of cybersecurity and governance practices in e-government environments.

2.1 Definition of cybersecurity

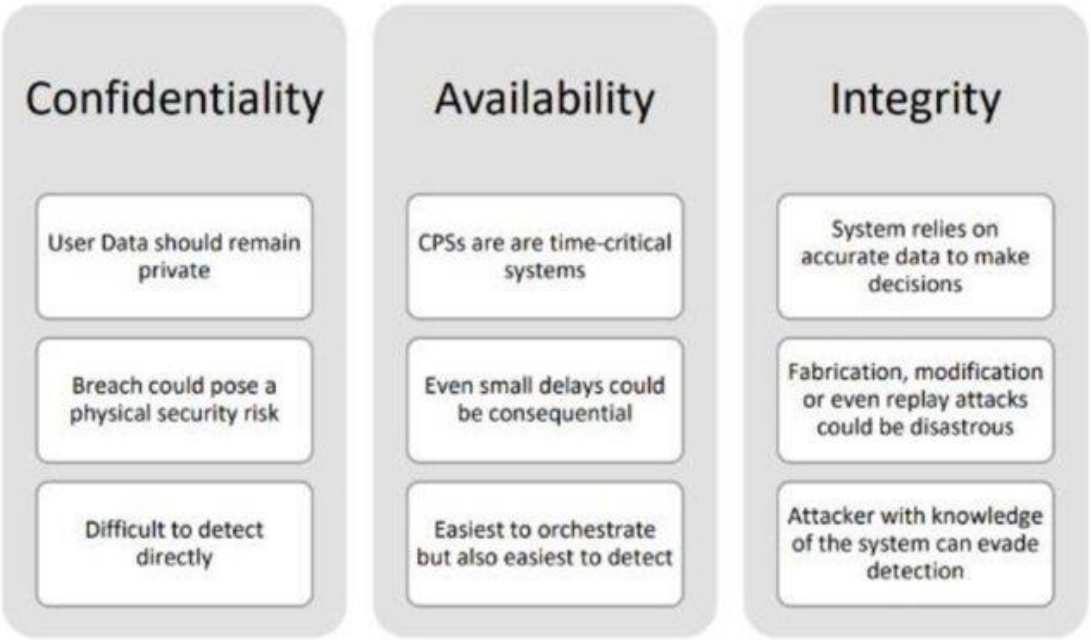
The process of protecting networks, computers, servers, mobile devices, electronic systems, and data against hostile intrusions is known as cybersecurity. It is often referred to as electronic information security or technological advances security. (kasperskey, 2024)

In order to secure the cyber environment, company, and user assets, cybersecurity refers to a set of tools, policies, security concepts, security safeguards, guidelines, risk management techniques, activities, training, best practices, assurance, and technology. The assets of an organization or user comprise linked computers, employees, telecommunications systems, infrastructure, applications, services, and any data that is transferred and stored in the cyber environment. The goal of cybersecurity is to protect user assets and organizational security properties against pertinent security threats in the online environment. (ITU, 2024)

Cybersecurity is the process of defending computer networks, systems, applications, and data from online dangers such malware, illegal access, and data leaks. It entails putting policies, procedures, and technological frameworks in place to guarantee the privacy, availability, and integrity of data and information systems. (National Institute of Standards and Technology, 2018) The goal of cybersecurity is to protect a variety of digital assets against threats such as malware, hacking attempts, denial of service attacks, illegal access, and data breaches. These assets include computers, servers, mobile devices, networks, software applications, and data repositories. (Union I. T., Overview of cybersecurity, 2008)

The three main objectives of cybersecurity are to prevent illegal access to systems and data when needed (availability), prohibit unauthorized alteration of data (integrity), and avoid unauthorized exposure of information (confidentiality). (Andress, The basics of information security: Understanding the fundamentals of InfoSec in theory and practice, 2014) Technical controls, security policies, risk management procedures, training initiatives, incident response plans, and the use of specialist cybersecurity tools and solutions are all part of the multi-layered strategy that accomplishes these objectives. (Whitman & Mattord, 2016)

Figure 3:Summary of three key network security objectives



Source: (Alvarez & Subburaj, 2023)

The process of preventing and mitigating possible threats and vulnerabilities, putting in place suitable protections, keeping an eye out for security events, and successfully responding to successful assaults is all part of cybersecurity. (Cybersecurity, 2021) Organizations must work together to safeguard their data and digital assets by developing a strong cybersecurity culture among stakeholders and staff in addition to using technology safeguards. (Standardization t. I., 2018)

Today's digital era has made cybersecurity a top priority for everyone—individuals, companies, and governments—due to the sophistication and prevalence of cyberthreats. Sufficient cybersecurity protocols aid in preserving the privacy, availability, and integrity of confidential data, guard against harm to one's finances and reputation, and guarantee the uninterrupted provision of vital services and activities. (Forum, 2022)

The following are some important indicators that are used to assess and gauge the success of cybersecurity initiatives and programs:

Number of security incidents/breach: This involves keeping tabs on the quantity and seriousness of security incidents, which include data breaches, malware infections, illegal access attempts, and other cyberattacks. (Chertoff, 2018)

Time to detect and respond to incidents: evaluates the organization's capacity to identify security issues fast, take appropriate action to mitigate their effects, and guarantee prompt remedy. (Technology, 2018)

Vulnerability management metrics: monitors the process of finding, classifying, and fixing software vulnerabilities. It also keeps track of how long it takes to fix serious flaws and how many vulnerabilities are exposed overall. (Jacobs, Romanosky, & Roytman, 2020)

Compliance with security standards and regulations: Assesses how closely the company complies with pertinent cybersecurity frameworks, standards, and laws (e.g., NIST, ISO 27001, GDPR, industry-specific legislation). (Standardization I. O., ISO/IEC 27001:2013 - Information security management systems -- Requirements, 2018)

Security awareness and training effectiveness: evaluates the efficacy of security awareness and training initiatives using data from phishing simulations, employee participation rates, and knowledge tests. (Rocha Flores & Ekstedt, 2016)

Patch management and system hardening: evaluates the organization's capacity to harden systems against known vulnerabilities and provide security fixes quickly, hence decreasing the attack surface. (Technology, 2021)

Secure configuration management: monitors the application and upkeep of safe system, application, and network device settings, guaranteeing compliance with security standards and industry best practices. (Security C. f., 2021)

Encryption and data protection: assesses the degree to which sensitive data is protected while in use, in transit, and at rest by encryption and other data security methods. (Technology, 2020)

Access control and identity management: Keeps an eye on the efficiency of user account management, privileged access management, and access control procedures. (Standardization I. O., 2016)

Network security and monitoring: Evaluates the strength of intrusion detection/prevention systems, firewalls, and other network security controls.

Assesses the organization's capacity to recognize, evaluate, and control cybersecurity threats using risk assessment procedures and risk management techniques. (National Institute of Standards and Technology, 2018)

Budget and resource allocation for cybersecurity: Monitors the amount of money the company spends on cybersecurity projects, as well as personnel numbers and resource use. (Technology, 2018)

Risk management related to third parties and the supply chain: Assesses how well the company manages cybersecurity risks posed by partners, suppliers, and other third parties. (Gartner, 2022)

Cyber resilience and incident recovery: Evaluates the efficacy of backup and disaster recovery procedures as well as the organization's capacity to continue operations and recover from cyber incidents. (Technology, 2020)

Table 2 indicators of cybersecurity

Category	Indicator
Incident Response	Incident response time
	Detection and analysis effectiveness
	Response effectiveness
Vulnerability Management	Timeliness of patching vulnerabilities
	Vulnerability assessment effectiveness
Security Awareness and Training	Level of employee awareness
	Effectiveness of training programs
Compliance	Regulatory Compliance
	Adherence to security standards and regulations
	Audit and Assessment Findings
Security Incidents	Frequency and severity of security incidents
	Types of security incidents
Security Controls	Effectiveness of security controls
	Efficiency of antivirus, firewalls, etc.
Data Protection Measures	Implementation of encryption and access controls
	Data loss prevention effectiveness
Cybersecurity Investment	Allocation of resources to cybersecurity

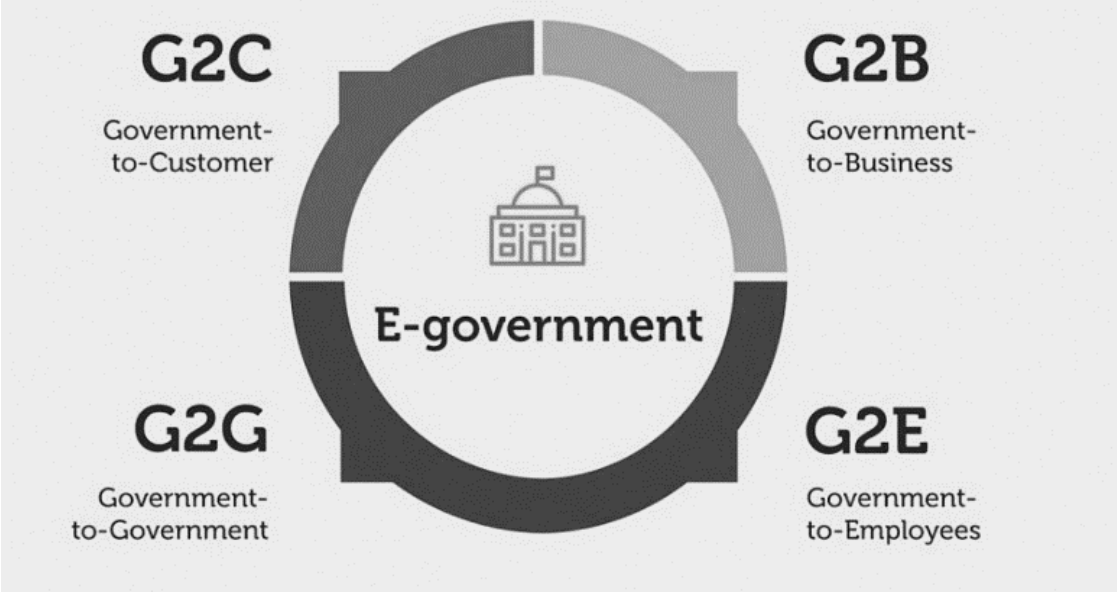
	Budget for cybersecurity initiatives
Cybersecurity Culture	Integration of cybersecurity into organizational culture
	Employee adherence to security policies
Cybersecurity Governance	Presence of dedicated cybersecurity teams
	Risk management frameworks
	Board oversight of cybersecurity

Source: created by us

2.2 Definition of E-government

The use of technology communications tools, such computers and the Internet, to deliver public services to residents and other people in a nation or area is known as e-government. With the advent of e-government, individuals may now connect with the government more easily and directly, as well as with companies and other government agencies. (Caves, 2004)

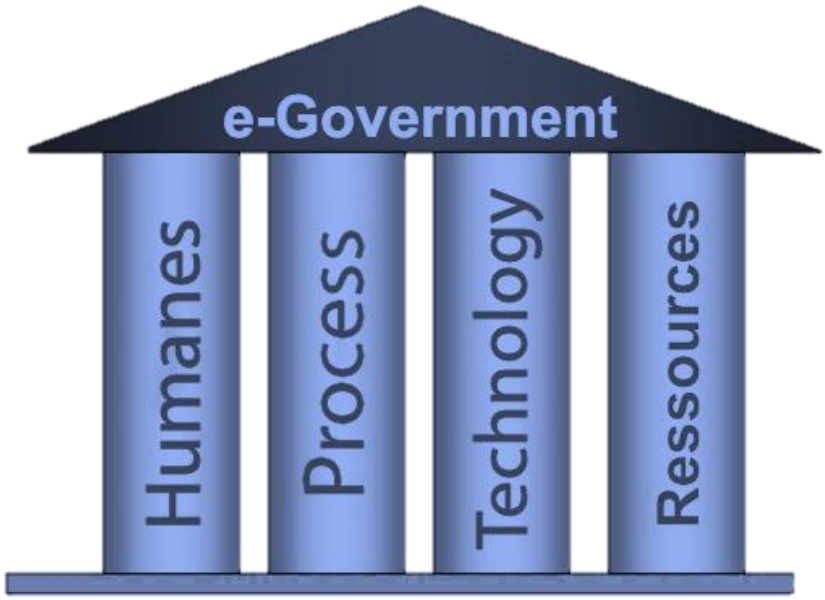
Figure 4:Type of e-government transactions



Source: (Hai & Ibrahim, 2007)

E-government, often known as digital or electronic government, is the use of information and communication technologies (ICTs) by government agencies to provide services, distribute information, and enable interactions with residents, companies, and other stakeholders. It includes a variety of programs aiming at using digital technology to reform and enhance how governments function and interact with their citizens. (United Nations Department of Economic and Social Affairs, 2020)

Figure 5:The 04 pillars of e-government



Source: (Mezhouda, 2019)

The provision of online services is a key component of e-government, allowing consumers and companies to access government information and services via websites, mobile applications,

and other digital platforms. (Bertot, Jaeger, & McClure, Proceedings of the 9th Annual International Digital Government Research Conference, 2008) This improves convenience and accessibility while also streamlining procedures, lowering administrative hassles and expenses. Furthermore, e-government programs aim to increase citizen involvement by allowing two-way communication, online discussions, and participatory decision-making processes, boosting openness and accountability. (Savić, E-Government Services, 2019)

Internally, e-government aims to increase the efficiency and effectiveness of government operations by utilizing ICTs for process automation, data exchange, and cooperation among various departments and levels of government. (Alshehri & Drew, 2010) This includes increasing interoperability and integration of diverse government systems and databases, allowing for smooth information interchange and service delivery across agencies. (Gil-Garcia & Pardo, E-government success factors: Mapping practical tools to theoretical foundations, 2005)

Furthermore, e-government projects seek to increase openness and accountability by making government information and data more accessible to the public, allowing for greater monitoring and supervision of government operations. (OECD, Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact, 2017) This is accomplished through open data programs, web portals, and other digital platforms that provide access to government information and decision-making processes. (Janssen, Charalabidis, & Zuiderwijk, Benefits, adoption barriers and myths of open data and open government, 2012)

In the end, e-government is a component of a larger public sector digital transformation initiative that makes use of cutting-edge technologies like blockchain, big data analytics, cloud computing, and artificial intelligence to spur innovation and raise the effectiveness, efficiency, and responsiveness of government services. (Scholl, 2017) Enhancing citizen involvement and engagement, fostering accountability and transparency, facilitating data-driven policy formulation and decision-making, and improving the quality and accessibility of public services are the main goals of e-government. (Commission, 2019)

Indicators of E-government

Category	Indicator	Explanation
Service Delivery	Online Service Availability	Percentage of government services available online, indicating the accessibility and convenience for citizens.
	Service Completion Time	Average time taken to complete online transactions or service requests, measuring efficiency and responsiveness.
	User Satisfaction	Feedback from citizens on the usability, reliability, and overall satisfaction with e-government services.
Digital Inclusion	Internet Penetration Rate	Percentage of the population with access to the internet, ensuring broad availability of e-government services.
	Digital Skills Development	Percentage of citizens with basic digital literacy skills needed to access and utilize e-government services effectively.
	Accessibility Compliance	Compliance with accessibility standards to ensure that e-government services are usable by all citizens, including those with disabilities.
Transparency	Open Data Availability	Availability of government data and information for public access, promoting transparency and accountability.
	Freedom of Information Requests	Number of requests for government information processed and fulfilled, demonstrating transparency and openness.
	Public Sector Integrity	Measures of corruption perception and public trust in government institutions, influencing transparency and accountability.
Efficiency	Cost Savings	Reduction in administrative costs and paperwork through the implementation of e-government services.
	Process Automation	Automation of government processes and workflows, leading to improved efficiency and reduced manual intervention.
	Interoperability	Integration of government systems and data to enable seamless exchange of information and services across departments.
Security and Privacy	Data Protection Compliance	Compliance with data protection laws and regulations to ensure the privacy and security of citizens' personal information.
	Cybersecurity Measures	Implementation of security controls and measures to protect e-government systems and data from cyber threats.
	Privacy Policy Compliance	Transparency and adherence to privacy policies and regulations to safeguard citizens' privacy rights in e-government services.
Governance	Digital Government Strategy	Existence and effectiveness of a government-wide strategy for digital transformation and e-government initiatives.
	Stakeholder Engagement	Engagement of citizens, businesses, and other stakeholders in the design and delivery of e-government services.
	Performance Monitoring	Regular monitoring and evaluation of e-government initiatives to assess progress, identify areas for improvement, and ensure accountability.

Source: created by us

2.3 Definition of cybersecurity in e-government

In e-government, cybersecurity is defined as the collection of tools, procedures, and methods used to defend programs, devices, networks, and data from harm, intrusion, or illegal access. Protecting networking systems, programs, and sensitive data from attackers requires cybersecurity. Its objectives are to lessen the likelihood of cyberattacks and guard against the unapproved use of technology, networks, and systems. Governments need cybersecurity because they handle, store, and gather vast volumes of data on computers and other devices—a large percentage of which may include sensitive information. Government, military, business, financial, and medical institutions gather, analyze, and store enormous volumes of data on computers and other devices, which makes cybersecurity crucial. (National Association of State Chief Information Officers (NASCIO), 2017)

In the context of government, cybersecurity refers to the entire suite of controls, guidelines, and policies put in place to guard government data, networks, and information systems against interruption, alteration, theft, and unauthorized use. It entails preventing illegal access, theft, or abuse of sensitive government data, including classified information, citizen personal data, and other private documents. (Andress, Cybersecurity for government: An overview, 2020) Protecting government computer networks and communication systems against online dangers including malware, denial-of-service (DDoS) assaults, and unauthorized access attempts is also included in this. Government cybersecurity is necessary for preventing cyberattacks that might seriously impair or disrupt critical infrastructure and services including transportation networks, emergency response systems, and power grids. (Union I. T., Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity, 2018)

Creating and putting into practice policies and processes to quickly identify, address, and recover from cyber events or breaches is essential to successful cybersecurity in government. Through an ongoing risk management process, cybersecurity threats to government systems and data must be identified, evaluated, and mitigated. Setting up governance structures and oversight procedures for cybersecurity projects, as well as adhering to applicable cybersecurity laws, rules, standards, and best practices, are also crucial. (Pereira, Cunha, Lipinsky, & Becker, 2020) To build a strong cybersecurity culture and improve government workers' and stakeholders' capacity to recognize and respond to cyber threats, it is essential to raise cybersecurity awareness

and offer training. For the government to continue providing essential services and activities, preserve national security interests, and uphold public trust, cybersecurity is essential. (Newmeyer, 2015) It necessitates cooperation between different government departments, partners in the corporate sector, and other interested parties, as well as a dedication to constantly adapting to new developments in cyber risks and technology. (U.S. Department of Homeland Security, 2021)

2.4 Overview of cybersecurity frameworks applicable to e-government

As digital technologies become more integrated into public service delivery and data management, e-government programs throughout the world face substantial cybersecurity challenges. To address these problems, a variety of cybersecurity frameworks and measures have been developed to provide advice and best practices for protecting government systems and information. The following describes major frameworks, measurements, and models relevant to e-government:

2.4.1 NIST Cybersecurity Framework (CSF):

The National Institute of Standards and Technology (NIST) developed the CSF, which offers a flexible method to improving cybersecurity risk reduction across critical infrastructure sectors, including government. It has five primary functions: identification, protection, detection, response, and recovery. E-government institutions can use the CSF to review and strengthen their cybersecurity position in accordance with industry norms. (E, Crawford , & Kristen, 2015)

2.4.2 ISO/IEC 27001:

an international standard for ISMS, provides an organized approach to controlling cybersecurity threats and protecting private data in e-government enterprises. By putting ISO/IEC 27001 into practice, e-government organizations may create strong security measures, evaluate risks, and prove that they are in conformity with legal requirements. (Ashman & Arthur , 2018)

2.4.3 COBIT:

created by ISACA, is an enterprise IT governance and management architecture that includes cybersecurity governance. COBIT is a tool that e-government organizations may use to establish and implement cybersecurity controls, coordinate IT spending with strategic objectives, and guarantee effective technology and information resource management. (Shahbaz & Adnan , 2017)

2.4.4 ITIL:

ITIL helps e-government organizations improve the efficacy and efficiency of their cybersecurity operations while guaranteeing alignment with business objectives by providing best practices for managing IT services, including cybersecurity incident management and response. (Abdeslam & Yousif , 2015)

2.4.5 CIS Controls:

The Center for Internet Security (CIS) Controls are a collection of best practices designed to strengthen cybersecurity defenses against common cyber-attacks and vulnerabilities. E-government enterprises may use CIS Controls to set a baseline for cybersecurity policies, minimize risks, and increase resilience to cyber-attacks. (Snoke, Kimppa, & Norros, 2019)

2.4.6 FISMA:

which mandates cybersecurity standards for US federal government agencies, requires regulatory compliance, the establishment of cybersecurity frameworks, and the deployment of appropriate security measures to protect government databases and assets. (T, Gorden, J, & Visner, 2017)

2.4.6 Cybersecurity Measures for E-Government Frameworks:

Encompassing technical and organizational controls tailored for addressing cybersecurity challenges in e-government environments, these measures include network segmentation, encryption, access controls, security awareness training, incident response planning, and continuous monitoring. (National Institute of Standards and Technology (NIST) Special Publication)

2.4.7 eGMMs:

Providing a structured framework for evaluating and enhancing the maturity of e-government initiatives, including cybersecurity capabilities, eGMMs aid e-government agencies in assessing their current cybersecurity posture, identifying improvement areas, and devising strategic roadmaps for bolstering cybersecurity resilience and governance. (Layne & Lee, 2001)

2.4.8 BCEB:

A self-assessment tool developed by NIST to evaluate and enhance cybersecurity practices within organizations. E-government agencies can leverage BCEB to assess their cybersecurity maturity levels, pinpoint gaps and opportunities, and prioritize investments in cybersecurity initiatives.

These frameworks, measures, and models offer invaluable guidance to e-government agencies in addressing cybersecurity challenges effectively while safeguarding critical digital assets and services. By adopting these frameworks and measures diligently, e-government organizations can fortify their cybersecurity resilience and adeptly manage cyber risks in an increasingly digital landscape. (National Institute of Standards and Technology (NIST), n.d.)

2.5 Importance of cybersecurity in e-government systems

Cybersecurity, often known as information technology security, is the protection of sensitive data, networking systems, and softwares from assaults, it protects against malicious attacks that seek to change, destroy, gain access to, extort, or erase sensitive data and systems owned by a government or an organization. (Sear, 2023)

Over the last year, hundreds of large-scale cyber assaults have been reported in nations around the world, and this trend is projected to continue in the future years. (Sear, 2023)

Government data is sensitive and secret information that should not be made public, it requires a high degree of cyber security to avoid unwanted access by viruses and hackers. (Sear, 2023)

Governments all across the globe keep classified material on the cloud and servers, this data might include military plans, personal information about residents, national investments, sensitive information, the nation's infrastructure, biometric data, and more. (Sear, 2023)

Hackers attempt to acquire this information by infiltrating government computers. Without a strong cybersecurity policy, that country's safety will be jeopardized. (Sear, 2023)

A strong cybersecurity plan protects critical government information prevents it from falling into the wrong hands. (Sear, 2023)

The public sector is unlikely to regress, with government services becoming less available online and only generating efficacy through physical labour and in-person interactions. Political and governmental communication over the Internet is not expected to decline; rather, it should be seen as the beginning of something bigger. With this in mind, e-government will advance alongside publicly accessible groups that have produced resources. (Lynn, 2010) Public organizations and staff will prosper with a better grasp of what has been entrusted with them because of the same development. Put differently, for public management and staff to sustain the digital culture as times change, e-government and understanding of its security would need to advance hand in hand—or at least in the sense of execution. (Lee, Chang, & & Berry, 2011) Furthermore, there are benefits for both the general public and public sector workers. The former show a stronger level of trust and active involvement with the government, while the latter boost productivity and effective services while working towards the larger objective.

The ideal outcome would be to confirm how well-informed public employees should be, increase public awareness of cybersecurity, and achieve closure of the gaps among individuals and the cybersecurity interdependency, where regular people assist in identifying potential threats against the network systems of their organizations. Numerous studies have been conducted on the importance, effects, and accurate definition of cybersecurity at all governmental levels; yet, none of them have provided a thorough explanation of how cybersecurity is first introduced and subsequently implemented inside an organization. Having started e-government projects during the Clinton presidency. (Moon, 2002) the ramifications for public's private data security and recognized technological issues with government internet services were barely discussed, if at all. (S, Norris, & Fletcher, 2003)

Even if the cybersecurity safeguards that e-government necessitates were taken into account, only a small segment of an organization would be aware of all the difficulties or potential dangers. One of the obstacles to the development of e-governments and its relationship to security is the fact that, aside from federal and state governments, very few local governments have intranet-specific administrators whose primary duty is to maintain these kinds of

government websites. There is a severe dearth of technical staff and website experience in the public sector's digital realm, which raises concerns about what happens when an online site crashes, becomes hacker-friendly, or stops functioning as intended. Finally, in order to clarify the differences.

2.6 Integration of cybersecurity into e-government architecture

In an increasingly digital world, the security, availability, and integrity of government services and data depend on the integration of cybersecurity into e-government architecture. Each of the several interrelated components of this integration is essential to enhancing the overall cybersecurity posture of e-government systems. Here, we offer a thorough analysis of every facet as well as further information:

Risk Assessment and Management:

In order to detect and analyze possible cybersecurity risks and vulnerabilities inside e-government systems, this element entails doing thorough risk assessments. It includes techniques for ranking risk mitigation initiatives according to importance and likelihood, figuring out risk tolerance levels, and evaluating the effect and likelihood of different threats. Identification, analysis, assessment, treatment, and monitoring of risks are all part of the risk management procedures that guarantee continuous resistance to changing cyberthreats. (Wong, Wong, Behnam, Li, & Yan, 2018)

Comprehensive methods to risk assessment and management are offered by detailed frameworks like the ISO/IEC 27005 and NIST Risk Management Framework (RMF), which incorporate elements including asset value, threat intelligence, and regulatory compliance concerns.

Security by Design:

This component entails conducting thorough risk assessments to identify and analyze possible cybersecurity risks and vulnerabilities in e-government systems. It includes methods for analyzing the likelihood and effect of various risks, establishing risk tolerance thresholds, and prioritizing risk reduction actions. Risk management techniques involve risk identification,

analysis, appraisal, treatment, and monitoring to guarantee long-term resilience against developing cyber threats. (Anderson R. , 2008)

Detailed frameworks, like the NIST Risk Management Framework (RMF) and ISO/IEC 27005, offer systematic approaches to risk assessment and management that take into account intelligence on threats, asset valuation, and regulatory

Access Control and Authentication:

Access control and authentication procedures are crucial for controlling access to e-government systems and safeguarding confidential information from unauthorized disclosure or change. This element entails putting in place strong access control methods including, access control based on attributes, and mandatory access control, which apply least privilege principles and limit user access to permitted resources. Also, multifactor authentication improves authentication security by demanding various types of verification. (Garfinkel, Spafford, & Schwartz, 2005)

Standards like NIST Special Publication 800-53, as well as legislative frameworks like the GDPR, specify precise standards and recommendations for access control and identification in government systems, such as managing identities, access enforcement, and authentication protocols.

Data Protection and Privacy:

Data protection and privacy safeguards are designed to secure confidential government data from unlawful access, disclosure, or abuse. This involves using encryption, data hiding, tokenization, and anonymization techniques to protect data in transit and at rest. Compliance with data protection standards and privacy legislation such as GDPR, HIPAA, and FISMA necessitates tight data handling methods, privacy policies, and breach notification protocols. (Stallings, 2017)

Comprehensive information about data protection strategies, privacy impact assessments, and compliance requirements for e-government agencies can be obtained from authoritative sources like the European Data Protection Board (EDPB), International Association of Privacy Professionals (IAPP), and sector-specific regulatory bodies.

Incident Response and Recovery:

To successfully identify, respond to, and recover from cybersecurity events and data breaches, incident response and recovery skills are crucial. This part entails creating and carrying out incident response plans, forming incident management teams, holding routine exercises and training sessions, and coordinating incident response activities with pertinent parties. Forensic investigation, root cause analysis, remediation, and putting remedial measures in place to stop recurrence are examples of post-incident tasks. (National Institute of Standards and Technology (NIST), 2012)

In e-government systems, best practices for incident detection, response coordination, and recovery operations are provided in detail by industry standards like ISO/IEC 27035 and frameworks like the NIST Computer Security Incident Handling Guide (SP 800-61).

Continuous Monitoring and Auditing:

Proactive detection of security dangers, weaknesses, and compliance deficiencies within e-government systems is made possible by ongoing monitoring and auditing. This step entails implementing security information and event management (SIEM) solutions, intrusion detection systems (IDS), and vulnerability scanners to track system activity, evaluate security events, and create real-time warnings. Regular audits of security, penetration testing, and compliance assessments assist evaluate security policies, discover flaws, and assure regulatory compliance. (Krutz, 2003)

Resources such as the NIST Continuous Monitoring Guide (SP 800-137), CIS Controls, and industry-specific audit frameworks provide detailed instructions for implementing continuous monitoring systems, conducting security assessments, and enhancing overall cybersecurity posture.

2.7 The role of cybersecurity in E-government

In the age of digitalization, e-government technologies are the foundation of modern public service delivery, providing citizens with easy access to government services and information online. However, as government processes become more digital, the potential of cyber threats to the availability, integrity, and confidentiality of e-government platforms increases. In this

part, we will discuss the critical importance of cybersecurity in e-government and how strong security measures are required to protect digital governance.

Enhancing Trust and Confidence:

Because cybersecurity makes sure that interactions between citizens and government platforms are safe and dependable, it serves as the foundation of public confidence in e-government systems. Citizens are more inclined to use e-government services when they trust that their data is sufficiently safeguarded from cyber dangers. Successful interactions between governments and populations, transparency, and the general legitimacy of governmental institutions all depend on this trust. Effective cybersecurity measures also aid in preventing cyber incidents and data breaches, which can damage public faith in government institutions. (Lyytinen, Kalle, & Rossi, 2018)

Protecting Against Cyber Threats:

Cybercriminals can target e-government systems at a high frequency, using techniques such as ransomware, phishing, and malware. The confidentiality, integrity, and accessibility of governmental data and services are seriously jeopardized by these threats. Through the effective implementation of comprehensive cybersecurity measures, such as intrusion detection systems, network firewalls, and endpoint safeguards, e-government entities may effectively identify, mitigate, and avoid cyber threats. To find and fix any possible vulnerabilities in e-government infrastructures, regular security assessments and vulnerability scans are also crucial. (Roman, Rodrigo, & al, 2016)

Ensuring Data Privacy and Compliance:

Data privacy is an essential component of e-government, as government organizations handle massive volumes of private citizen data. Cybersecurity is critical to ensuring compliance with data privacy standards, such as the General Data Protection Regulation (GDPR) in the European Union and the Health Insurance Portability and Accountability Act (HIPAA) in the US. Encryption, access controls, and data masking techniques are critical for safeguarding sensitive information from unwanted access or exposure. By prioritizing data privacy and compliance, e-government enterprises may maintain citizens' trust while reducing legal and reputational risk. (Solove & J, 2006)

Supporting Digital Transformation:

Cybersecurity is a critical component in e-government's digital transformation path, allowing governments to use technology to provide effective and citizen-centric services. Secure-by-design concepts, such as embedding security needs into the planning and creation of e-government systems, can help reduce security risks from the start. Furthermore, risk-based methods to cybersecurity ensure that resources are efficiently deployed to address the most significant vulnerabilities and threats. Governments may construct resilient and safe e-government infrastructures by including cybersecurity into the digital transformation process at every level. (800-53, 2020)

Facilitating Secure Online Transactions:

Digital government platforms enable a variety of online transactions, such as tax filings, permit applications, and social benefit claims. Ensuring the security of these transactions is critical for protecting citizens' financial information and avoiding fraud. Strong authentication systems, such as multi-factor authentication and biometric verification, improve user account security and lower the likelihood of illegal access. Secure payment gateways and encryption mechanisms preserve sensitive financial data during transmission, ensuring people' privacy and trust in e-government services. (Chen, Liangliang, & al, 2017)

Building Resilience Against Cyber Attacks:

Continuity planning, which includes the creation of incident response frameworks and business continuity plans, aids e-government entities in effectively anticipating and responding to cyber incidents. Regular security assessments and penetration testing uncover vulnerabilities and weaknesses in e-government infrastructures, enabling organizations to proactively address security gaps. Governments can adopt a proactive approach to cybersecurity and build resilience against cyber threats, thereby minimizing the impact of cyberattacks and maintaining service availability for citizens. (Centre, 2021)

Promoting Collaboration and Information Sharing:

Cooperation and information exchange in the cybersecurity domain are essential for strengthening e-government organizations' overall defensive posture. Government agencies, industry partners, and cybersecurity experts may work together to successfully identify and

mitigate new cyber risks by exchanging threat intelligence, best practices, and lessons learned. Public-private partnerships promote innovation and information sharing, allowing governments to further bolster their cybersecurity capabilities by utilizing resources and sector experience. Furthermore, global cooperation and coordination enable cross-border threat reduction and response activities, guaranteeing a synchronized and cohesive strategy for cybersecurity in the e-government industry. (D'Onofrio, Stefano, & al, 2020)

2.8 legal framework of cybersecurity

The legal framework for cybersecurity is made up of an intricate web of rules, laws, and international agreements that are intended to combat cyberthreats, safeguard digital assets, and advance a safe and resilient online environment. Here is a summary of the main components of the cybersecurity legal framework:

2.8.1 National Legislation:

Many nations' legal frameworks for cybersecurity are based on national legislation. These laws provide the rights and obligations of people, corporations, and government agencies in terms of cybersecurity measures, data protection, incident reporting, and accountability for cyber incidents. They frequently handle concerns such as illegal computer system access, data breaches, cybercrime, and critical infrastructure security. (Green, G, & al, 2020) National legislation differs greatly between nations in terms of breadth, enforcement procedures, and punishments for noncompliance. These regulations play an important role in setting clear legal duties and supporting cybersecurity best practices across many industries. (Choo, K, & R, 2018)

2.8.2 Summary of Algeria's national laws and cybersecurity legal framework:

In order to combat cybersecurity and cybercrime, Algeria has passed a number of laws and regulations. Law No. 09-04 of August 14, 2009, which establishes precise guidelines for the prevention and prosecution of offenses relating to information and communication technology, is one of the important pieces of legislation. This legislation outlines a number of cybercrimes, including unauthorized access, device abuse, interference with data, and interference with systems. It also specifies cybersecurity precautions and sets fines for infractions. (Ministry of Justice, 2009)

Executive Decree No. 15-109 on April 25, 2015, which established the National Electronic Certification Authority (ANCE), is another significant rule. Digital certificate management and

the provision of secure electronic communications inside the nation are within the purview of the ANCE. emphasizing its contribution to the advancement of cybersecurity and confidence in online transactions. (Ministry of justice, 2015)

Ordinance No. 18-07 of July 25, 2018, which also deals with data protection and individual privacy while processing personal data, is another important document. This regulation, which attempts to protect personal data and guarantee its appropriate management in digital systems and surroundings, is strongly tied to cybersecurity issues. (Ministry of justice, 2018)

It is important to note that studies like Bellouki and Haddad (2019) have offered summaries of Algeria's cybersecurity environment along with an examination of pertinent policies and programs. Their work serves as a testament to the nation's attempts to create a thorough legislative framework that will fight cybercrime, advance cybersecurity, and conform to global norms and industry best practices. (Bellouki & Haddad, 2019)

Despite these efforts, there are still difficulties in putting these rules and regulations into practice and enforcing them since cybersecurity threats are always changing. strengthening Algeria's cybersecurity posture and guaranteeing the safety of digital assets and vital infrastructure need ongoing cooperation between public and private sector entities as well as foreign partners.

The legislation related to information and communication technologies in the country includes several key laws and decrees aimed at regulating this vital sector and ensuring its security and efficiency. Among these legislations, Law No. 09-04, issued on August 5, 2009, establishes specific rules for the prevention and fight against crimes related to information and communication technologies, providing a comprehensive legal framework to address cybercrimes and protect society from the risks of advanced technologies.

Law No. 15-04, issued on February 1, 2015, sets the general rules for electronic signatures and certification, enhancing trust in electronic transactions and ensuring the validity and acceptance of electronic signatures as a legally binding method. This law is a significant step towards promoting the digital economy and simplifying administrative and commercial procedures.

Law No. 18-07, issued on June 10, 2018, focuses on the protection of individuals in the processing of personal data, ensuring the confidentiality and security of personal information.

This law reflects the country's commitment to protecting citizens' privacy rights and aligns with international standards in this field.

Additionally, Ordinance No. 21-09, issued on June 8, 2021, addresses the protection of administrative information and documents, enhancing the security of sensitive data and protecting it from unauthorized access. This ordinance aims to strengthen transparency and accountability in public administration.

Presidential Decree No. 20-05, issued on January 20, 2020, establishes a national framework for the security of information systems to ensure the resilience and protection of IT infrastructures, ensuring the country's readiness to face cyber threats and maintain the continuity of government and private sector operations.

Finally, Executive Decree No. 19-271, issued on October 7, 2019, sets the national framework for the interoperability of information systems, promoting coherence and efficiency in the exchange of information between different systems. This decree enhances the ability of institutions to cooperate and integrate technologically, supporting sustainable development and improving the effectiveness of government services and national projects.

Data Protection Regulations:

Protection of information rules control how personal data is collected, processed, stored, and shared in order to preserve individuals' privacy rights. These rules seek to guarantee that enterprises manage personal data in a responsible and transparent manner, safeguarding it against unlawful access, disclosure, or abuse. (Union O. J., 2016) Data protection regulations normally require enterprises to put in place suitable security measures to protect personal information and notify individuals in the case of a data breach. Compliance with data protection legislation, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, is critical for enterprises seeking to retain the faith and confidence of their consumers and stakeholders. (Information, 2018)

Critical Infrastructure Protection:

Critical infrastructure protection laws and regulations seek to protect critical systems and resources, including energy, transportation, telecommunications, and financial services, against cyber-attacks. (Technology, Framework for Improving Critical Infrastructure Cybersecurity, 2018) These requirements compel critical infrastructure operators to deploy cybersecurity safeguards, perform risk assessments, and establish incident response capabilities to guarantee the resilience and dependability of vital services. Critical infrastructure protection legislation frequently includes sector-specific cybersecurity requirements, information exchange channels, and regulatory monitoring to meet the unique security risks that critical infrastructure sectors face. (Cybersecurity, EU NIS Directive: Overview of National Implementation Measures, 2020)

Cybercrime Legislation:

Cybercrime legislation includes offenses such as illegal access to computer systems, data theft, fraud, and other destructive behaviors carried out in cyberspace. (Crime, 2001)These laws provide law enforcement authorities the authority to investigate and punish cybercriminals, levy fines for cyber-crimes, and improve international cooperation in combatting cybercrime. Hacking, identity theft, online fraud, and virus distribution are all examples of cybercrime actions that may be subject to regulation. These laws are critical in preventing cybercriminal activity, safeguarding persons and businesses from cyber risks, and guaranteeing responsibility for cyber-related crimes. (Justice, 1986)

International Agreements and Treaties:

International treaties and agreements play an important role in developing international collaboration in the fight against transnational cyber threats and the promotion of cybersecurity standards. (Assembly, 2001) Treaties like the Budapest Convention on Cybercrime promote international cooperation in combatting cybercrime by unifying legal frameworks and improving law enforcement capacities across borders. Bilateral and multilateral agreements between governments encourage information sharing, capacity building, and collaborative efforts to handle growing cyber risks and concerns. International collaboration is required to successfully handle global cybersecurity threats while also guaranteeing cyberspace security and stability. (Europe, 2001)

Regulatory Compliance Requirements:

Organizations operating in certain industries or sectors are subject to cybersecurity duties and standards established by regulatory compliance requirements. (Council, 2016) These regulations demand the deployment of security measures, risk assessments, and incident response protocols in order to secure sensitive data, preserve vital infrastructure, and reduce cyber threats. Specific standards for securing payment card data and personal health information are established by compliance frameworks like the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA), respectively. In order to reduce legal and financial risks, uphold consumer trust, and exhibit due care in cybersecurity, firms must adhere to regulatory regulations. (Services, 1996)

Government Cybersecurity Strategies:

The goals, objectives, and actions for strengthening cybersecurity resilience, thwarting cyberattacks, and fostering a safe and resilient cyberspace are outlined in government cybersecurity plans. In order to fully address cybersecurity concerns, these solutions frequently entail collaboration with a variety of stakeholders, including government agencies, corporate partners, academia, and civil society. (Security U. S., 2018) Initiatives to improve the security of key infrastructure, share threat intelligence more effectively, raise public awareness of cybersecurity challenges, and encourage international collaboration on cybersecurity matters are all common components of government cybersecurity plans. Governments may better safeguard their people, companies, and important assets from cyber-attacks and maintain the safety and stability of cyberspace by giving cybersecurity top priority at the national level. (Australia, 2020)

Regulatory Authorities and Enforcement Agencies:

When it comes to monitoring adherence to cybersecurity rules and regulations, looking into cyber events, and imposing sanctions for non-compliance or cybercriminal activity, regulatory bodies and enforcement agencies are essential. These businesses may be subject to audits, fines, and punishments if it is discovered that they have violated cybersecurity regulations. (Agency, n.d.) Additionally, regulatory bodies and law enforcement agencies are essential in helping firms

strengthen their cybersecurity posture and successfully counteract cyber-attacks by offering advice, resources, and assistance. Effective regulation and enforcement of cybersecurity rules and regulations need cooperation between regulatory bodies, law enforcement organizations, and other relevant parties. (Cybersecurity, About ENISA, n.d.)

2.9 The most common types of cyber-attacks on e-government systems

In the digital era, governments throughout the world are increasingly relying on electronic platforms to provide efficient and transparent services to their residents. However, this reliance on technology exposes e-government systems to a wide range of cyber-attacks, endangering confidential data, operational integrity, and public trust. Understanding the most frequent forms of cyber assaults on e-government systems and adopting effective mitigation methods are essential steps toward protecting these vital infrastructures.

Common Cyber Threats to E-Government Systems:

Malware: Malicious software, such as viruses, worms, and Trojans, is a major danger to e-government systems. Malware is intended to disrupt operations, undermine data integrity, or obtain unauthorized access to critical information. (Doe, 2020)

Phishing: Cybercriminals use phishing techniques to trick government officials and others into disclosing sensitive information, such as login passwords or financial information, via bogus emails, texts, or websites. (Smith J. , 2019)

SQL injection attacks exploit weaknesses in online applications, allowing hackers to alter databases, execute illegal instructions, or steal sensitive data from e-government systems. (Johnson A. , 2018)

DoS and DDoS attacks: DoS and DDoS attacks interrupt services by overwhelming e-government servers or networks with traffic, making them unavailable to genuine users. (Brown, 2017)

Ransomware: Ransomware prevents access to electronic government systems by encrypting data and holding it hostage until a ransom is paid. This type of cyber-extortion can lead to large losses in terms of money as well as disruptions in business. (Johnson M. , 2021)

Supply Chain Attacks: Supply chain attacks, which target third-party suppliers and service providers linked to e-government networks, take use of supply chain weaknesses to obtain illegal access and threaten system integrity. (Williams, 2019)

Insider Threats: Malicious or careless activities by personnel with authorized access to e-government systems are a serious insider threat. These insiders may actively leak sensitive information, sabotage systems, or unintentionally reveal weaknesses. (Jones, 2016)

DNS Tunnelling: Cybercriminals can create secret communication channels to exfiltrate data or carry out harmful orders within e-government networks by using DNS requests and answers to get beyond typical security measures. (Anderson L. , 2018)

IoT-Based Attacks: As Internet of Things (IoT) devices proliferate, more avenues for attack are opened up for e-government systems. Hackers can jeopardize network integrity and obtain unauthorized access to sensitive data by taking advantage of flaws in IoT devices. (Smith R. , 2022)

2.10 Role of stakeholders in ensuring cybersecurity in e-government

Various parties must work together in a coordinated and cooperative manner to ensure cybersecurity in e-government activities. Government organizations and legislators are essential in creating and implementing cybersecurity laws, rules, and policies as well as providing funding and setting up governance structures. Risk assessments, technical advice, and the design, implementation, and maintenance of strong security systems are the responsibilities of cybersecurity specialists and professionals. (Sá, Rocha, & Cota, 2016) System and IT administrators oversee the underlying infrastructure, apply security upgrades, and keep an eye out for any risks to the systems. End users—citizens and companies alike—contribute by following cybersecurity protocols, disclosing events, and staying informed about potential security risks. (Gupta, Yamaguchi, & Nomura, 2018)

Private sector partners and vendors are crucial in developing and providing secure hardware, software, and services, collaborating with government agencies to ensure the security and integrity of their solutions. Academic and research institutions conduct research on emerging threats, provide expertise, and develop training programs to build a skilled cybersecurity workforce. (Soomro, Shah, & Ahmed, 2016) International organizations and standard bodies

establish global standards, facilitate information sharing, and provide guidance for capacity-building initiatives. Effective collaboration and clear communication channels among these stakeholders are essential for implementing a comprehensive and robust cybersecurity strategy that addresses the evolving challenges faced by e-government systems in the digital age. (Weerakkody, Dwivedi, & Kurunananda, Implementing e-government in Sri Lanka: Lessons learned from the UK, 2009)

Conclusion of the chapter:

In employing these qualitative data collection methods, we aim to uncover the multifaceted dimensions of cybersecurity in e-government from its technical implementations to its organizational and societal implications. By triangulating data from observations, document analysis, interviews, and bibliographical references, we seek to provide a nuanced and holistic understanding of how cybersecurity influences the functioning and security of e-government systems .

CHAPTER 2: DATA AND METHODS

The second chapter provides an overview of the case study background by presenting a detailed account of the organizational history and missions of the Scientific and Technical Information Research Center (CERIST). The context is essential for comprehending the particular setting in which the research is carried out. The chapter subsequently introduces the methodological framework employed in the study, elucidating the qualitative research design and the justification for selecting CERIST as the case study. The text outlines the data gathering techniques employed, such as semi-structured interviews, document analysis, and direct observation. It elucidates how these procedures enhance the overall comprehension of the study inquiries**.**

Section 1. Case study context

The next chapter describes the CERIST organizational context using data from various documents and information gleaned from the company itself. It also includes a methodological framework that includes qualitative study, as well as information about the research's procedures and an epistemological approach.

1.1 CERIST Organizational History

The Research Centre on Scientific and Technical Information, CERIST, in Ben Aknoun, Algeria, is a leading institution dedicated to advancing research and innovation in science and technology. it Was created in 1985 by virtue of the decree No 85-56 of March 16th, 1985. Under the aegis of the Prime Minister, the CERIST had to undertake any research related to the creation, the setting up and the development of a national scientific and technical information system.

Later on, the CERIST joined the "Haut Commissariat à la Recherche" according to the decree No 86-73 of April 08th, 1986.

Currently, the CERIST is a scientific and technological public institution placed under the aegis of the Minister of Higher Education and Scientific Research by virtue of the decree No 03-454 of December 1st, 2003.

The CERIST is organized in administrative and technical departments and research divisions. Besides the head office located in Algiers, the CERIST has regional sites and representations across the country.

CERIST plays a crucial role in the development and dissemination of scientific knowledge, as well as in supporting Algeria's efforts to strengthen its research and technological capabilities.

CERIST's primary objective is to foster research excellence and promote the application of scientific findings to address societal challenges and contribute to national development goals. The Center conducts multidisciplinary research across various fields, including information and communication technologies (ICTs), biotechnology, renewable energy, environmental sciences, and more. Through its research activities, CERIST seeks to generate new knowledge, develop innovative solutions, and facilitate technology transfer to industry and other sectors.

One of CERIST's key functions is to serve as a hub for scientific information and technology transfer. The Center operates several specialized units and laboratories that engage in cutting-edge research, technology development, and capacity-building activities. These units focus on areas such as data mining, cybersecurity, bioinformatics, remote sensing, and knowledge management, among others. By leveraging state-of-the-art facilities and expertise, CERIST contributes to the advancement of scientific knowledge and the enhancement of Algeria's research infrastructure. (CERIST, about us , 2024)

CERIST plays a vital role in promoting collaboration and partnerships among researchers, academia, industry, and government agencies, both nationally and internationally. The Center facilitates networking opportunities, joint research projects, and knowledge-sharing initiatives to foster innovation ecosystems and address global challenges collaboratively. Through its collaborative efforts, CERIST aims to strengthen Algeria's position in the global scientific community and contribute to regional and international scientific cooperation.

CERIST is committed to promoting science, technology, engineering, and mathematics (STEM) education and training to build a skilled workforce capable of driving innovation and sustainable development. The Center offers various capacity-building programs, workshops, and seminars to support researchers, students, and professionals in acquiring new skills, staying abreast of emerging trends, and enhancing their competencies in scientific research and technological innovation.

In summary, CERIST plays a pivotal role in Algeria's scientific and technological landscape, serving as a catalyst for research excellence, technology transfer, and innovation. With its

multidisciplinary approach, state-of-the-art facilities, and commitment to collaboration and capacity-building, CERIST contributes significantly to advancing knowledge, fostering economic development, and addressing societal challenges in Algeria and beyond.

functions as a regional center of representation for seven wilayas, demonstrating its impact and scope across the nation. Among these wilayas are Tizi Ouzou, Béjaïa, Ouargla, Constantine, Oran, and Setif. Cerist's dedication to serving and supporting different populations, enabling technical growth, and promoting innovation throughout Algeria is demonstrated by its presence in these varied locations. (CERIST, about us , 2024)

In CERIST, cybersecurity is considered a top priority, with the center developing and implementing advanced strategies and solutions to protect against cyber threats and ensure the safety of data and critical systems. The Cybersecurity Laboratory at CERIST provides consultancy and technical services in cybersecurity to various sectors, including government, industry, and academia. (CERIST, 2022)

CERIST's efforts in cybersecurity include:

Research and Development: Researchers at CERIST study modern cybersecurity challenges and develop effective solutions to address them. Research and development areas in the laboratory include intrusion detection, malware analysis, encryption and access control tool development, and countering advanced cyber-attacks. (Benmohammed, 2018)

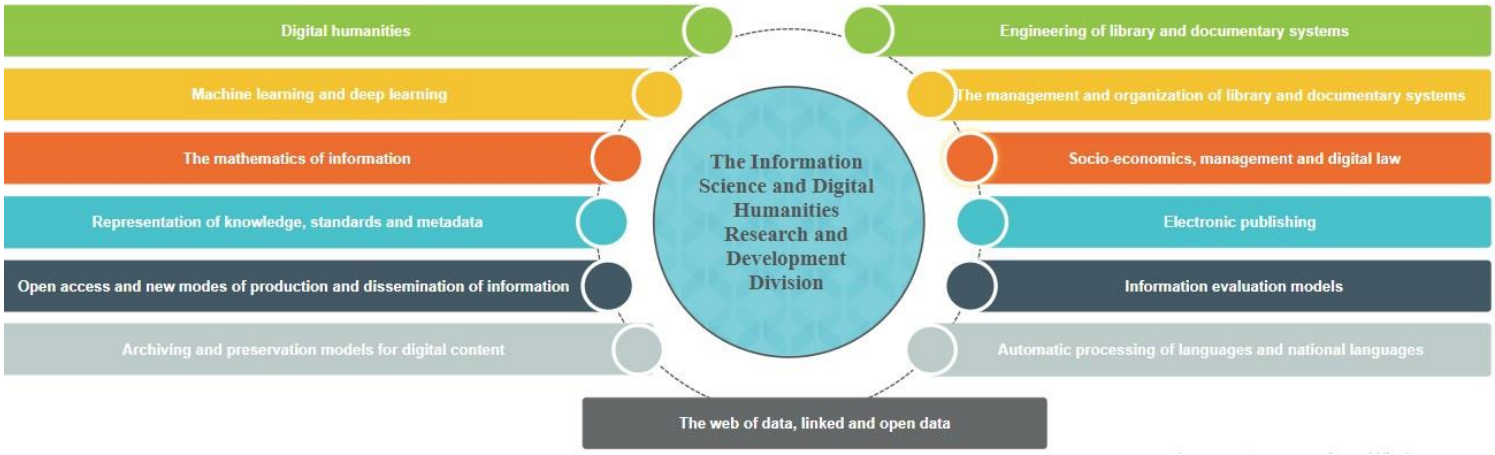
Training and Awareness: CERIST offers training courses and workshops in cybersecurity to increase awareness and enhance skills among professionals in various sectors. This training aims to improve the ability to detect and mitigate cyber threats effectively. (Moussaoui, 2019)

Consultancy Services: The Cybersecurity Laboratory at CERIST offers customized consultancy services to institutions and companies to help them assess cybersecurity risks and implement appropriate protection strategies. (Ministry of Post and Information and Communication Technologies, 2020)

National and International Collaboration: CERIST works to enhance collaboration with national and international institutions in the field of cybersecurity through knowledge and experience exchange and participation in joint research projects. (CERIST, 2021)

As a leading center for scientific and technological research in Algeria, CERIST's efforts in cybersecurity significantly contribute to enhancing the country's cybersecurity infrastructure and its ability to address increasing cyber threats.

Figure 6: Missions of ISDHRD Division



Source: Created by us using (MERAD, 2024)

1.2 Missions of CERIST:

The Research Centre on Scientific and Technical Information is in charge of the fulfilment of research and development programs in the scientific and technical information field and their missions are:

• Guide any research action related to the creation, the setting up and the development of the national scientific and technical information

• Promote the research in the scientific and technical information field and take part in the development of such fields.

• Contribute to the coordination and the setting up of national scientific and technical information programmes in liaison with the concerned sectors.

• Take part in the edification and promotion of the information society by setting up and developing specialized information networks especially the academic and research network and insuring their connectivity with other international networks as well as the development and the propagation of information and communication techniques in connection with higher education activities.

• Take part in the modernization of the national academic documentation system by setting up digital libraries.

• Gather the necessary tools to build up national databases in science and technology fields and insure their dissemination.

• Promote the research in information security and networks field. (Missions CERIST, n.d.)

Missions under the heading of CERIST:

Research Domains

Research Areas

CERIST is active in the following areas:

- Networks and distributed systems
- Information and multimedia systems
- Sciences of information
- Theories and engineering of computer systems
- IT security

Research Divisions

Information security is an important challenge in the field of new information technologies.

Regarding the important place occupied by the new information technologies in modern societies, information security is nowadays present in the areas of systems, contents and services in order to prevent, identify and reduce malicious attacks. The information security task is to ensure the integrity, the confidentiality, the availability and the traceability of data and their process. Security is an essential element in all Computer systems.

The Division of computer security is mainly aiming to acquire expertise and to suggest solutions to ensure a smooth operating of computer systems and to protect those systems from intruders.

The division seeks to participate in the development of the national network of scientific and technical information by leading research and development projects, and training.

The computer security division teams work includes all of the following areas: systems, networks, data and applications. (Khiati, 2013)

Theories and engineering of computer systems

The division computer systems theory and engineering explore the emergent problems related to the next generation infrastructures and distributed and pervasive systems. We focus on the dynamic interactions and the wide scale resources sharing among the different communities and organizations combining computing power, data, and human knowledge.

Research and Development in Information Sciences The evolution of the Internet and the development of digital tools have revolutionized the production and the use of information in general and Scientific and Technical Information in particular.

The Scientific and Technical Information is the basic building block of society knowledge and thus, it becomes a digital content that must be made intelligible to everyone

according to their specific needs while controlling the legal and the socio-economic environment related to digital technology.

With its multidisciplinary components and researchers specialized in computer science, mathematics and humanities, the Division of Research and Development in Information Science is striving to offer large corpus analysis tools including Arabic language, using techniques of Automatic Language Processing and Artificial Intelligence. The division also proposes mathematic models for the evaluation of information and modelling digital uses, along with a

national approach of STI strategic intelligence, conducting reflections on open access, new business models and the legal framework of STI and ICT. (Khiati, 2013)

Multimedia and information systems. The division of multimedia and information systems is a division of research and development. In the terms of research, the division is responsible for conducting projects on information modelling, information structuring, information management methods, and means to be implemented to manage information (information retrieval, storage…)

In the terms of development, we design IT projects integrating multimedia information, to acquire, organize, manage, distribute and access to multimedia type of information in information systems. The division also elaborates the design and implementation of information systems of decision aids for organizations using new sciences and management information technologies as well as studies, such as information technology master plans, specifications, IT audit and specific software development. (Bakhouche, 2006)

Networks and Distributed Systems. Technological advances in networking and e-infrastructures require in-depth follow-up and technological follow allowing the development of major projects of national importance and insuring scalability and openness to new communication and interconnection services of systems and networks.

The activities of the Division of Networks and Distributed Systems target to study, master and introduce technologies associated with e-infrastructures.

These e-infrastructures induce mastering of communication technologies and developing new application architectures such as CLOUD and GRID technologies which aim to share resources in terms of computing power and storage.

These activities aim to establish e-infrastructures such as the Algerian Research Network (ARN) and the National Computing Grid “DZ e-Science GRID” and to consolidate the skills and technological know-how.

Innovative Research Projects

Restoring old Algerian manuscripts. This project aims to restore the old Algerian manuscripts held by the National Center of Manuscripts of Adrar. The state of these manuscripts is so

deplorable that it is essential to intervene to stop their degradation and try to remedy the damage incurred.

Wireless sensor networks for irrigation control. This project aims to provide a system based on wireless sensor networks that can:

- Demonstrate the efficiency of irrigation water management.
- Avoid costly effects on the environment caused by improper practices observed in the management of irrigation water in traditional systems.
- Allow the development of agriculture and regeneration of water resources.

DZ-CERT Algerian Computer Emergency Response Team.

The **DZ-CERT** mission is to assist the Algerian community in improving communications and systems safety and to reduce the risk of security incidents.

DZ-CERT aims to be a national center for the collection and spreading of information related to threats, vulnerabilities, and incidents affecting computer networks. It ensures the development of IT security in Algeria and risk minimization in coordination with international CERTS.

TELELT

TELELT is a project that uses ICT to manage problems that arise following a disaster.

TELELT contributes in the establishment of a disaster management national information system.

National Research Programs -PNR-(2011-2013)

Information and Communication Technology -National Research Programs

Fundamental computer science - National Research Programs - (CERIST, Research & Developement, 2024)

Services of CERIST:

Advise & expertise:

- Setting up of an intranet network (wiring, network administration and configuration)

- Setting up of various computer services (mail, ftp, DNS…)
- Installation of machines.
- Assistance in drawing up specifications
- Technical assistance (computer, software, documentation)

Audiovisual & Multimedia Internet:

- Covering seminars within the CERIST and outside the CERIST
- Realization of documentary film and Reportage
- WebTV broadcast channel of CERIST.
- Mastery of filmmaking process (documentary and Reportage)
- screenwriting
- Shooting and sound recording
- Editing
- Publication on the CERIST WebTV
- Design and production of websites
- Design and development of Information Catalogues
- Computer graphics (design. Etc.)
- Production of interactive CDs

Networks & Internet:

In the field of networks and network services:

- The development of infrastructure networks.
- The Academic and Research Network ARN: www.arn.dz
- The Wissal Internet at a National level: www.wissal.dz
- Management of DZ domain name for Algeria: www.nic.dz

Networks under Intranet / Extranet / Internet:

- Mail, authentication, domain management systems, ...
- Videoconferencing and audio / video streaming systems

In the field of information networks:

- Dynamic web services and e-services
- Informational and documentary networks: e-library
- E-learning systems
- E-commerce systems and e-banking platform
- Information networks security

Library:

- Access to the data base and scientific publications of the CERIST.
- Selective Dissemination of Information (SDI).
- Development of press files and Dissemination of documentary products.
- Enhancement of CERIST's scientific heritage.
- Provision with primary documentation.
- Analyses of journals and development of specialized bibliographies.
- Selective dissemination of information through profiles management.
- Acquisition of work and purchasing books Suggestions.
- Watch and prospecting.
- Online subscription to databases.
- Support tools for library automation.
- Audiovisual animation.
- Inter library loan.
- Receive, inform, guide and monitor trainees' group

Scientific and Technical Information:

The Department of STI offers:

- A range of bibliographic databases covering most fields of science and technology.
- The basics of bibliographic data of reporting and localization of primary documents available at participating libraries to projects of the collective national catalogues.
- 450,000 microfiche documents, representing all production of the IAEA (International Atomic Energy Agency).
- Part of the national theses fund (FNT), under construction.

- A large collection of periodicals including a section on CD-ROM.
- Provision of primary documents upon request, through agreements with foreign documentaries institutions.

Register under .dz domain name

The management of registrations under .dz domain names is an activity that was initiated by the CERIST since the introduction of Internet in Algeria in 1994.

The registration of domain names in the registry .DZ is supported by the NIC.DZ cost-free to registrars for the benefit of applicants. The registration procedure must be done online via the website: http://www.nic.dz/ **22/05/2024**

Register under Algeria. domain name

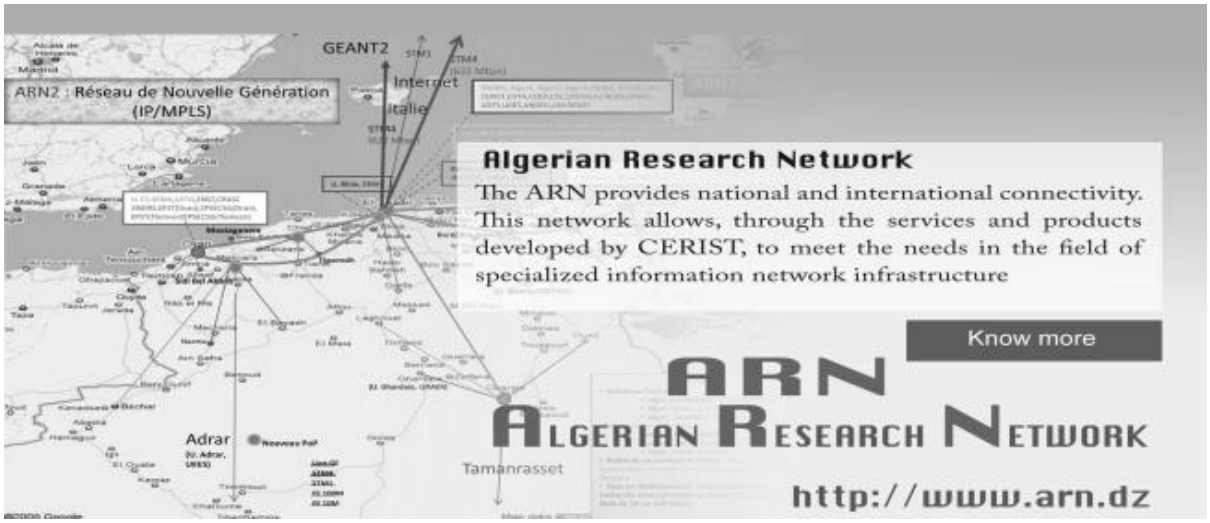
Domain Management. Algeria

The registration of domain names under Algeria. is supported in the same manner as domain names under.DZ. Registration procedures are listed on the site: http://www.nic.dz/ named: Center for domain names. Algeria

The ARN Network

ARN

Figure 7 :Algerian Research Network



Source: (Cerist , 2024)

ARN targets:

- The development of the communication infrastructure.
- The integration of all document structures in order to build a technologic and software infrastructure.
- The development of the technologic infrastructure for distance learning.
- The integration of scientific computing means to build a computing network "GRID".

The ARN network includes all institutions in the field of science and technology. It is a national research network, interconnected to foreign networks of research and to internet.

National computing Grid: DZ e-Science GRID

The infrastructure of national scientific computing Grid aims to meet the needs of scientists that rely on computing and storage means in their scientific work.

Dz e-Science GRID, initiated in 2006 and accessible through the ARN network, Z e-Science GRID aims to:

- Gather a set of resources (CPU and storage disks)
- Ensure the overall management of infrastructure for the access to the grid (authentication & authorization) and the allocation of resources,
- Keep the overall system operational through a package of monitoring services, organize and manage virtual organizations (VOs) through the website voms.grid.arn.dz.

DZ e-Science CA

The infrastructure for managing digital certificates is operational since September 2011. DZ e-Science CA produces and issues digital certificates to authenticate people, servers, and services integrated into the national grid DZ e-Science GRID. The created DZ e-Science CA is also approved by international GRID authorities.

Figure 8: Logo of Cerist

Source: Cerist Website

Section 02. Methodological framework (Qualitative Approach)

In the next section, we provide a high-level overview of the steps we took to conduct our research. First, we explain our chosen methodological approach, which uses qualitative research methods to collect and analyze data, we then identified the study population, which included participants from various backgrounds and age groups. We also discuss how we select participants and the criteria we use to ensure they are suitable for our study. Finally, we review

the data collection tools we used in our research, including surveys, interviews, and observations. We explain how we develop these tools to collect relevant data and how we ensure their validity and reliability and analysis.

2.1 Presentation of the research methodology

To address the research topic and achieve the goals of the study, we have opted for a qualitative approach, focusing solely on qualitative methodologies.

Meaning of research. Significance of scientific inquiry. "Re" and "search" are the two parts of the word "research." "Re" is a prefix that means "again," "new," or "over again," while "search" is a verb that means "to examine closely and carefully," "to test and try," or "to probe." In essence, research is the process of seeking for information, explanations, and solutions to problems. Its goal is to investigate theoretical assertions regarding the assumed relationships between various phenomena by methodical, controlled, empirical, and critical study. A problem may be identified, a hypothesis can be developed, data can be gathered and examined, and conclusions that address the current situation or improve theoretical formulations in a more general sense can be reached through research. (Walliman, 2017)

The qualitative research. According to Flick (2018), qualitative research entails immersing the observer in the reality and employing a range of interpretative strategies to make it apparent. These tools, which include field notes, interviews, pictures, recordings, and self-reflection memos, turn the environment into a collection of representations. This research style is naturalistic and interpretative because it examines objects in their natural environment and attempts to understand them in terms of the meanings that people assign to them.

Understanding a social or human phenomena necessitates providing a comprehensive and in-depth viewpoint utilizing diverse approaches, as well as a detailed assessment of the setting in its natural environment. This is the core of a qualitative research approach. This method assists academics in obtaining a greater grasp of a certain issue that has just arisen as a study subject and is still poorly understood. It also stresses understanding the subject topic from a humanistic or philosophical perspective. (Islam, Baikady, & Ahmed Khan, 2022)

2.2 Reason for choosing the qualitative approach

The choice of a qualitative approach for this dissertation stems from several key reasons. Firstly, qualitative research allows for a deep and nuanced exploration of complex phenomena such as cybersecurity within the context of e-government. By using qualitative methods such as interviews, focus groups, and case studies, we can gain rich insights into the perceptions, experiences, and behaviors of stakeholders involved in e-government initiatives and cybersecurity practices. Additionally, qualitative research enables us to uncover the underlying meanings, motivations, and contextual factors that influence the effectiveness and challenges of cybersecurity measures in the e-government domain. This approach is particularly suitable for understanding the multifaceted nature of cybersecurity risks, governance issues, and the socio-technical dynamics inherent in e-government systems. Furthermore, qualitative methods offer flexibility in adapting to emergent themes and exploring unexpected findings, allowing for a holistic understanding of the complexities surrounding cybersecurity in e-government. Therefore, the qualitative approach chosen for this dissertation provides a robust framework for investigating the intricate relationship between cybersecurity and e-government, offering valuable insights for policymakers, practitioners, and researchers in the field.

In this study, we have adopted a sequential exploratory approach to investigate the role of cybersecurity on e-government services. Initially, we will conduct qualitative research to gain a comprehensive understanding of the phenomenon under study. This approach is particularly suitable for our research context as it allows us to delve deeply into the perceptions, experiences, and practices of stakeholders involved in e-government initiatives and cybersecurity measures.

2.3 Research design strategy

Given the complex and evolving nature of cybersecurity in the context of e-government, qualitative research will provide valuable insights into the challenges, strategies, and implications of cybersecurity implementation. Through methods such as in-depth interviews, focus groups, and document analysis, we aim to capture rich, context-specific data that can inform subsequent phases of the study.

Following the qualitative phase, we will use the findings to inform the development of quantitative research tools, such as surveys or structured questionnaires. This sequential

approach ensures that the quantitative data collection instruments are tailored to the specific needs and insights identified during the qualitative phase.

2.4 Data collection tools

There are four basic techniques for data collection in qualitative scientific research, namely: individual interview, group interview, observation and documentary analysis.

Given that the qualitative approach of this dissertation aims to delve deep into understanding the role of cybersecurity in e-government services, we have carefully selected specific qualitative data collection methods.

In this section, we'll go over the observation, interviews, and bibliographical references that we employed as our instruments for gathering qualitative data.

Observation:

In the observation method, the degree of participation of the researcher in the work of the study members varies depending on the type and nature of the research. The study can be participatory, or the researcher can take a distance from the participants and play a spectator role during the information collection period. There are two types of observation:

Quantitative observation

The researcher will gather digital information through tools prepared in advance, for example, the number of students interacting in the classroom, the numbers of displaced persons crossing borders, the calculation of the time required to complete the border process.

Qualitative observation

Qualitative observation is less structured, since the researcher does not use predetermined classifications or patterns, but automatically records his observations, capturing reality as it progresses. The basic idea here is the classification and description of the information generated by the observation. (Mack, Woodsong, MacQueen, & Namey, 2005)

Observation serves as a fundamental tool in our qualitative research methodology. By observing the operations, protocols, and behaviors within e-government environments, we aim to gain rich insights into how cybersecurity is implemented and its effects on daily practices. Through

structured observations in e-government settings, we can directly witness the application of cybersecurity measures and identify any challenges or successes encountered by employees and stakeholders. This firsthand observation allows us to capture nuances and contextual details that may not be evident through other data collection methods.

Document Analysis:

Document analysis is integral to our qualitative research strategy as it allows us to examine existing policies, reports, guidelines, and other documents related to cybersecurity and e-government initiatives. By analyzing these documents, we can understand the formal frameworks, strategies, and priorities set by government agencies regarding cybersecurity. Moreover, document analysis enables us to uncover the historical evolution of cybersecurity practices in e-government, providing valuable insights into trends, challenges, and areas for improvement. (Bowen, 2009)

Interview:

Interviewing is a method commonly used to address sensitive subjects, personal experiences, or to deepen understanding of the attitudes and perspectives of individuals in society. It enables them to learn more about the participants' thoughts, feelings and points of view. The researcher can also reconstruct social events through the answers obtained during interviews. This method is based on building confidence between the researcher and the research participant, in order to guarantee the credibility and accuracy of the answers. (Seidman, 2006)

There are two types of interviews: direct and semi-direct.

Directive interview

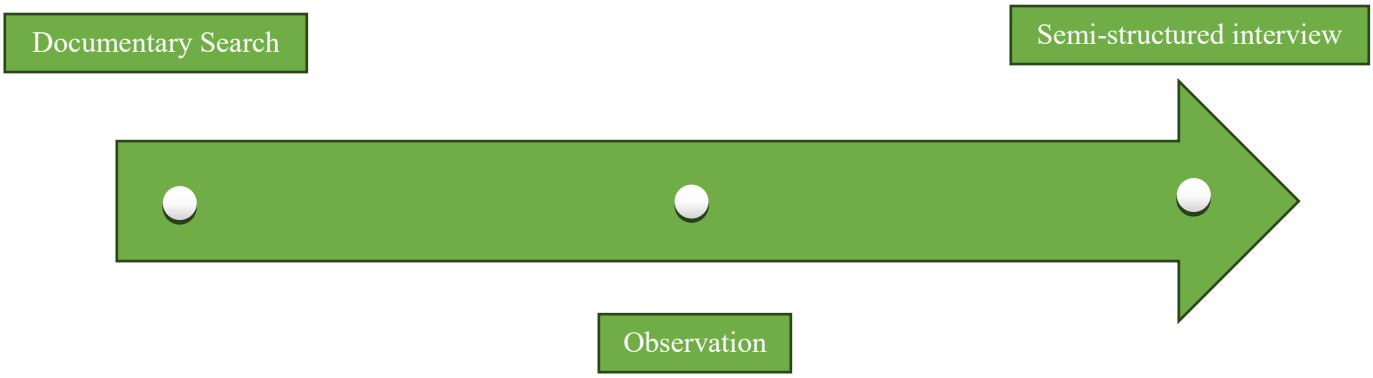
The direct interview consists of asking a series of questions to the participants, all receiving the same questions in the same order and the same way prepared in advance. The researcher must be neutral, focusing on rational rather than emotional issues. Answers can be precise in advance and open questions can be used to allow participants to answer freely.

Semi-directive interview

Semi-direct interview, on the other hand, is a form of unstructured interview, with open and in-depth questions. The role of the researcher is closer to that of a dialogue director than a

correspondent. This type of interview allows the researcher to understand participants' thinking and behavior without reference to previous assumptions, which can limit participants' words and interaction. (Rubin & Rubin, 2011)

Figure 9: Data collection tools



Source: Prepared by ourselves (Madjed, 2016)

Semi-Structured Interviews:

Semi-structured interviews are a key component of our qualitative data collection strategy, providing an opportunity to explore the perspectives, experiences, and perceptions of stakeholders involved in e-government and cybersecurity. Through in-depth interviews with government officials, IT professionals, policymakers, and other relevant actors, we seek to understand their views on the current state of cybersecurity in e-government, as well as the challenges, priorities, and potential solutions. The flexibility of semi-structured interviews allows for probing into specific topics while also allowing participants to share their insights and concerns freely.

The Interview guide:

The interview guide is a list of questions or themes that act as a guide for conducting semi-structured interviews with research participants. It is sometimes referred to as an interview procedure or interview schedule. It is an essential tool in qualitative research since it allows for freedom in exploring emergent themes and following up on pertinent replies, while also assisting

in ensuring consistency across interviews. (Patton, 2015) Typically, an interview guide consists of the following elements:

An interview guide usually has the following components:

Introduction:

A brief summary of the research effort and its aims

- The purpose of the interview
- Assurance of secrecy and anonymity.
- Explanation of the interview procedure, including the anticipated time and the use of audio/video recording (where appropriate).
- Participants have the opportunity to ask questions before commencing.

Background/Demographic Questions:

- Questions for gathering useful background information about the participant, such as their job title, role, experience, or other relevant demographic facts.

Main Interview Questions:

- Open-ended inquiries on the study questions or themes.
- These questions should be structured logically, beginning with broad, general queries and progressively progressing to more detailed or difficult ones.
- Follow-up probes or prompts can be used to encourage participants to expound on their comments or give further details.

Closing:

- The last open-ended question allows participants to express any further comments or observations.
- Thanking the participant for their time and contribution
- Information about future steps or follow-up, if relevant

When creating the interview guide, it is critical to ensure that the questions are clear, neutral, and in line with the study objectives. The guide should act as a flexible framework, allowing the

interviewer to change the sequence or wording of questions as required and explore emergent topics or themes during the interview. (Castillo-Montoya, 2016)

It is also advised to conduct pilot or practice interviews to improve the interview guide and ensure that the questions are understandable and effective in generating meaningful and insightful replies from participants.

Bibliographical References:

To enrich our understanding of cybersecurity and e-government, we rely on a wide range of academic literature, research articles, and official reports. Sources such as academic journals, government publications, and industry reports provide theoretical frameworks, case studies, and empirical evidence that support our analysis of the topic. By synthesizing information from diverse sources, we aim to develop a comprehensive understanding of the complexities surrounding the role of cybersecurity in e-government services. (Wyld & Baker, 2020)

Data collection equipment

To guarantee extensive and accurate data collection, we employed a range of techniques, including filming the interviews with our own phones, taking notes on our laptops and notebooks throughout the interviews to record essential information, and highlighting key points. by collecting data on computers and phones, we were able to capture a wide range of information that would otherwise go unreported. and guaranteeing the privacy and confidentiality of the information gathered. (Musselwhite, Cuff, McGregor, & King, 2007)

2.5 The research sample (qualitative research)

Selecting the right people to answer your research questions at the beginning of a project might be tough. In general, researchers seek out competent individuals who may throw light on the issue at hand, as well as those who have opposing viewpoints. The term "sampling" is commonly used to describe a procedure in which the "right" instances are randomly selected from a known pool of cases.

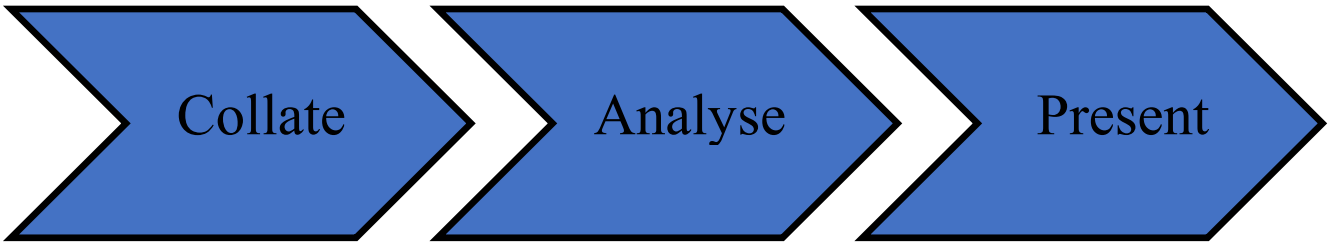
But with qualitative research, especially when interviews are involved, the process is often iterative. As researchers get to know the subject and its people better, their methods for choosing and sampling participants may change based on their evolving views of who has the most relevant expertise and unique perspectives. In qualitative research, sampling usually does not refer to the formal, random selection of a sample from the real or anticipated population. Rather, it comprises selecting specific examples, objects, or events that will assist researchers in creating a valuable corpus of empirical samples for studying the subject of interest. Because of this, most recommendations for qualitative sampling are focused on accomplishing certain goals. (Flick, 2018)

The table provides a profil of the respondents' names, employment positions, and the duration of their interviews, allowing for a clear understanding of their roles and the amount of time they were engaged in the interviews.

Table 3: The Profiles of The Interviewees

Name	Job position	Duration of the interview
Mr. Bouabid	RSSI (Information system security responsible)	50 min
Ms. Amira	Expert researcher	45 min
Mr. Krinah	Expert researcher	30 min
Mr. Saidi	Expert Researcher in Information Security.	30 min

Qualitative data analysis



Reliability Ensure that the source data is comprehensive and trustworthy during the investigation.	**Coding** Applying codes to streamline and establish uniformity in data for analytical objectives	**Agree purpose and format** Concise and specific scope and question. Ensure that the format is appropriate for the intended audience
Reshaping Organizing chaotic data into a standardized and practical manner	**Annotating** Highlighting the aspects that you deem to be the most important	**Validity** Describing potential bias, methods followed and any subjective conclusions
Reducing Eliminating extraneous noise that is unrelated to the research.	**Labelling** Categorizing data to facilitate efficient grouping	**Interpretation** Providing an explanation of the potential implications and underlying motifs of the analysis.
Transforming Converting data into a more manageable format	**Selection** Selecting compelling, meaningful, or exemplary materials to exemplify an argument	**Conclusions** Answering the research question and making recommendations
	Summarizing Selecting one or many samples to serve as a summary of the entire dataset.	

Source: (Cox, 2014)

Data compilation: involves the systematic gathering and organizing of information from diverse sources, including but not limited to interviews, personal reflections, existing literature, secondary data, documents provided by participants, and visual materials such as images or diagrams. This process includes verifying the accuracy of the collected data, filtering out personal or extraneous details, excluding casual conversation that does not contribute to the research objectives, restructuring the data for better organization and analysis, and adding contextual information to highlight important insights and enhance comprehension. (Creswell J. W., 2017)

Data Analysis: Data analysis involves organizing, structuring, and thoroughly examining data. Transcripts serve as a crucial source of information in this process. The analysis process includes categorizing, coding, counting, and mapping the data, which divides qualitative data into distinct sections and assigns each section a reference. Categorization aids the coding process, helping to generate data points that confirm or refute theories or premises in the final findings. Coding enables researchers to locate important data and establishes the framework for deriving conclusions and understanding meaning. Counting reveals interesting trends and linkages within the data, aiding in answering research questions and producing more reliable results. Finally, mapping the data aids in presenting the data sets, their relationships, and analysis, enhancing the understanding of the problem and the process's outcomes for both the researcher and the reader. (Miles, 2014)

Data Presentation: Data presentation involves organizing and condensing data to enable readers and researchers to draw conclusions and be motivated to take further action. By displaying information using matrices, graphs, charts, and networks, researchers can illustrate how various data points are interconnected. During this phase, the research question is addressed, and valuable discoveries, both positive and negative, from the data interpretation are shared. The research findings and outcomes are validated, appropriate data display formats are selected, and the data representations are scrutinized before presentation. (Bazeley, 2013)

We opted to utilize a statistical approach for the data treatment and analysis procedure, employing the NVivo data analysis program. NVivo was chosen due to its capability to efficiently organize and manage large volumes of qualitative data, along with its extensive and advanced analysis features. Moreover, it offers collaborative features and can be tailored to accommodate various types of data and research methodologies. (Bazeley, 2013)

In conclusion, NVivo proves to be a valuable tool for researchers seeking to streamline the organization and analysis of their data, establish structure and order, and derive comprehensive insights from their research, as we did in our study.

Conclusion of the chapter:

In employing these qualitative data collection methods, we aim to uncover the multifaceted dimensions of cybersecurity in e-government, from its technical implementations to its organizational and societal implications. By triangulating data from observations, document analysis, interviews, and bibliographical references, we seek to provide a nuanced and holistic understanding of how cybersecurity influences the functioning and security of e-government systems.

CHAPTER 3: RESULTS AND DISCUSSION

In this chapter, we delve into the core findings and analytical insights derived from our qualitative study on the role of cybersecurity in e-government services, with a particular focus on the CERIST. This chapter is structured into two main sections. The first section presents the results obtained from our qualitative research, which was conducted in the previous chapter. The second section discusses these findings in detail, exploring their implications for the implementation and security of e-government services.

The qualitative study involved in-depth interviews and comprehensive data analysis aimed at understanding the challenges and opportunities associated with cybersecurity in the context of CERIST's e-government initiatives. By examining these results, we aim to shed light on the critical role that cybersecurity plays in ensuring the reliability, efficiency, and public trust in digital government platforms. Through this analysis, we hope to provide actionable insights that can inform future strategies and policies for enhancing cybersecurity measures in e-government systems.

This chapter, therefore, serves as a crucial component of our thesis, bridging the gap between theoretical considerations and practical applications, and highlighting the significant role of robust cybersecurity protocols on the success of e-government projects at CERIST.

Section 1. Results

In this analysis, we will delve into the insights gained from interviews conducted with cybersecurity experts and senior officials at CERIST, the These interviews aimed to shed light on the critical role of cybersecurity in ensuring the reliability, trustworthiness, and success of e-government services in Algeria.

The findings highlight the strategic importance placed on robust cybersecurity measures, the establishment of advanced monitoring systems and incident response protocols, the proactive approach to vulnerability management, the emphasis on continuous education and training for employees, and the commitment to compliance with industry standards and regulatory requirements.

Table 4: Analysis of Mr. Bouabid's Responses

Section	Question	Response Summary	Analysis
Background and understanding	Can you provide an overview of your role and responsibilities within CERIST, particularly regarding e-government services and cybersecurity?	Information Systems Security Responsible	Mr. Bouabid oversees security measures and protocols to ensure the protection of e-government services and data at CERIST.
	How would you define cybersecurity in the context of e-government and what do you see as its main objectives and challenges?	All human, legal, technical, and technological means to ensure protection, monitoring, and resilience of e-government information systems.	Cybersecurity encompasses a wide range of measures to protect e-government systems, with a focus on resilience and comprehensive security.
	Could you describe the e-government initiatives managed by CERIST and their significance in the context of Algeria?	CERIST develops and/or hosts e-government solutions upon request from interested institutions.	CERIST plays a crucial role in developing and hosting e-government solutions, supporting digital government initiatives in Algeria.
	What are some of the key cybersecurity measures and protocols currently in place within CERIST to protect e-government services and data?	General information security policy, access controls, remote surveillance, network access controls, identity and authentication management, auditing, traceability, data encryption, backups.	CERIST employs a comprehensive set of security measures, including policies, controls, surveillance, and data protection techniques.
Role of Cybersecurity in E-Government Services	From your perspective, how important is cybersecurity for ensuring the effectiveness and reliability of e-government services provided by CERIST?	It strengthens the trust of state services and citizens, enhances the trust of foreign partners, and protects the informational assets of the state and citizens.	Cybersecurity is deemed crucial for maintaining trust and protecting informational assets, essential for the effectiveness and reliability of e-government services.
	Can you share any examples of cybersecurity incidents or challenges that CERIST has encountered in the past and how they have	None	Mr. Bouabid indicates there have been no significant cybersecurity incidents impacting e-government operations at CERIST.

	impacted e-government operations?		
	How do you assess the level of public trust and satisfaction in CERIST's e-government services regarding cybersecurity?	Number of e-government services developed/hosted, minimal number and scope of attacks.	Public trust is gauged by the number of services and the limited impact of attacks, suggesting a strong security posture.
	What measures has CERIST implemented to mitigate cybersecurity risks and enhance the resilience of its e-government infrastructure?	Duplication of datacenter infrastructures, acquisition of protection solutions, backup and restoration policy.	CERIST enhances resilience through redundancy, protection solutions, and robust backup policies.
Incident Response Time	Can you describe the process your organization follows to detect and respond to cybersecurity incidents such as data breaches or malware attacks?	Installation of next-generation firewalls, proactive infrastructure supervision.	CERIST uses advanced firewalls and proactive supervision to detect and respond to incidents promptly.
Vulnerability Management	How does your organization identify and prioritize software vulnerabilities for patching?	Regular audits of information systems and application of patches as soon as they appear.	Regular audits and prompt patching are key strategies for vulnerability management at CERIST.
Security Awareness and Training	What measures does your organization take to raise awareness about cybersecurity among employees?	Training seminars, emails.	Training seminars and email communications are used to raise cybersecurity awareness among CERIST employees.
Compliance with Security Standards	To what extent does your organization comply with industry standards and regulatory requirements for cybersecurity?	Application of best practices, regular audits.	Compliance with best practices and regular audits ensures CERIST meets industry standards and regulatory requirements.
Number of Security Incidents Government Services Availability	How frequently does your organization experience security incidents such as malware infections, phishing attacks, or unauthorized access attempts?	No response	No specific frequency of incidents was provided.

	How would you rate the availability of government services online in terms of accessibility and convenience for citizens?	Average	The availability and convenience of online government services are rated as average.
Government Services Availability Government Services Availability	Could you share your experience in using e-government services and how important do you think digital literacy is for effectively utilizing these services?	Occasional use (education-related services)	Digital literacy is implied to be important, though Mr. Bouabid only occasionally uses e-government services.
	How would you assess the availability of government data and information for public access and have you ever made information access requests?	No experience	Mr. Bouabid has no personal experience with government data access requests.
Cybersecurity Measures	Can you provide examples of cybersecurity measures implemented by the government to protect e-government systems and data from cyber threats and how effective do you think they are?	Development of the national information system security framework, establishment of national cybersecurity mechanism.	Government measures are advancing towards better protection and resilience against cyber threats.
Future Directions and Recommendations	Looking ahead, what do you see as the main priorities for improving cybersecurity in CERIST's e-government services?	Compliance with current regulations, particularly the national cybersecurity framework.	Ensuring compliance with national regulations is a priority for improving cybersecurity.
	Are there any specific areas where you believe CERIST can further strengthen its cybersecurity posture to better protect e-government data and systems?	Private/public cloud computing.	Cloud computing (both private and public) is identified as an area for strengthening cybersecurity.
	How do you envision the role of collaboration and partnerships in enhancing cybersecurity for e-	Strengthening national capacities, sharing experiences, real-time information exchange.	Collaboration and partnerships are seen as vital for enhancing cybersecurity through

	government, both within Algeria and internationally?		capacity building, experience sharing, and information exchange.

Table 5: Analysis of Mr. Saidi's Responses

Section	Question	Response Summary	Analysis
Background and understanding	Role and Responsibilities	Expert Researcher in Information Security. Conducts advanced research, develops protocols, and collaborates with experts.	Comprehensive understanding of cybersecurity, contributing to CERIST's research and development.
	Definition of Cybersecurity	Protecting digital services and data from threats. Focus on data integrity, confidentiality, and availability.	Emphasizes the importance of protecting sensitive data and maintaining public trust.
	E-Government Initiatives	National Online Documentation System, SNLL. Enhance efficiency, transparency, and citizen access.	Highlights key projects enhancing public administration and access to information.
	Cybersecurity Measures	Multi-factor authentication, encryption, regular audits, advanced threat detection.	Implements a robust set of measures to protect e-government services.
Role of Cybersecurity in E-Government Services	Importance of Cybersecurity	Critical for effectiveness, data integrity, and public trust.	Recognizes cybersecurity as vital for the reliability of e-government services.
	Cybersecurity Incidents	Example of DoS attack. Led to enhanced DDoS protection.	Demonstrates responsiveness to incidents and improvement of security measures.
	Public Trust	High, due to continuous implementation and communication of security measures.	Public trust maintained through effective security practices and transparency.
	Risk Mitigation	Continuous monitoring, penetration testing, advanced technologies, incident response plans.	Proactive approach to mitigating risks and enhancing system resilience.
Cybersecurity Practices	Incident Response	Real-time monitoring, immediate investigation, structured response.	Effective incident response process in place.
	Incident Resolution Time	Minor issues resolved within hours, complex issues in days.	Efficient resolution of incidents, minimizing impact.

	Vulnerability Management	Automated scanning, prioritization, immediate patching of critical vulnerabilities.	Prioritizes and addresses vulnerabilities promptly.
	Security Awareness	Regular training, newsletters, phishing simulations.	Strong focus on raising employee awareness.
	Compliance with Standards	Full compliance with standards, regular audits.	Adheres to national and international standards.
	Frequency of Incidents	Regular phishing attempts, rare major incidents.	Proactive measures keep major incidents infrequent.
Future Directions and Recommendations	Improving Cybersecurity	Enhance infrastructure, increase training, improve incident response, strengthen collaborations.	Focus on continuous improvement and collaboration.
	Strengthening Cybersecurity Posture	Advanced threat intelligence, frequent training, rigorous drills.	Specific areas identified for strengthening security.
	Collaboration and Partnerships	Crucial for sharing resources, accessing threat intelligence.	Collaboration seen as vital for enhancing cybersecurity.

Table 6: Analysis of Mr. Krinah's Responses

Section	Question	Response Summary	Analysis
Background and understanding	Role and Responsibilities	Expert researcher	Strategic oversight and management of e-government systems and security.
	Definition of Cybersecurity	Protecting services and data from threats. Focus on integrity, confidentiality, and resilience.	Emphasizes the need for robust security to protect e-government services.
	E-Government Initiatives	National Online Documentation System, SNLL. Enhance public access and service efficiency.	Key projects aimed at improving government services and transparency.
	Cybersecurity Measures	Firewalls, intrusion detection, encryption, regular audits, incident response plans.	Comprehensive set of measures to protect e-government infrastructure.
Role of Cybersecurity in E-Government Services	Importance of Cybersecurity	Critical for data protection, service reliability, public confidence.	Recognizes the fundamental role of cybersecurity in e-government services.

	Cybersecurity Incidents	Data breach attempt mitigated through quick response. Led to enhanced protocols.	Demonstrates effectiveness in handling incidents and improving measures.
	Public Trust	High, due to transparent communication and effective security practices.	Maintained through transparency and robust security measures.
	Risk Mitigation	Continuous monitoring, regular updates, incident response drills, training programs.	Proactive risk mitigation strategies in place.
Cybersecurity Practices	Incident Response	Real-time monitoring, rapid threat identification, coordinated response.	Efficient incident response process.
	Incident Resolution Time	Typically resolved within hours for minor issues; longer for complex ones.	Quick resolution, minimizing impact on services.
	Vulnerability Management	Regular assessments, prioritization, timely patching.	Effective management and mitigation of vulnerabilities.
	Security Awareness	Ongoing training, awareness campaigns, phishing simulations.	Emphasizes the importance of continuous employee education.
	Compliance with Standards	Adherence to standards, regular audits.	Ensures compliance with relevant standards and regulations.
	Frequency of Incidents	Regular phishing and unauthorized access attempts, rare major incidents.	Proactive measures maintain security, preventing major incidents.
Future Directions and Recommendations	Improving Cybersecurity	Enhance threat intelligence, increase training, improve incident response.	Focus on improving key areas for better security.
	Strengthening Cybersecurity Posture	Advanced detection technologies, frequent training, stronger partnerships.	Specific improvements identified to enhance security.
	Collaboration and Partnerships	Essential for staying ahead of threats, sharing best practices.	Collaboration viewed as crucial for strengthening cybersecurity.

Table 7: Analysis of Ms. Amira's Responses

Section	Question	Response Summary	Analysis
Background and understanding	Role and Responsibilities	Expert researcher	Key role in ensuring network security and managing cybersecurity.
	Definition of Cybersecurity	Protecting network infrastructure and data. Focus on preventing unauthorized access, ensuring resilience.	Highlights the importance of network security in e-government services.
	E-Government Initiatives	National Online Documentation System, Network and Security Unit projects.	Projects aimed at enhancing security and reliability of digital services.
	Cybersecurity Measures	Intrusion prevention, firewalls, encryption, SIEM systems, regular audits.	Comprehensive measures to secure network infrastructure.
Role of Cybersecurity in E-Government Services	Importance of Cybersecurity	Essential for data protection, service continuity, public trust.	Recognizes the critical role of cybersecurity in maintaining reliable services.
	Cybersecurity Incidents	Attempted network intrusion blocked, improved response strategies.	Demonstrates effective incident management and protocol enhancement.
	Public Trust	High, due to effective communication and incident handling.	Maintained through transparency and successful incident management.
	Risk Mitigation	Comprehensive security strategies, regular assessments, continuous training.	Proactive approach to mitigating cybersecurity risks.
Cybersecurity Practices	Incident Response	Real-time detection, immediate investigation, coordinated response.	Effective incident response process in place.
	Incident Resolution Time	Quick identification and resolution, typically within hours.	Efficient resolution of incidents, minimizing disruption.
	Vulnerability Management	Regular scans, prioritization, prompt patching.	Effective management of vulnerabilities, ensuring timely mitigation.
	Security Awareness	Regular training, awareness campaigns, phishing simulations.	Emphasizes the importance of employee awareness and education.

	Compliance with Standards	Compliance with standards, regular audits, continuous updates.	Ensures adherence to best practices and regulatory requirements.
	Frequency of Incidents	Regular phishing and unauthorized access attempts, infrequent major incidents.	Proactive security measures keep major incidents rare.
Future Directions and Recommendations	Improving Cybersecurity	Enhance threat intelligence, increase training, improve incident response.	Focus on continuous improvement and capacity building.
	Strengthening Cybersecurity Posture	Advanced threat detection, frequent training, stronger collaborations.	Specific areas identified for strengthening security measures.
	Collaboration and Partnerships	Vital for improving security, sharing expertise, staying updated on threats.	Collaboration seen as crucial for enhancing cybersecurity effectiveness.

Source: elaborated by us using their answers

Section 2. Discussion

An analysis of the role of cybersecurity in e-government services at CERIST was conducted by interviewing important persons. This discussion part will analyze the primary discoveries from these interviews and establish connections with current literature and theoretical frameworks on cybersecurity and e-government.

The initial interviews offered a thorough understanding of the duties and obligations of important persons in CERIST, with a specific emphasis on their participation in e-government services and cybersecurity.

These roles highlight a multi-layered approach to cybersecurity, encompassing both strategic and operational dimensions. This structure ensures that both high-level strategies and day-to-day security measures are effectively managed, which is crucial for robust cybersecurity in e-government services. The shared understanding among the interviewees about the objectives and challenges of cybersecurity reflects a cohesive and aligned approach within CERIST, which is essential for effective cybersecurity governance.

Role of Cybersecurity in E-Government Services

The interviews consistently emphasized the significance of cybersecurity in upholding the efficiency and dependability of e-government services.

These viewpoints emphasize the crucial significance of cybersecurity in guaranteeing the credibility and dependability of e-government services. Trust is a fundamental element for the acceptance and achievement of e-government efforts, and strong cybersecurity measures are necessary to establish and preserve this trust. The unanimity among the interviewees about this matter highlights the significance of a robust cybersecurity framework in the effective implementation of e-government services.

Incident Response Time:

The interviews highlighted the need of actively identifying and promptly addressing cybersecurity incidents.

CERIST's cybersecurity strategy places great importance on taking a proactive approach to incident detection and response. The utilization of advanced technology and ongoing monitoring allows for the prompt detection and resolution of potential threats, which is crucial for upholding the security and dependability of e-government services. This strategy is in line with the recommended methods in cybersecurity, which prioritize the prompt reaction to mitigate the consequences of security incidents.

Security Awareness and Training:

The importance of cybersecurity awareness and training among employees was a key theme.

Ongoing education and frequent training are essential for retaining a workforce that is vigilant about security. It is crucial for the organization's overall cybersecurity stance to have well-informed and capable workers who can identify and address possible risks. The emphasis on employee training and awareness in this context demonstrates a complete approach to cybersecurity, highlighting the importance of both technical measures and human aspects.

Compliance with Security Standards:

All interviewees emphasized the importance of adhering to industry standards and regulatory regulations.

CERIST ensures that it meets essential cybersecurity benchmarks through regular audits and strict adherence to best practices. By adhering to this compliance, the e-government services are improved in terms of reliability and user trust is established. Complying with established standards and laws is essential for preserving the security and integrity of e-government systems.

Future Directions and Recommendations:

In anticipation, the respondents have identified numerous goals for enhancing cybersecurity.

Future priorities for CERIST involve improving current measures, implementing new technologies, and promoting collaborations. Consistently enhancing and adopting innovative technologies are crucial for staying ahead of emerging cyber threats and maintaining strong e-government services. These priorities guarantee that CERIST can effectively safeguard its e-government systems and data, offering secure and dependable services to users.

The results align closely with the literature review, reinforcing several key points. Both highlight the necessity of a comprehensive approach to cybersecurity that integrates strategic planning, technological adoption, and continuous monitoring. The challenges identified, such as dealing with legacy systems and sophisticated cyber-attacks, are prevalent in both findings and the literature. Additionally, the role of advanced technologies like AI and blockchain is emphasized across both sources, and CERIST's practical implementations mirror these theoretical recommendations. The importance of training and awareness programs to mitigate human error is a shared focus, with CERIST's initiatives reflecting the literature's emphasis on human factors. Finally, adherence to regulatory standards is a consistent theme, with CERIST's compliance efforts aligning with global best practices outlined in the literature. This comparison underscores the practical applicability of theoretical frameworks in enhancing cybersecurity within e-government services.

Conclusion:

The examination of interview responses underscores CERIST's all-encompassing and forward-thinking strategy towards cybersecurity, encompassing strategic planning, pragmatic execution, ongoing surveillance, and cooperation. The unwavering focus on safeguarding, overseeing, and fortifying e-government services expressed by all interviewees indicates a firm dedication of the organization to ensuring their security. It is crucial to prioritize future actions such as upgrading existing measures, using new technologies, and promoting cooperation in order to sustain and enhance the cybersecurity framework. By adopting this holistic approach, CERIST guarantees its position as a leader in cybersecurity, offering dependable and secure e-government services to its consumers.

CONCLUSION

The study conducted at CERIST on the role of cybersecurity in e-government services has uncovered valuable findings on the institution's endeavors to safeguard its digital infrastructure. By conducting comprehensive interviews with important staff, we have successfully identified the crucial procedures and protocols being implemented, as well as the obstacles and future prospects for cybersecurity in e-government services.

CERIST has adopted a comprehensive approach to cybersecurity, which includes strategic analysis, practical implementation, and ongoing monitoring. This technique guarantees the efficient management of both overarching strategies and daily security measures. The institution's unwavering focus on safeguarding citizen data and state information highlights its dedication to upholding the reliability and credibility of its e-government services.

The literature study offers a comprehensive theoretical basis for comprehending the significance and intricacies of cybersecurity in the domain of e-government services. The text provides an overview of the development and goals of e-government, which involve enhancing the effectiveness, openness, and availability of public services via digital methods. Nevertheless, the research highlights that these advantages may be completely actualized only if strong cybersecurity measures are implemented to safeguard critical government data and uphold public confidence. The text explores a range of cybersecurity concerns, including the requirement for safe digital infrastructure, advanced technological solutions, and the significance of addressing human elements through ongoing training and awareness programmes. The evaluation also discusses the crucial need of adhering to international cybersecurity standards and implementing thorough incident response methods.

Conversely, the discussion section provides pragmatic observations obtained from interviews conducted with CERIST personnel. This section provides an in-depth examination of how CERIST addresses cybersecurity in the context of e-government services. It encompasses precise methodologies and procedures, such as the organization's strategy for responding to incidents, which guarantee prompt identification and resolution of cybersecurity breaches. The debate also examines CERIST's approach to prioritizing and mitigating software vulnerabilities, promoting security awareness among personnel, and complying with industry standards and regulatory obligations. The practical viewpoint of managing public trust and mitigating

cybersecurity events encountered by CERIST, together the theoretical insights from the literature analysis, are emphasized as real-world challenges.

Both parts emphasize the crucial significance of cybersecurity in e-government. The literature study presents the essential need to incorporate cybersecurity into e-government frameworks, emphasizing that the advantages of digital government services cannot be completely achieved without strong security measures. The text emphasizes the significance of having a safe infrastructure, making technology improvements, and considering the human factor in cybersecurity. It proposes a multi-faceted strategy to achieving complete security.

The discussion portion, however, demonstrates the practical implementation of these theoretical notions within CERIST. The text presents instances of CERIST's strategic endeavors, including the establishment of incident response protocols, vulnerability management procedures, and security awareness campaigns. These empirical observations demonstrate how CERIST effectively tackles the conceptual obstacles identified in the literature review, guaranteeing the durability and dependability of its e-government services.

Moreover, the discussion emphasizes the current endeavors and future objectives for strengthening cybersecurity in CERIST's e-government services, demonstrating the persistent enhancement and strategic planning emphasized in the literature review. The alignment between theory and practice highlights the crucial importance of cybersecurity in e-government, illustrating that efficient cybersecurity measures are vital for realizing the complete potential of digital government services. The study offers a comprehensive understanding of the role of cybersecurity in e-government by comparing the theoretical insights from the literature review with the practical implementation discussed. It highlights the significance of incorporating strong security measures into all aspects of e-government operations.

BIBLIOGRAPHY

Bibliography

1. 800-53, N. S. (2020). *Security and Privacy Controls for Federal Information Systems and Organizations.* National Institute of Standards and Technology.
2. Abdeslam, A. N., & Yousif , A. (2015). Evaluating the Benefits of Implementing ITIL in the Public Sector: A Case Study from the UAE. *Government Information Quarterly*, 378-387.
3. Affairs, U. N. (2020). *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.* United Nations Department of Economic and Social Affairs. Retrieved from https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020
4. Affairs, U. N. (2020). *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.* United Nations Department of Economic and Social Affairs. Retrieved from https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020
5. Agency, U. S. (n.d.). *About CISA*. Retrieved from Cybersecurity and Infrastructure Security Agency.
6. Alexander S. Gillis. (2024, February). *What is cybersecurity?| definition from TechTarget*. Retrieved from TechTarget: https://www.techtarget.com/searchsecurity/definition/cybersecurity
7. Almarabeh, T., & AbuAli, A. (2010). A general framework for e-government: Definition, maturity challenges, opportunities and success. *European Journal of Scientific Research, 39*(1), 29-42. Retrieved from https://www.researchgate.net/publication/228434888
8. Alrubaiq, A., & Alharbi , T. (2021). Developing a Cybersecurity Framework for e-Government. *Journal of Cybersecurity and privacy*, 304.
9. Alshehri, M., & Drew, S. (2010). E-government fundamentals. *IADIS International Conference ICT, Society and Human Beings.* Retrieved from https://www.dora.dmu.ac.uk/handle/2086/8391
10. Alshibly, H. H., & Irani, , Z. (2020). E-Government Implementation: A Review of Critical Success Factors and Barriers. *International Journal of Electronic Government Research*, 1-21.
11. Alvarez, M. R., & Subburaj, D. V. (2023). Smart Resilient Cyber Secure Micro-grids: A Study onCyber-Attacks and Resilience.
12. Anderson, J. (2018). Cybersecurity in E-Government: Challenges and Opportunities. *Studies and Best Practices*, 45-62.

13. Anderson, L. (2018). Detecting and Preventing DNS Tunneling Attacks in E-Government Networks. *International Conference on Cyber Security and Protection of Digital Services*, 250-265.

14. Anderson, R. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems.* Wiley.

15. Anderson, R., & Moore, T. (27-29). Information security economics – and beyond. *Communications of the ACM*.

16. Andress, J. (2014). *The basics of information security: Understanding the fundamentals of InfoSec in theory and practice.* Syngress.

17. Andress, J. (2020). Cybersecurity for government: An overview. In J. W. M. Gupta, *Cyber-security standards, risk management and risk assessment for operational information and communication technology* (pp. 1-16). Springer, Cham. doi:10.1007/978-3-030-41624-2_1

18. Ashman, H., & Arthur , T. (2018). Implementing the ISO/IEC 27001 Information Security Management Standard: The Experience of Dunedin City Council. *Information Systems Frontiers*, 237-257.

19. Assembly, U. N. (2001). *International Cooperation in the Fight Against Cybercrime.*

20. Australia, G. o. (2020). *2020 Cyber Security Strategy.* Australian Government.

21. Awad, A., Atef, A., & El-Zayat, M. (2019). Cybersecurity Challenges in E-Government: An Insider Threat Perspective. *International Journal of Advanced Computer Science and Applications*, 432–439.

22. Bakhouche, B. (2006). ICTs in Algeria. In J. Berbiers (ed.), Encyclopedia of Life Support Systems (EOLSS). *Web-Based Instruction (WBI) for Distance Education. UNESCO*.

23. Barcevičius, E. (n.d.). elaboration) eGovernment 2.0. In the second half of the 2000s. Lithuania.

24. Basahel, A., & Mohammad , Y. (2017). Measuring success of e-government of Saudi Arabia. *springer*.

25. Bazeley, P. &. (2013). *Qualitative Data Analysis with NVivo.*

26. Bellouki, M., & Haddad, E. J. (2019). Cybersecurity in Algeria: An overview. *Proceedings of the 2nd International Conference on Networking, Information Systems & Security* (pp. 1-6). Association for Computing Machinery.

27. Benmohammed, M. &. (2018). Cybersecurity challenges and strategies in Algeria. *Journal of Cybersecurity Research*, 45-58.

28. Bertino, E., & Islam, N. (2019). Cybersecurity in E-Government. *IEEE Security & Privacy*, 50-57.

29. Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, 264-271.

30. Bertot, J. C., Jaeger, P. T., & McClure, C. R. (2008). Proceedings of the 9th Annual International Digital Government Research Conference., (pp. 137-142). doi:10.1145/1367832.1367858

31. Bowen, G. A. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal* , 27-40.

32. Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 77-101.

33. Brown, E. (2017). Understanding Denial-of-Service Attacks: Patterns, Impacts, and Countermeasures. *IEEE Transactions on Dependable and Secure Computing*, 200-215.

34. Castillo-Montoya, M. (2016). Preparing for interview research: The interview protocol refinement framework. 811-831. doi:https://doi.org/10.46743/2160-3715/2016.2337

35. Caves, R. W. (2004). Encyclopedia of the City. Routledge.

36. Centre, N. C. (2021). *Cyber Security Incident Response: What to Expect.* Government of the United Kingdom.

37. *Cerist* . (2024). Retrieved from https://www.cerist.dz/index.php/en/our-services/327-arn

38. CERIST. (2021). Proceedings of the International Conference on Cybersecurity and Protection of Digital Services.

39. CERIST. (2022). Retrieved from https://www.cerist.dz/index.php/en/

40. CERIST. (2024). *about us* . Retrieved from CERIST: https://www.cerist.dz/index.php/en/about-us-en-3/730-historique

41. CERIST. (2024). *Research & Development*. Retrieved from https://www.cerist.dz/index.php/en/rechercheetdevelop-en/148-programme-nationaux-de-recherche-pnr

42. Chen, Liangliang, & al. (2017). A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications. *IEEE Internet of Things Journal*, 1125-1142.

43. Chertoff, M. (2018). *Exploring risk appetite and risk tolerance.* The CERT Division, Software Engineering Institute.

44. Choo, K., K, & R. (2018). Legislating Cybersecurity: A Comparative Analysis of Cybersecurity Legislation and Regulation in Selected Jurisdictions. *Journal of Internet Law*, 21(4), 3-18.

45. Commission, E. (2019). *Digital government strategies for transforming public services in the European Union*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/strategies-digital-transformation-public-services

46. Council, p. C. (2016). *PCI Data Security Standard (PCI DSS) Version 3.2.1.*

47. Cox, L. J. (2014, 01 12). Qualitative data analysis. *Student L*.

48. Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* SAGE Publications.

49. Creswell, J. W. (2017). *Qualitative Inquiry and Research Design: Choosing Among Five Approaches.*

50. Crime, U. N. (2001). *convention on Cybercrime.* Council of Europe.

51. *Cybersecurity*. (2021). (Cybersecurity & Infrastructure Security Agency, U.S. Department of Homeland Security) Retrieved from https://www.cisa.gov/cybersecurity

52. Cybersecurity, E. U. (2020). *EU NIS Directive: Overview of National Implementation Measures.* European Union Agency for Cybersecurity.

53. Cybersecurity, E. U. (n.d.). *About ENISA*.

54. Disterer, G. (2018). Cyber Security Challenges in E-Government. *Procedia Computer Science*, 126,1573–1581.

55. Doe, J. (2020). Understanding Malware: Analysis and Mitigation Strategies. *Journal of Cybersecurity Research*, 50-65.

56. D'Onofrio, Stefano, & al. (2020). Framework for Cybersecurity Information Sharing and Collaboration in the European Union. *Computers & Security*.

57. Dunleavy, P., Margetts, H., Bastow, S., & Tinkler, J. (2006). *Digital Era Governance: IT Corporations, the State, and e-Government.* Oxford University Press.

58. Dwivedi, Y. K., Pan, S., Sharif, A., & Weerakkody, V. (2009). conceptualising a Framework for E-Government Adoption: A Study of Indian Central Excise. *information Systems Frontiers*, 389–414.

59. E, D., Crawford , & Kristen, N. (2015). The NIST Cybersecurity Framework: Advancing Critical Infrastructure Protection. *Journal of Homeland Security and Emergency Management*, 353-356.

60. Europe, C. o. (2001). *Convention on Cybercrime: Explanatory Report.* Council of Europe.

61. European Commission. (2019). *Digital Government Factsheets – European Union*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/egovernment

62. Flick, U. (2018). The qualitative research. In U. In Flick, *The Sage handbook of qualitative data collection* (pp. (pp. 3-18)). Sage.

63. Forum, W. E. (2022). *The Global Cybersecurity Outlook 2022.* World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

64. Garfinkel, S., Spafford, G., & Schwartz, A. (2005). *Practical Unix & Internet Security.* O'Reilly Media.

65. Gartner. (2022). *IT Key Metrics Data 2022: Key Industry Measures: Cross-Industry Analysis.* Gartner. Retrieved from https://www.gartner.com/en/publications/standard?publicationId=634100000

66. Gil-Garcia, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly*, 187-216. doi:10.1016/j.giq.2005.02.001

67. Gil-Garcia, J. R., & Pardo, T. A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. *Government Information Quarterly*, 187-216. doi:10.1016/j.giq.2005.02.001

68. Goutam, R. K. (2021). *Understand the Role of Cybersecurity,Its Importance and Modern Techniques Used by Cybersecurity Professionals.*

69. Green, D., G, & al. (2020). The Legal Landscape of Cybersecurity. *Georgetown Law Technology Review*, 4(1), 118-151.

70. Gupta, B. B., Yamaguchi, S., & Nomura, S. (2018). Cybersecurity risk management for e-governance portals: A comprehensive risk management framework. *International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)* (pp. 260-267). IEEE.

71. Hai, J. C., & Ibrahim. (2007). *Fundamental of Development Administration.* Selangor: Scholar Press.

72. Heeks, R. (2006). *Implementing and Managing eGovernment: An International Text.* SAGE Publications.

73. Heeks, R. (2006). Implementing and Managing E-Government: An International Text. *SAGE Publications*.

74. Horan, T. A., & Åke, G. (2005). Introducing e-Go oducing e-Gov: Hist v: History, Definitions, and Issues , Definitions, and Issues. *Communications of the Association for Information Systems*, 713-714-715.

75. Huffman, B. D. (2017). E-Participation in the Philippines: A Capabilities Approach to Socially Inclusive Governance. *jedem*.

76. Information, C. L. (2018). *California Consumer Privacy Act of 2018.*

77. Islam, M. M., & Mohammad , E. (2012). *From Government to E-Governance: Public Administration in the Digital Age.*

78. Islam, M. R., Baikady, A., & Ahmed Khan, R. (2022). Understanding Qualitative Research Methods. *Journal of Qualitative Studies*, 45-62.

79. itu. (2024). *cybersecurity*. Retrieved from itu: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

80. Jacobs, J., Romanosky, S., & Roytman, A. (2020). Vulnerability management metrics: Data-driven models for measurement and improvement. *Empirical Software Engineering*, 2687-2720.

81. Jaeger, P. T., & Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly*, 371-376.

82. Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management*, 258-268. doi:10.1080/10580530.2012.716740

83. Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management*, 258-268. doi:10.1080/10580530.2012.716740

84. Johnson, A. (2018). SQL Injection Attacks: Detection and Prevention Techniques. *International Journal of Computer Applications*, 100-115.

85. Johnson, M. (2021). Ransomware: Evolution, Trends, and Mitigation Strategies. *Information Systems Security Association (ISSA) Journal*, 80-95.

86. Jones, D. (2016). Insider Threats to E-Government Systems: Detection and Prevention Approaches. *Government Information Quarterly*, 70-85.

87. Justice, U. S. (1986). *Computer Fraud and Abuse Act.*

88. kasperskey. (2024). *What is Cybersecurity? Types, Threats and Cyber Safety Tips*. Retrieved from kasperskey: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

89. Kelley, K. (2023, october 25). *what is cybersecurity & importance of cybersecurity*. Retrieved from simplilearn: https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-cyber-security

90. Khiati, A. (2013). The CERIST: An institution dedicated to scientific and technical information in Algeria. *OCLC Systems & Services*, 24-34.

91. Krutz, R. (2003). *The CISSP Prep Guide: Mastering the Ten Domains of Computer Security.* Wiley.

92. Layne, K., & Lee, J. (2001). Developing fully functional E-government: A four stage model. *Government Information Quarterly*, 18(2), 122-136.

93. Lee, C., Chang, K., & & Berry, F. (2011). Testing the development and diffusion of e-government and e-democracy: A global perspective. *Public Administration review*, 71(3), 444-454.

94. Lynn, W. (2010). Defending a new domain: The pentagon's cyberstrategy. *Foreign affairs*, 89(5), 97-108.

95. Lyytinen, Kalle, & Rossi, M. (2018). Government Digitalization and Public Trust in Public Institutions: A Comparative Analysis of E-Government Systems. *Public Administration Review*, 228-238.

96. Mack, N., Woodsong, C., MacQueen, K. M., & Namey, E. (2005). *Qualitative research methods: A data collector's field guide.* Family Health International.

97. Madjed, R. (2016). *Scientific Research Methodology.* بيروت : Friedrich Ebert.

98. MERAD, B. (2024). *OFFICIAL JOURNAL OF THE ALGERIAN REPUBLIC*, 16.

99. Merriam, S. B., & Tisdell, E. J. (2015). *Qualitative Research: A Guide to Design and Implementation.* Jossey-Bass.

100. Mezhouda, A. (2019). introduction to e-government.

101. Miles, M. B. (2014). *Qualitative Data Analysis: A Methods Sourcebook.*

102. Ministry of Justice. (2009, august 14). *Law n° 09-04.* Retrieved from joradp: https://www.joradp.dz/FTP/jo-francais/2009/F2009047.pdf

103. Ministry of justice. (2015, april 25). *law n° 15-109.* Retrieved from joradp: https://www.joradp.dz/FTP/jo-francais/2015/F2015022.pdf

104. Ministry of justice. (2018, july 25). *law n° 18-07.* Retrieved from joradp: https://www.joradp.dz/FTP/jo-francais/2018/F2018046.pdf

105. Ministry of Post and Information and Communication Technologies. (2020). *National Cybersecurity Strategy. Algiers: Government of Algeria.*

106. *Missions CERIST*. (n.d.). Retrieved from https://www.cerist.dz/index.php/en/about-us-en-3/733-missions

107. Moon, M. (2002). The evolution of e-government among municipalities: Rhetoric or reality. *Public Administration Review*, 62(4), 424-433.

108. Moussaoui, A. &. (2019). Enhancing cybersecurity through international collaboration: The CERIST experience. *International Journal of Cyber Studies*, 102-120.

109. Musselwhite, K., Cuff, L., McGregor, L., & King, K. M. (2007). The telephone interview is an effective method of data collection in clinical nursing research: A discussion paper. *International Journal of Nursing Studies*, 1064-1070.

110. NASCIO. (2016). *State Cybersecurity Resource Guide.* National Association of State Chief Information Officers.

111. National Association of State Chief Information Officers (NASCIO). (2017). *The Importance of Cybersecurity in Government: A Guide to Understanding the Challenges and How to Protect Government Data and Networks.* Retrieved from https://www.nascio.org/wp-content/uploads/2017/11/NASCIO-The-Importance-of-Cybersecurity-in-Government_FINAL.pdf

112. National Institute of Standards and Technology (NIST). (2012). *Computer Security Incident Handling Guide.* NIST Special Publication 800-61 Revision 2.

113. National Institute of Standards and Technology (NIST). (n.d.). *Baldrige Cybersecurity Excellence Builder: Key characteristics of cybersecurity risk management*. Retrieved from Key characteristics of cybersecurity risk management: https://www.nist.gov/baldrige/products-services/baldrige-cybersecurity-initiative

114. National Institute of Standards and Technology (NIST) Special Publication. (n.d.). Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. 800-37 Rev. 2.

115. National Institute of Standards and Technology. (2018). *Glossary: Cybersecurity*. Retrieved from https://csrc.nist.gov/glossary/term/cybersecurity

116. National Institute of Standards and Technology. (2018). *NIST Special Publication 800-94 Rev. 1: Guide to Intrusion Detection and Prevention Systems (IDPS).* National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-94r1

117. Newmeyer, K. S. (2015). Elements of national cybersecurity strategy for developing nations. *Fletcher F. World Aff*, 93-108.

118. *NVivo Lumivero*. (2022). Retrieved from https://lumivero.com/products/nvivo/#:~:text=What%20is%20NVivo%3F,from%20their%20qualitative%20data%20faster.

119. OECD. (2014). *Recommendation of the Council on Digital Government Strategies.* Retrieved from https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0406

120. OECD. (2017). *Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact.* OECD. Retrieved from https://www.oecd.org/gov/open-government-data-report-9789264280984-en.htm

121. Oliveira, T., & Martins, M. (2020). E-Government Evolution: A Systematic Literature Review. *Government Information Quarterly*, 37(3), 101487.

122. Patel, S., & Lee, C. (2020). Integrating Cybersecurity into E-Government Maturity Models: A Conceptual Framework. *Government Information Quarterly*, 301–315.

123. Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice (4th ed.).* SAGE Publications.

124. Pereira, G. V., Cunha, M. A., Lipinsky, H., & Becker, K. (2020). Cybersecurity for the digital government. In *Digital government: Toward a citizen-centric perspective* (pp. 115-134). Springer, Cham. doi:https://doi.org/10.1007/978-3-030-38986-1_6

125. Pfleeger, C. P. (2002). *Security in Computing.* Prentice Hall.

126. Ramzy, M., & Ibrahim, Bahaa. (2024). The evolution of e-government research over two decades: applying bibliometrics and science mapping analysis. *EMERALD GROUP PUBLISHING LIMITED*, 227-260.

127. Rocha Flores, W., & Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational tactics. *Journal of Information Security and Applications*, 13-26.

128. Roman, Rodrigo, & al. (2016). A Survey of Mobile Malware in the Wild. *IEEE Communications Surveys & Tutorials*, 393-413.

129. Rubin, H. J., & Rubin, I. S. (2011). *Qualitative interviewing: The art of hearing data.* sage.

130. S, H., Norris, D., & Fletcher, P. (2003). Electronic government at the local level: Progress to date and future issues. *Public Performance and Management Review*, 26(4), 325-344.

131. Sá, F., Rocha, Á., & Cota, M. P. (2016). From the quest for citizen's trust in e-government relying on cognitive computing to blockchain ancentric cybergovernance. *Proceedings of the 18th International Conference on Enterprise Information Systems* , (pp. 475-483).

132. Savić, D. (2019). E-Government Services. In *Digital Assistance for Citizens and Organizations: Principles and Management* (pp. 33-54). Palgrave Macmillan. doi:10.1007/978-3-030-19320-7_3

133. Savić, D. (2019). E-Government Services. In *Digital Assistance for Citizens and Organizations: Principles and Management* (pp. 33-54). Palgrave Macmillan. doi:10.1007/978-3-030-19320-7_3

134. Scholl, H. J. (2017). The Digital Transformation of Government: What's the story so far? In *Digitally Transforming Government* (pp. 1-30). Routledge. doi:10.4324/9781315282107

135. Sear, M. J. (2023, april 20). *The Importance of Cybersecurity for Governments*. Retrieved from LinkdIn: https://www.linkedin.com/pulse/importance-cybersecurity-governments-mohammad-j-sear/

136. Security, C. f. (2021). *CIS Benchmarks*. Retrieved from https://www.cisecurity.org/cis-benchmarks/

137. Security, U. S. (2018). *National Cyber Strategy of the United States of America.* Department of Homeland Security.

138. Seidman, I. (2006). *Interviewing as Qualitative Research: A Guide for Researchers in Education and the Social Sciences* (3rd Edition ed.). Teachers College Press.

139. Services, U. S. (1996). *Health Insurance Portability and Accountability Act.*

140. Shahbaz, B., & Adnan , A. (2017). Implementing COBIT 5 for Information Security in a Governmental Organization. *Government Information Quarterly*, 680-695.

141. Shareef, M. A., Dwivedi, Y. K., Stamati, T., & Williams, M. D. (2014). SQualIT: A quality management approach for measuring web service quality. *International Journal of Information Quality*, 298-319.

142. Smith, J. (2019). The Art of Deception: How Hackers Use Phishing Emails to Steal Data. *Cybersecurity Today Magazine*, 30-35.

143. Smith, R. (2022). Security Challenges in IoT-Based E-Government Systems. *IEEE Internet of Things Journal*, 120-135.

144. Smith, R., & Johnson, M. (2019). securing E-Government: A Comparative Analysis of Cybersecurity Frameworks. *International Journal of Cybersecurity Research*, 78-92.

145. Snoke, T., Kimppa, K., & Norros, L. (2019). Prioritizing Security Controls in an Institutional Environment: A Case Study on the Implementation of the CIS Controls at a Large Higher Education Institution. *Computers & Security*, 212-228.

146. Solove, & J, D. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 477-560.

147. Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach. *International Journal of Information Management*, 215-225.

148. Stallings, W. (2017). *Cryptography and Network Security: Principles and Practice.* Pearson.

149. Standardization, I. O. (2016). *ISO/IEC 27002:2013 - Information technology -- Security techniques -- Code of practice for information security controls.* International Organization for Standardization.

150. Standardization, I. O. (2018). *ISO/IEC 27001:2013 - Information security management systems -- Requirements.* International Organization for Standardization.

151. Standardization, t. I. (2018). *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and*

vocabulary. International Organization for Standardization. Retrieved from https://www.iso.org/standard/73906.html

152. Stylianou, A., Skouloudis, A., Georgiadou, A., & Malesios, C. (2020). Cybersecurity and E-Government: A Review of Trends, Practices, and Challenges. *Sustainability*, 4978.

153. T, D., Gorden, J, S., & Visner. (2017). Implementing FISMA-Compliant Cyber Security Frameworks. *International Journal of Critical Infrastructure Protection*, 1-9.

154. Technology, N. I. (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* NIST Cybersecurity Framework Version 1.1.

155. Technology, N. I. (2018). *NIST Special Publication 800-184: Guide for Cybersecurity Event Recovery.* National Institute of Standards and Technology.

156. Technology, N. I. (2018). *NIST Special Publication 800-37 Rev. 2: Risk Management Framework for Information Systems and Organizations.* National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-37r2

157. Technology, N. I. (2020). *NIST Special Publication 800-161 Rev. 1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.* National Institute of Standards and Technology. doi:10.6028/NIST.SP.800-161r1

158. Technology, N. I. (2020). *NIST Special Publication 800-175B Rev. 1: Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms.* National Institute of Standards and Technology.

159. Technology, N. I. (2021). *NIST Special Publication 800-40 Rev. 4: Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology.* National Institute of Standards and Technology.

160. The United Nations Department of Economic and Social Affairs (UNDESA). (2020). *E-Government Survey 2020.*

161. U.S. Department of Homeland Security. (2021). Retrieved from Cybersecurity strategy: https://www.dhs.gov/cybersecurity-strategy

162. Union, I. T. (2008). *Overview of cybersecurity.* Retrieved from https://www.itu.int/rec/T-REC-X.1205-200804-I/en

163. Union, I. T. (2018). Guide to developing a national cybersecurity strategy: Strategic engagement in cybersecurity. International Telecommunication Union.

164. Union, O. J. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC . *European Union*.

165. United Nations Department of Economic and Social Affairs. (2020). *E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development.* United Nations Department of Economic and Social Affairs. Retrieved from https://publicadministration.un.org/egovkb/en-us/Reports/UN-E-Government-Survey-2020

166. Walliman, N. (2017). *Research methods: The basics. Routledge.*

167. Wang, D., & Xiao, J. (2019). The Evolution of E-Government: A Bibliometric Analysis. *Government Information Quarterly*, 36(1), 101369.

168. Wang, L., & Chen, h. (2021). Strengthening Cybersecurity in E-Government Operations: A Comparative Study. *Journal of Information Security and Cybercrimes*, 189–204.

169. Weerakkody, V., & Dhillon, G. (2008). Moving from e-Government to t-Government: A study of process reengineering challenges in a UK local authority context. *International Journal of Electronic Government Research*, 1-16.

170. Weerakkody, V., Dwivedi, Y. K., & Kurunananda, A. (2009). Implementing e-government in Sri Lanka: Lessons learned from the UK. *Information Technology for Development*, 171-192.

171. West, D. M. (2004). E-Government and the Transformation of Service Delivery and Citizen Attitudes. *Public Administration Review*, 15-27.

172. West, D. M. (2004). E-Government and the Transformation of Service Delivery and Citizen Attitudes. *Public Administration Review*, 15-27.

173. Whitman, M. E., & Mattord, H. J. (2016). *Management of information security* (5th ed.). Cengage Learning.

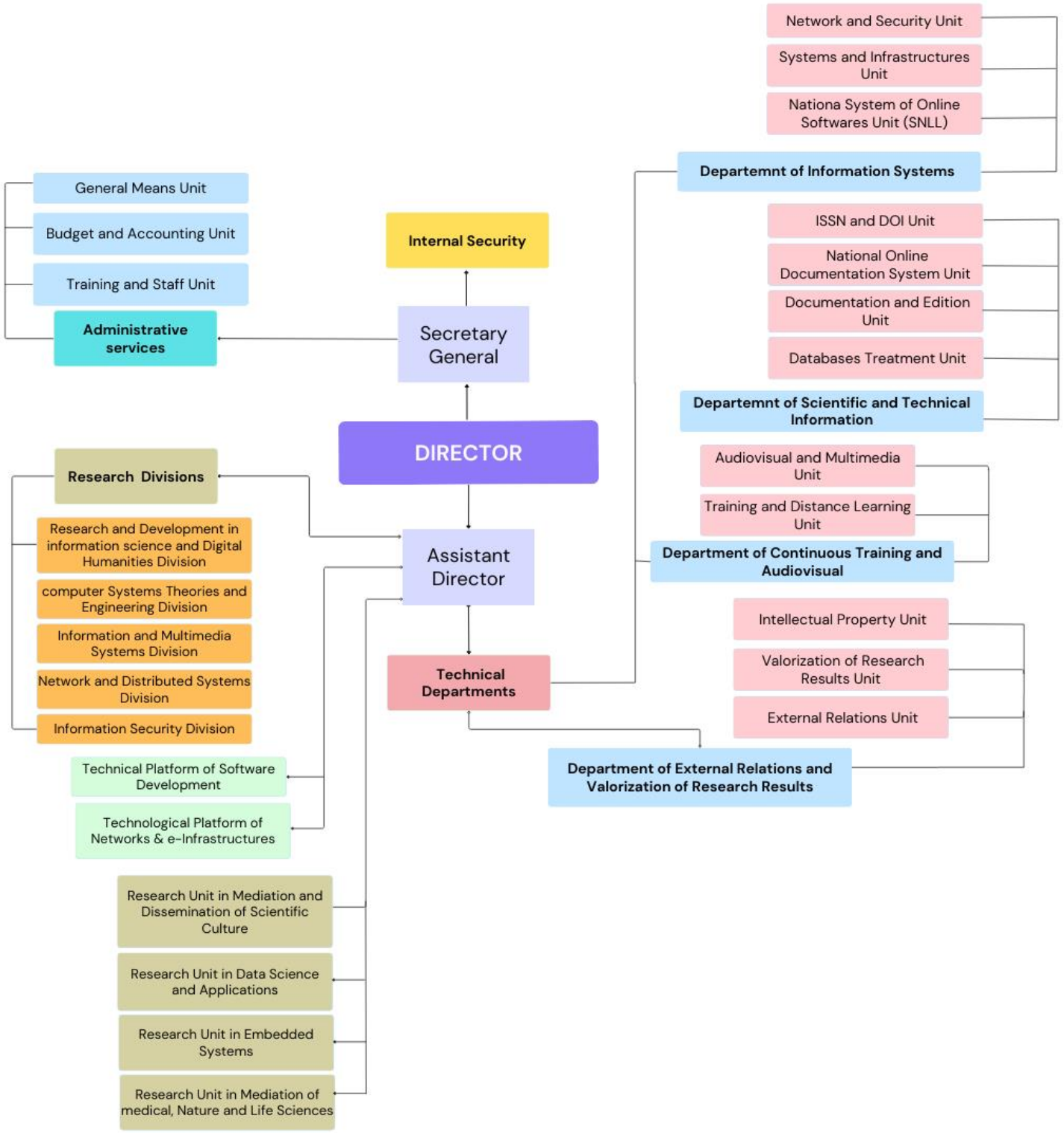
174. Williams, S. (2019). Understanding Supply Chain Cybersecurity Risks and Countermeasures. *Journal of Supply Chain Management*, 150-165.

175. Wong, W. E., Wong, E., Behnam, M. R., Li, Q., & Yan, G. (2018). Cybersecurity Risk Assessment for Critical Infrastructures: A Novel Framework. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 48(4), 535-551.

176. Wyld, D. C., & Baker, W. H. (2020). *E-Government and Cyber-Security: Principles, Strategies, and Applications.* Emerald Publishing Limited.

177. Yin, R. K. (2017). *Case Study Research and Applications: Design and Methods.* SAGE Publications.

Appendix A: ORGANIZATION CHART OF CERIST


Network and Security Unit
Systems and Infrastructures Unit
Nationa System of Online Softwares Unit (SNLL)
Departemnt of Information Systems
General Means Unit
Budget and Accounting Unit
Training and Staff Unit
Administrative services
Internal Security
Secretary General
ISSN and DOI Unit
National Online Documentation System Unit
Documentation and Edition Unit
Databases Treatment Unit
Departemnt of Scientific and Technical Information
DIRECTOR
Research Divisions
Research and Development in information science and Digital Humanities Division
computer Systems Theories and Engineering Division
Information and Multimedia Systems Division
Network and Distributed Systems Division
Information Security Division
Assistant Director
Audiovisual and Multimedia Unit
Training and Distance Learning Unit
Department of Continuous Training and Audiovisual
Technical Departments
Intellectual Property Unit
Valorization of Research Results Unit
External Relations Unit
Department of External Relations and Valorization of Research Results
Technical Platform of Software Development
Technological Platform of Networks & e-Infrastructures
Research Unit in Mediation and Dissemination of Scientific Culture
Research Unit in Data Science and Applications
Research Unit in Embedded Systems
Research Unit in Mediation of medical, Nature and Life Sciences

Appendix B: INTERVIEW GUIDE

The Interview Guide :

Section 1: Background and Understanding

- Can you provide a brief overview of your role and responsibilities within CERIST, particularly in relation to e-government services and cybersecurity?
- How would you define cybersecurity in the context of e-government, and what do you see as its main objectives and challenges?
- Could you describe the e-government initiatives managed by CERIST and their significance in the context of Algeria?
- What are some of the key cybersecurity measures and protocols currently in place within CERIST to protect e-government services and data?

Section 2:Role of Cybersecurity on E-Government Services

- From your perspective, how important is cybersecurity for ensuring the effectiveness and reliability of e-government services provided by CERIST?
- Can you share any examples of cybersecurity incidents or challenges that CERIST has encountered in the past, and how they have impacted e-government operations?
- How do you assess the level of public trust and confidence in CERIST's e-government services regarding cybersecurity?
- What measures has CERIST implemented to mitigate cybersecurity risks and enhance the resilience of its e-government infrastructure?
- Can you describe the process your organization follows to detect and respond to cybersecurity incidents, such as data breaches or malware attacks?
- How quickly are cybersecurity incidents typically identified and resolved within your organization?
- How does your organization identify and prioritize software vulnerabilities for patching?
- What measures does your organization take to raise awareness about cybersecurity among employees?
- To what extent does your organization comply with industry standards and regulatory requirements for cybersecurity?

- How frequently does your organization experience security incidents such as malware infections, phishing attacks, or unauthorized access attempts?
- How would you rate the availability of government services online in terms of accessibility and convenience for citizens?
- Could you share your experience in using e-government services and how important do you think digital literacy is for effectively utilizing these services?
- How would you assess the availability of government data and information for public access, and have you ever made Freedom of Information requests?
- Can you provide examples of cybersecurity measures implemented by the government to protect e-government systems and data from cyber threats, and how effective do you think they are?

Section 3: Future Directions and Recommendations

- Looking ahead, what do you see as the main priorities for improving cybersecurity in CERIST's e-government services?
- Are there any specific areas where you believe CERIST can further strengthen its cybersecurity posture to better protect e-government data and systems?
- How do you envision the role of collaboration and partnerships in enhancing cybersecurity for e-government, both within Algeria and internationally?

Interview Guide (French version):

Section 1 : Contexte et Compréhension

- Pouvez-vous donner un aperçu de votre rôle et de vos responsabilités au sein du CERIST, en particulier en ce qui concerne les services de e-gouvernement et la cybersécurité ?
- Comment définiriez-vous la cybersécurité dans le contexte du e-gouvernement, et quels en sont, selon vous, les principaux objectifs et défis ?
- Pourriez-vous décrire les initiatives de e-gouvernement gérées par le CERIST et leur importance dans le contexte de l'Algérie ?

- Quelles sont certaines des principales mesures et protocoles de cybersécurité actuellement en place au sein du CERIST pour protéger les services et les données de e-gouvernement ?

Section 2 : Rôle de la Cybersécurité dans les Services de E-Gouvernement

- De votre point de vue, quelle est l'importance de la cybersécurité pour assurer l'efficacité et la fiabilité des services de e-gouvernement fournis par le CERIST ?
- Pouvez-vous partager des exemples d'incidents ou de défis en matière de cybersécurité que le CERIST a rencontrés par le passé, et comment ils ont impacté les opérations de e-gouvernement ?
- Comment évaluez-vous le niveau de confiance et de sécurité du public dans les services de e-gouvernement du CERIST en matière de cybersécurité ?
- Quelles mesures le CERIST a-t-il mises en place pour atténuer les risques liés à la cybersécurité et améliorer la résilience de son infrastructure de e-gouvernement ?
- Pouvez-vous décrire le processus que votre organisation suit pour détecter et répondre aux incidents de cybersécurité, tels que les violations de données ou les attaques de logiciels malveillants ?
- En général, combien de temps faut-il pour identifier et résoudre les incidents de cybersécurité au sein de votre organisation ?
- Comment votre organisation identifie-t-elle et priorise-t-elle les vulnérabilités logicielles pour les corriger ?
- Quelles mesures votre organisation prend-elle pour sensibiliser les employés à la cybersécurité ?
- Dans quelle mesure votre organisation se conforme-t-elle aux normes industrielles et aux exigences réglementaires en matière de cybersécurité ?
- À quelle fréquence votre organisation rencontre-t-elle des incidents de sécurité tels que des infections par des logiciels malveillants, des attaques de phishing ou des tentatives d'accès non autorisé ?
- Comment évalueriez-vous la disponibilité des services gouvernementaux en ligne en termes d'accessibilité et de commodité pour les citoyens ?

- Pourriez-vous partager votre expérience de l'utilisation des services de e-gouvernement et à quel point pensez-vous que la littératie numérique est importante pour utiliser efficacement ces services ?
- Comment évalueriez-vous la disponibilité des données et informations gouvernementales pour l'accès public, et avez-vous déjà fait des demandes d'accès à l'information ?
- Pouvez-vous donner des exemples de mesures de cybersécurité mises en œuvre par le gouvernement pour protéger les systèmes et données de e-gouvernement contre les cybermenaces, et quelle en est l'efficacité selon vous ?

Section 3 : Orientations Futures et Recommandations

- En regardant vers l'avenir, quels sont, selon vous, les principales priorités pour améliorer la cybersécurité des services de e-gouvernement du CERIST ?
- Y a-t-il des domaines spécifiques où vous pensez que le CERIST peut renforcer davantage sa posture de cybersécurité pour mieux protéger les données et systèmes de e-gouvernement ?
- Comment envisagez-vous le rôle de la collaboration et des partenariats dans l'amélioration de la cybersécurité pour le e-gouvernement, à la fois en Algérie et à l'international ?