Digital Transformation and Its Impact on the Application of Cyber Security in the Ministry Of Interior and National Security in Palestine

Mazen J. Al Shobaki[1], Suliman A. El Talla[2], Mahmoud T. Al Najjar[3]

[2]College of Intermediate Studies – Al-Azhar University – Gaza, Palestin
[3]Faculty of Administrative and Financial Sciences, Israa University – Gaza, Palestine.
[1]mazen.alshobaki@gmail.com, [2]Eltallasuliman@gmail.com, [3]malekzain750@gmail.com

Abstract **:** *This study aimed to identify the digital transformation and its impact on the application of Cyber Security in the Palestinian Ministry of Interior and National Security. The study used the analytical descriptive approach. The study tool (questionnaire), and the comprehensive survey method was used, where (61) questionnaires were retrieved (87.1%), and they were unloaded and analyzed using the SPSS statistical package. The study found several results, including that there is a statistically significant correlation between all dimensions of Digital transformation and the application of Cyber Security in the Ministry of Interior and National Security. And that there is an impact of Digital transformation on the application of security in the Ministry of Interior and National Security in the governorates of Gaza, and the impact coefficient was (0.897). It was found that the dimensions affecting the dependent variable of Cyber Security are dimensions (organizational structure, job description, data privacy and security, technical infrastructure required for digital transformation), as these dimensions affect (89.7%) of the variation in the application of Cyber Security. The study presented a set of recommendations, the most important of which are: The need for the Ministry's administration to provide a special budget to develop the quality of its electronic services as a lever for digital transformation. And the need for the number of workers in computer and information technology departments and units to be commensurate with the volume and quality of work to bridge the gap between the required performance and the actual performance. The ministry should set a clear methodology for exchanging data and information between the components of the ministry. And the need for the Ministry of Interior and National Security to use a protection network capable of detecting all threats.*

Keywords: Digital Transformation, Cyber Security, Ministry of Interior and National Security, Gaza Strip, Palestine.

Introduction

The technological progress and the information revolution that the world has witnessed in the world of communications for decades have brought about tremendous changes and a positive impact on the business world through the introduction of new variables. Raising efficiency in addition to improving performance levels based on harnessing the capabilities of this technology on the human element, which represents the main driver for the use of these technologies. It is not necessary to abolish all traditional systems.

According to (Jarbou, 2018), it has become imperative for decision makers and those interested in managing these organizations to keep up with the changes that contribute positively to the process of development in various fields, to advance scientific progress, and to study the challenges they face in various fields, including economic, social, And technology in order to confront and overcome it without colliding with it, and for that, decision makers and interested parties took it upon themselves to make the necessary arrangements and apply some modern management concepts.

This information revolution has had a role in developing some new administrative concepts and patterns, including digital transformation and electronic management, and other concepts that depend on information technology, as (Al-Halabi et al., 2022) believes that digital transformation is a key factor for providing services efficiently and effectively. High, as it is a necessity for all institutions that seek to improve their services and achieve governance and effective communication, both internally at the level of the organization, or externally with various partner institutions. Rather, it has become a natural process for organizations that seek to maintain their competitive advantage, and within the framework of the efforts of the Ministry of Interior and Security It is necessary for it to develop in an integrated manner, taking into account the necessity of exploiting all the opportunities and possibilities offered by the technological revolution and digital technology.

According to the study (Bahour, 2016), the benefit of these advanced technologies in the public and private sector institutions operating in Gaza Strip still does not rise to the desired level due to the presence of some challenges, especially in the field of readiness of these organizations to manage and implement such modern concepts, in addition to the spread of the phenomenon of Cybercrimes and the penetration of information centers, which prompted decision makers in organizations to seriously think about following methods and procedures to confront these crimes, and to use safe systems known as the Cyber Security Department, which is interested in providing advanced systems and protocols in order to protect data from these risks, taking into account the need to monitor threats And evaluate them first, as cyber security is a strategic weapon to confront these risks.

The researchers believe that digital transformation and Cyber Security management help organizations, including the Ministry of Interior, to provide electronic services at low costs, in addition to growing their work, obtaining good statistics and data analysis, and helping them to face some challenges represented in the dangers of cybercrime.

Based on the foregoing, the study seeks to highlight The Reality of Digital transformation and Cyber Security at the Ministry of Interior and National Security in Gaza Strip. The importance of Cyber Security in facing challenges that may hinder the process of Digital transformation will also be addressed from the point of view of computer and information technology units.

Definition of Key Terms

There are many terms that were used in the study, the most important of which are:

- **Digital Transformation**: integrating digital technology into all areas of work with the aim of providing advanced modern technologies through a digital environment (Al-Halabi et al., 2022)
- **Procedural definition**: A process by which the business model of government institutions is transformed into a digital technology-based model.
- **Cyber Security**: A set of technical and administrative measures that include the processes and mechanisms applied by institutions to secure their digital infrastructure and maintain the confidentiality of data and information (Al-Jifnawi, 2021).
- **Procedural Definition**: A set of technical, organizational and administrative means adopted by organizations that are used to prevent network penetration and maintain digital infrastructure.
- **The Ministry of Interior and National Security**: It is one of the sovereign and most important ministries in the Palestinian government, as it performs an outstanding performance in carrying out its tasks and ensuring the interest of the homeland and the citizen, organizing civil life, and implementing the law for everyone (http://www.moi.gov.ps).

Problem Statement

Today, digital technology in general and the digital cloud in particular has become a new model for benefiting from the information revolution, in coordination and cooperation between companies, governments and institutions within the framework of exchanging data and information and enhancing the role of technology and the Internet in the administrative, control and regulatory process for it, and this is consistent with the study of (Saleem, 2011) which It turns out that digital transformation has become one of the concepts that most attracted the attention of stakeholders in the information field because of the opportunities it provides to organizations to improve the electronic services they provide. The process of Digital transformation is an advanced idea that is in line with the requirements of the times and helps to establish an infrastructure at reduced costs. It also provides a wide scope for companies and organizations as it provides many benefits to the data owner and users, and works to secure data and services, flexibility and cost efficiency for the user (Al-Assaf, 2000).

Although governmental institutions in Gaza Strip, including the Ministry of the Interior, have many scientific and practical achievements, they still face many challenges and obstacles, the most prominent of which are electronic hacking operations and attempts to steal data. From this standpoint, it has become necessary for all organizations to adopt a number of approaches. Which contribute to the provision of protection rules and systems in order to address electronic penetration, and this is one of the most prominent tasks of the Department of Cyber Security, so this study comes to shed light on the importance of applying digital transformation and the availability of the necessary requirements for managing the digital transformation process for adoption in administrative work, and providing services to the public, taking into account Data privacy and security.

Based on the foregoing, the researchers discovered the problem of the study and its importance. Therefore, the study will focus on exploring The Reality of managing the digital transformation process, in addition to the process of managing Cyber Security at the Ministry of Interior and National Security - Gaza Strip.

Research Questions

From the foregoing, the main question that the head will answer has been concluded, which is:

What is The Reality of applying the requirements of Digital transformation and Cyber Security management by the Ministry of Interior and National Security from the point of view of workers in computer and information technology units?

A number of sub-questions will be divided, which the study will answer, as follows:

Q1-: What is the extent of senior management support in the Ministry of Interior necessary to manage the digital transformation process?

Q2-: What is the availability of strategic directions in the Ministry of Interior necessary to manage the digital transformation process?

Q3-: What is the availability of the technical infrastructure in the Ministry of Interior necessary to manage the digital transformation process?

Q4-: What is the availability of the human and organizational resources in the Ministry of Interior and National Security necessary to manage the digital transformation process?

Q5-: How appropriate is the organizational structure for managing the digital transformation process in the Ministry of Interior and National Security?

Q6-: What is the extent of the necessary coordination to manage the digital transformation process in the Ministry of Interior?

Q7-: What is the degree of impact of data privacy on the Ministry of Interior and National Security's management of a digital transformation process?

Q8-: What are the most important challenges facing the Ministry of Interior and National Security to manage Cyber Security?

Research Objectives

Based on the established research questions, this study aims to achieve the following objectives:

1. Knowledge of The Reality of Digital transformation and cyber security at the Ministry of Interior and National Security.
2. Studying the role of senior management in the Ministry of Interior in managing the digital transformation and cyber security process.
3. Identify the strategic directions for the successful management of the digital transformation process and cyber security
4. Exploring the readiness of the technological and technical environment to manage the process of Digital transformation and Cyber Security.
5. Studying the impact of coordination between the components of the ministry in managing the digital transformation process and Cyber Security.
6. Studying the role of human and organizational resources in managing the digital and cyber transformation process.
7. Learn about the role of the organizational structure and job description in managing digital transformation and cyber security.
8. Learn about the impact of data privacy on adopting digital transformation and cyber security.
9. Identify the most important challenges facing Cyber Security management.
10. Coming up with recommendations that contribute to strengthening the management of the digital transformation process and managing Cyber Security.

Research Importance

The aspects of the importance of the study can be identified from the contribution and the expected addition from it, as follows:

Scientific (Theoretical) Importance:

1. The importance of this scientific study is evident in the fact that digital transformation and Cyber Security are one of the most important modern technologies that are expected to bring about a major revolution in the performance of institutions in terms of quality and improvement of the service provided by these institutions to beneficiaries, for their role in providing distinguished programs and applications, very large storage spaces, data monitoring and preservation Security and less cost.
2. Enriching scientific research on this topic, as it is considered one of the modern topics, according to the researchers' point of view.

Practical (Applied) Importance:

1. You may work to support decision-making at the Ministry.
2. May support the oversight process of the Ministry's services and projects.
3. Assist in organizing and arranging work within the ministry.

Research hypothesis

Ho$_1$: There is a statistically significant relationship at the level of significance ($\alpha \leq 0.05$) between digital transformation and the application of Cyber Security in the Ministry of Interior in the southern governorates.

Ho$_2$: There is a statistically significant effect at the level of significance ($\alpha \leq 0.05$) of the digital transformation in its dimensions on the application of Cyber Security in the Ministry of Interior and National Security in the governorates of Gaza.

Research Limits and Scope

The scope of the study shall be as follows:

1. **Objective Limits**: The study focused on the requirements of managing the process of Digital transformation and Cyber Security.
2. **Human Limits**: The study was conducted on workers in the computer and information technology units of the Ministry of Interior.
3. **Institutional Limits**: The study was conducted on a sample of workers in the Ministry of Interior - the southern governorates.
4. **Spatial Limits**: The study was conducted in the State of Palestine.
5. **Temporal Limits**: the year 2022.

Previous Studies

- Study of (Al Najjar et al., 2022) aimed to identify the extent of the application of Cyber Security at the Ministry of Interior and National Security from the point of view of workers in the computer and information technology units. 70 employees, and the study tool (questionnaire) was distributed, and the comprehensive survey method was used, as (61) questionnaires were retrieved at a rate of (87.1%), and they were unloaded and analyzed using the SPSS statistical package. The study reached several results, including: There was a high degree of agreement on the degree of Cyber Security application, which amounted to (74.8%). With a relative weight of (74.8%), and The Dimension efforts to monitor threats, it received a high degree of approval and a relative weight of (73.4%). Privacy has a high degree of approval with a relative weight of (78.4%).
- Study of (Al Najjar et al., 2022) aimed to identify the reality of Digital transformation in the Palestinian Ministry of Interior and National Security from the point of view of workers in computer and information technology units.) employees, and the study tool (the questionnaire) was distributed, and the comprehensive survey method was used, where (61) questionnaires were retrieved with a percentage of (87.1%), and they were unloaded and analyzed using the statistical packages SPSS. The study reached several results, including: The availability of dimensions of Digital transformation to a large extent in the Ministry of

Interior, Security and National and its amount reached (77.5%). The average overall score for the senior management support dimension scored a large approval degree and a relative weight (78.2%), and The Dimension strategic directions it received a large approval degree and a relative weight (76.3%), The Dimension the technical infrastructure necessary for digital transformation achieved a large approval degree and a relative weight. (73.4%), The Dimension human resources, it scored a large approval degree and a relative weight (72.2%), The Dimension coordination, a large approval degree and a relative weight (82.7%), The Dimension data privacy and security, it scored a large approval degree and a relative weight (80.7%), The Dimension the organizational structure and job description, it received a high degree of approval and a relative weight of (79.3%).

- Study of (Al-Halabi et al., 2022) aimed at identifying the impact of transformational leadership and its role in managing the digital transformation process in the Ministry of Interior and National Security - the civil part. To achieve the objectives of the study, the researchers used the analytical descriptive approach, and the questionnaire was used as a tool for collecting data from a sample The study consisted of (207) employees working in supervisory positions in the Ministry, and (165) questionnaires were retrieved from the distributed questionnaires. The study reached a number of results, the most prominent of which is the existence of a direct relationship between the application of Digital transformation and transformational leadership in all its dimensions.
- A study of (Al-Jifnawi, 2021) titled "Digital Transformation of National Institutions and Cyber Security Challenges from the Point of View of Academic Police Officers in Kuwait", which aimed to identify the digital transformation and challenges of Cyber Security in the State of Kuwait from the point of view of academic officers, and the researcher used the descriptive analytical approach To achieve the objectives of the study, and to collect data for the study, the researcher designed a questionnaire and distributed it to the study sample consisting of 80 academic officers. For educational qualification, experience, age and training courses.
- A study of (Kuzu, 2020), which aimed to identify the impact of strategic planning on the adoption of Digital transformation by universities, in addition to identifying methods of Digital construction of education systems in universities. The researcher used the descriptive approach, and the researcher built a special questionnaire to collect data from the study sample, which is a number of universities. Turkish, and the results showed that strategic planning has an important and major role in adopting digital transformation, and the adoption of computerized systems has a fundamental role in digital transformation.
- A study of (Madi and Abu Hajeer, 2020), which aimed to identify the extent of the readiness of Palestinian private universities for digital transformation, and the researchers used the descriptive analytical approach to achieve the purpose of the study. , Gaza), and (170) questionnaires were distributed, and 65% of the questionnaires were retrieved by (110) questionnaires. They are good at adopting digital transformation, and the scarcity of human and financial resources was the most important obstacle facing the implementation of the transformation.
- A study of (Abdullah, 2019), which aimed to identify the most important factors that contribute to the implementation of Digital transformation in the Sultanate of Oman. The study concluded that the Ministry's Information Authority adopted a strategic plan for all government departments to implement digital transformation.
- A study of (Faraj, 2021), which aimed to address the reasons and importance of promoting a culture of Cyber Security in light of Prince Sattam University’s adoption of Digital transformation according to a number of variables, the most important of which are the years of experience in addition to the scientific specialization. Purpose The researcher built a questionnaire consisting of 26 paragraphs, and it was distributed to the study sample, which amounted to 125 members of the faculty at the university. This was followed by the cognitive reasoning axis, and finally the technical reasoning axis.
- A study of (Moskal, 2020), which aimed to study the importance of enhancing Cyber Security in American universities in light of the digital transformation, and the researcher used the descriptive approach to achieve the purpose of the study, and the researcher built a special questionnaire to collect data from the study sample of 100 American universities, and the study showed the importance of developing a vision To establish a cyber security center in American universities with the aim of increasing cyber awareness.
- A study of (Al-Sanea et al., 2020), which aimed to identify the degree of awareness of teachers about Cyber Security and its relationship to national values. The study raises teachers' awareness of cyber security in the field of protecting private devices.
- A study of (Al-Qahtani, 2019), which aimed to identify the extent of awareness of Cyber Security among university students in Saudi universities, in addition to studying the most important methods of community prevention from cybercrime. The researcher used the analytical descriptive approach, and the researcher built a special questionnaire to collect data of the study sample, which amounted to 486 male and female students, the study showed that the crime of electronic fraud is the most common crime that Cyber Security deals with.
- A study of (Al-Jundi, 2019), which aimed to identify the importance of practicing and applying Cyber Security and the accuracy of the practical application of information security. The researcher used the descriptive analytical approach to achieve the objectives of the study. The researcher collected data through a special questionnaire that was distributed to the study sample, which amounted to 80 students. From the Department of Computer Science at Umm Al-Qura University. The study showed that the application of Cyber Security practices will enable students to understand the guiding standards for conducting risk assessments.

- A study of (Catota & Sicker, 2019) aimed at clarifying the importance of building national capacities for Cyber Security, which were relied upon to successfully confront cyberattacks, in addition to the importance of drawing up a national strategy for Cyber Security through which you can protect the digital technological infrastructure of developing countries. Cyber programs and technological awareness, in addition to cooperation and integration of roles between universities contribute to the promotion of cyber culture.
- A study of (Maranga & Nelson, 2019), which aimed to identify ways universities secure their sites and data from cyber attacks, and to achieve the purpose of the study, the researchers used the descriptive analytical approach through the questionnaire as a tool for collecting data from university workers. The study showed that one of the most important means of protecting universities is good planning of mechanisms Cyber security, in addition to spreading cyber concepts.
- A study of (Al-Arishi and Al-Dosari, 2018), which aimed to study the electronic risks that threaten information security in cyberspace, and the study also touched on the most important procedures that must be followed to promote a culture of Cyber Security in society. The researcher built a special questionnaire to collect data that contributes to achieving the objectives of the study, while the study sample consisted of 702 students from King Saud University. The study showed that the development of cultural thought on the importance of information security is one of the most important roles of society to promote a culture of Cyber Security.
- A study of (Ninkeu, 2018), which aimed the study to identify the concepts of cyber security and cyber violations, and to achieve the purpose of the study, the researcher used the interview as a tool to collect data from the study sample, who are the students of the Catholic University, and the study showed that there is a weakness among university students in the concepts of internet security and cyber security in addition to cyber risks, and the study recommended the need to strengthen cyber security concepts by including them in academic curricula.

Commenting On Previous Studies

It is clear from a review of previous studies that these studies have varied and differed according to the goals they sought to achieve, as well as the different environments in which they were applied, the variables they studied, the methods used and the tools that were used. Below, the researchers will present the most important aspects of agreement and disagreement, as well as what distinguishes his study about previous studies:

Advantages of previous studies

- Enriching the theoretical framework in the study.
- Building the questionnaire study tool.
- Ensure that the current study is not repeated.
- Provide the necessary references for the study, especially foreign references.

The Study Is Characterized

- The study was applied to the environment of the government sector institutions in Gaza Strip and the administration of the Ministry of Interior and National Security.
- The use of a number of tools for the data, as the researchers relied on more than one method in collecting primary data, most notably interviews, questionnaires, and holding a workshop.

Theoretical Framework

The prominent role of knowledge has led to the emergence of societies called knowledge societies, which are societies based on knowledge, keeping pace with the rapid technological transformations that the world is witnessing, whether by using new technologies, or updating and upgrading existing programs and technologies, in addition to contributing to the emergence of modern terms in This aspect as the term digital transformation. According to (Al-Balochi et al., 2020), there are many concepts for the term digital transformation, which can be considered a phenomenon resulting from a group of modern digital technologies that operate simultaneously, and among these technologies are computer, artificial intelligence, cloud computing, and others. (Lanzolla, 2018) believes that digital transformation contributes to decision-making and strategic planning through the production of large and new amounts of information (Al Najjar et al., 2022).

According to the Omani Ministry of Technology and Communications, digital transformation is defined as the use of information and communication technology with the aim of developing institutional performance, increasing effectiveness and efficiency in the level of government service provision by employing modern and renewable technologies, and (Al-Shoubri, 2020) defines digital transformation as organizations' use of technical methods in managing its business and activities, in addition to data processing through the provision of a secure digital technical environment based on databases protected by a secure system. (Hajjaj, 2021) defines digital transformation as organizations investing in digital programs and applications available via the Internet in order to reach the beneficiaries of their provided services with the aim of improving performance, and (Madi and Abu Hajeer, 2020) defines it as a continuous process through which all elements are introduced. Technology and electronic means in all administrative work policies and procedures in order to provide high quality services that are in line with international standards.

The researchers adopt the following definition of Digital transformation as a procedural definition, which is a process through which the business model of government institutions is transformed into a model based on digital technology.

According to (Al-Balochi et al., 2020), the use of Digital transformation technologies was not limited to companies or private institutions, but rather the government sector and its institutions took the initiative to use them.

According to Saudi Vision 2030, the most important digital transformation technologies are:

- Digital Video.
- Cloud Computing.
- Mobile Phone Devices.
- Social Networks.
- Online Platforms.
- Smart Sensors.
- Location Detection Technology.
- Electronic Display Screens.

Digital Transformation Goals

Spear (2020) sees that digital transformation achieves a number of important goals, the most important of which are:

- Spreading the culture of Digital transformation and building the digital mentality among all employees in organizations.
- Organizations have an important information digital infrastructure that enables them to carry out their work via the Internet.
- Providing electronic services at all times with high quality and low costs.
- Achieving a competitive advantage, in addition to distinguishing between all institutions.
- Developing the outputs of the administrative process and strengthening the electronic system.

Hajjaj (2021) believes that the purposes of Digital transformation are:

- Determine the target sectors and the field of work, and identify the targeted geographical boundaries for providing services, through the use of modern technical means in research and communication.
- Gathering the necessary basic information about the audience of beneficiaries in order to facilitate communication.
- Creating databases that include all beneficiaries.
- Combine centralization and delegation through centralization and decentralization of work.
- Increase the efficiency of management and field work

Benefits of Digital Transformation in Organizations (Al Najjar et al., 2022):

The digital transformation achieves a set of benefits for all service providers and also for the beneficiaries of the services, according to (Hajjaj, 2021), among these benefits:

- Significantly saving time, effort and cost for beneficiaries and institutions.
- It contributes to improving the quality of services.
- Simplify procedures for obtaining services.
- Helps eliminate duplication, in addition to achieving transparency in work.
- Contributes to getting rid of routine procedures.
- Achieving excellence in government performance and improving the level of services provided.
- Develop organizational structures within organizations.

According to (Al-Balochi et al., 2020), digital transformation has effects on performance, which are as follows:

- Speed in doing business.
- Enhancing the ability and flexibility to keep pace with changes quickly.
- Eliminate red tape and bureaucracy.
- Increase business efficiency.
- Achieving integrity, transparency and maintaining data confidentiality.
- Networking between all components of the ministry.
- Reducing employee errors.
- Saving financial expenses.
- Facilitate easy updating and dissemination of information.

Factors affecting the management of the digital transformation process (Al Najjar et al., 2022)**:**

The researchers studied and reviewed a number of previous literature on digital transformation. It was noted that a number of previous researchers touched on some models that contribute to some of the requirements necessary for the digital transformation process. Some of these factors will be addressed as follows:

▪ **Digital Transformation Strategy** (Al Najjar et al., 2022)**:**

- Building the vision and mission of Digital transformation.
- Senior management support
- Nurturing creative individuals within the ministry.
- Determine responsibilities and roles and monitor and review the system.

- **Spreading The Culture Of Digital Transformation** (Al Najjar et al., 2022)**:**
- Emphasizing the right of individuals to training.
- Participation of workers in digital transformation programs.
- Spreading the culture of training and continuing education.
- **Human Resources:**
- Developing workers' skills by identifying current and future needs in information systems.
- Attracting the best qualified individuals in the field of programming and computing.
- **Technological And Material Requirements** (Al Najjar et al., 2022)
- The availability of the technological environment and digital communications.
- Availability of financial support.
- The existence of an electronic network linking the components of the ministry to each other.
- Data privacy and security and an approved data security policy.
- **Administrative And Organizational Requirements** (Al Najjar et al., 2022)**:**
- Provide flexible management systems.
- Partnership with entities, experts and outsiders.
- Existence of systems for evaluation and technical development.
- Issuing legislations that allow digital transformation.
- Reviewing applicable laws and regulations.

Al Najjar et al., (2022) believes that there is a set of practices that lead to the adoption of Digital transformation in organizations, namely:

- Adopt a clear policy for the introduction of information and communication technology.
- Freedom of decision and dedication to human resources.
- Provides outstanding technological performance associated with the latest technological developments.
- An outstanding investment in continuous technical training.
- Continuous emphasis on hiring the best human resources.

Digital transformation steps (Al-Halabi et al., 2022) and (Al Najjar et al., 2022)**:**

- Preparing a strategic vision to achieve digital transformation and identify future needs.
- Analyzing the external environment as an essential step before starting the digital transformation due to the rapid technological developments in order to build an updated strategy according to the latest developments.
- Designing a digital experience for users by adopting a specific application to work through.
- Evaluating the current reality, examining the basic digital infrastructure, and determining its extent and suitability for the objectives.
- Consulting with a range of external experts to ensure digital excellence is achieved and successful.

Digital Transformation Tools (Al Najjar et al., 2022):

- Email System.
- File Transfer System.
- Lists Search Service.
- Postal Menus Service.
- Spider Network Service.

Second - Cyber Security:

Cyber security includes protecting the privacy of data and key devices from external risks and cyber threats. According to (Al-Jifnawi, 2021), the origin of the word cyber security goes back to the Latin word Cyber, by which we mean information space, and by this cyber security we mean the security of information space. (Al-Bahi, 2017) said that Cyber Security is linked to the World Wide Web and the communications network, where Cyber Security represents the basic pillar of any digital transformation, and according to (Al-Janabi, 2017), Cyber Security aims directly at moving from routine work to technical work in its various forms through The use of non-traditional techniques, and the most important of these technologies is computer networks that depend on linking all organizational units with each other, in addition to the oversight bodies charged with following up the workflow, preserving information accurately, and facilitating dealing with it with better accuracy, in addition to the main role of the oversight bodies represented in Identify hackers' devices and their identity (Al Najjar et al., 2022).

Kennedy (2017) was defined as a system that works to protect electronic data from risks through the use of organizations for a group of technical and administrative means in order to protect the privacy of data and files, in addition to taking the necessary measures to protect them.

(Qari et al And their data from the electronic attacks that target them, and it is measured by the degree that the teacher gets through his answer to the Cyber Security paragraphs, and he (Al-ManThari, 2020) is known as a security concept for the protection of information and all its money is related to that information of operations, services and technologies against any external danger, or Use it negatively.

(Richardson Etc Al, 2020) is known as the technical security and precautions that are followed for the garrison of devices, information systems and data from unauthorized access to maintain the safety and integrity of the data stored in digital devices.

The researchers adopt a procedural definition of Cyber Security as a set of technical, organizational and administrative means that are used to institutions that are used to prevent networking and maintaining digital infrastructure.

Cyber Security Departments (Al Najjar et al., 2022)**:**

Moore (2018) divided Cyber Security into several sections, namely:

- Communications Security: It aims to protect against threats affecting the infrastructure and technology of communications and to protect and preserve it from any external threat.
- Operations security: It aims to protect operations and workflow methods from any external risks.
- Information security: It aims to protect information and restrict access to it by unauthorized persons, in addition to protecting its privacy from theft.
- Physical security: It aims to protect the physical assets related to the cyber system, such as servers and electronic networks, from any external risks.
- Application Security: It aims to protect applications and provides a degree of security and protection from defects that may arise from design, development or installation defects.

Cyber Security Requirements (Al Najjar et al., 2022)**:** Kennedy (2017) believes that there are a number of basic requirements for the success of Cyber Security, and among these elements:

- Physical elements: These are devices, technical and electronic parts, and tools that represent the necessary infrastructure for the operation of information systems.
- Software components: These are the non-physical components that include the basic software required to operate the systems.
- Human elements: They are people with competence and skills in the field of information technology, and they are interested in operating and updating systems, and maintaining the continuity and continuity of work.
- Support for the top management of the organization:
- Flexibility of the organizational structure and non-resistance to change.

Cyber Security Objectives (Al-Janabi, 2017) and (Al Najjar et al., 2022)**:**

- Ensure the continuity of applications and information systems.
- Updating information systems and protecting them from external risks.
- Work to protect the privacy and confidentiality of information in all its forms.
- Use the necessary measures in order to protect citizens from the risks arising from the use of the Internet.
- Protect operational and technical devices from cybercrime.
- Maintaining the information network.

The Importance of Cyber Security: The imposition of falling as a victim of cybercrime is increasing day by day, in light of the lack of sufficient awareness, and reliance on the use of the World Wide Web in all aspects of life, especially after relying on digital transformation (Shiling ford & Stewarb, 2011). This confirms the importance of Cyber Security that it has a number One of the advantages and the primary task of Cyber Security is to maintain the confidentiality of data and protect its privacy, and (Al-Janabi, 2017) believes that the name of the user and the request to verify his identity is the basis for preventing the access of unauthorized persons to view the data, and Cyber Security is also concerned with maintaining the unity of Information by preventing tampering with it, and (Al-Wakil, 2017) adds that there are a number of advantages:

- The ability to save costs in return for high quality and accurate results.
- Remote work, ensuring protection from risks.
- Identify the amount of deviation in performance.
- Save time for comprehensiveness and integration of results.

Cyber Risks: Cyber risks are represented in all practices that have a criminal purpose in cyberspace and that target individuals, institutions, and governments. According to (Tiwari. et al, 2016), they can be classified into two parts, where the first part targets digital devices and information networks, and the other: targets individuals who use the Internet personally. Or within their various functions in governments.

Among the forms of cyber risks are viruses, cyberbullying, defamation, hacking, and phishing, and according to 2022 statistics, 28% of cyber attacks on data involved the use of viruses and 52% of attacks involved hacking techniques (Information and Decision Support Center, 2020) and these can be clarified The risks are as follows:

- ▪ **Viruses**: They are harmful computer programs that are transmitted through digital devices in several ways, and they spread between files and constitute extremely serious damage, and they vary in their forms, strength and continuation within the digital system, and their danger can reach the point of destroying the digital environment and disrupting its movement (tochi. Et al 2012).

- **Electronic Bullying**: Electronic bullying is the most prevalent forms of cybercrime, especially among school and university students, and it is classified as a form of Digital harassment; Where the victim is harmful for a long time, and he is pursued, controlled by his actions, and the victim threatens to harm, scandal and contempt, and it has spread in the past years significantly. (MENESINI. & Nocentini, 2009)
- **Reputation**: where the victim is aimed at spreading incorrect information and abusing the person and reducing his position using incorrect images or videos that have been treated to serve the crime goals, and send them through social media or e -mail, and it can also aim to distort institutions also with the intention of reducing Its competitive position on the market. (Nathaanael J.2012).
- **Piracy**: It is the process of unauthorized entry in digital information systems with the aim of breaking the security protections of information systems and obtaining secret information and data, whether for individuals, institutions or governments, and causing their loss (Hall & Watson, (2016).
- **Hunting**: It is one of the easiest cyber risks in preparation; where the construction creates a website (for unknown institutions or companies) and sends messages via e -mail from those sites for the purpose of obtaining personal data and information that is used for criminal purposes (Vayansky. & Kumar / 2018)
- **Internet Terrorism**: Terrorist organizations use the Internet to implement a wide variety of purposes that include: recruitment, financing, advertising, training, incitement to commit terrorist acts, collecting and publishing information for terrorist purposes. The Internet is also used to facilitate communication between all terrorist organizations (United Nations, 2013).
- **Violation Of Information Security**: All the uses of information systems and their digital applications loaded on computers are exposed to harmful attacks or failure and disclose the confidentiality of their information or not to save the privacy of the data of the bodies and those dealing with them or delay in their availability at the appropriate time for those who need it quickly, that is, there are many risks to access Unintended, inappropriate and unoccupied use, or the failure of the same systems for side causes, knowing that many information systems and applications, whether public or private, such as those used in military and security purposes, banks, hospitals, and others represent a fertile ground for growing information terrorism today (Al -Hadi, 2006).
- **Intellectual Evidence**: The damage resulting from placing the name of the plaintiff includes scientific work, forging the author's seal, and assaulting any of the rights of the author or neighboring rights (Al-Manthari and Hariri, 2020).

Methods of Protection from Cyber Risks (Al Najjar et al., 2022)**:** One of the most important means of protection that must be followed and applied to address cyber risks is to develop awareness among Internet users of how to use safely through networks. After many cases of cyber attacks occurred in many countries that targeted schools, universities and other institutions, the matter required the Ministry to play a clear role in planning for cyber security. To protect its environment from these attacks.

Third- Ministry of Interior and National Security:

It is one of the most important ministries in the Palestinian government, bearing complex responsibilities under intertwined conditions, difficult data and multiple security and political crises, as it contributed to finding solutions to many problems, providing an appropriate work environment, finding appropriate alternatives, developing work and facilitating administrative operations and procedures. The Ministry must impose the rule of law on everyone without discrimination or favoritism, control the security situation, provide security for the citizen, and protect the internal front - and to address the events and security crises. The Ministry of Interior received the attention and care of the Palestinian political leadership as one of the most important political ministries for its role in providing security and safety for the Palestinian citizen, and it undertakes important changes and seeks to develop new leaders in order to implement its role, a more comprehensive security service for the Palestinian public.

The Ministry of Interior and National Security consists of two civil and military parts, and the civil part is represented by a number of agents, assistants, departments, directorates, and some public departments such as: the General Administration of Passports and the General Administration of Tribes Affairs, in addition to the competent units that belong to the minister directly, or belong to the ministry’s agent.

As for the security part, which is the subject of the research, it is represented by the competent agencies, departments and security bodies of the ministry, and some of them are followed directly to the minister and some of them are affiliated with the Commander -in -Chief of the National Security Forces (http://www.moi.gov.ps Accessed 2/11/2022).

Methodology and Procedures:

The study’s methodology and procedures are considered a main axis through which the applied aspect of the study is accomplished. Accordingly, the researchers will address in this chapter the procedures that were followed in preparing the study by clarifying the study’s approach and its community and then determining the sample on which the study was applied, as well as preparing a tool The main study (the questionnaire) and the mechanism of its construction, development, validity and reliability, and the chapter ends with the statistical treatments that were used in analyzing the data and drawing conclusions.

First- Study Methodology: The researchers used the analytical descriptive approach in order to achieve the objectives of the study, through which it tries to describe the phenomenon under study, analyze its data, and the relationship between its components and the opinions that are raised about it and the processes that it includes. According to (Al-Assaf, 2000), the The descriptive analytical approach did not stop at collecting information to describe the phenomenon, but rather went beyond that to clarifying the relationship and its amount, and deducing the reasons behind a certain behavior from previous data.

Second- Study Population And Sample: The study population is considered to be all the vocabulary of the phenomenon that the researchers will carry out its study on (Abu Al-Hasani, 2017) and through the problem of the study and its objectives, the target study community consists of workers in computer and information technology units and departments at the Ministry of Interior and National Security, and for Data collection for the study was done using the simple random sampling method.

Third- Study Tool: We consider the questionnaire as the most widely used and widespread tool among researchers, and the questionnaire is defined as "a tool that includes a number of dimensions, axes, and paragraphs used to obtain opinions or data by a group of respondents according to certain controls, and the respondents respond by themselves to it, which is written.

Table 1: Scores of the scale used in the questionnaire

Response	Strongly Disagree	⟵								Strongly Agree
Degree	1	2	3	4	5	6	7	8	9	10

Validity of the Study Tool

The validity of the questionnaire reflects the measurement of the paragraphs of the questionnaire, what it was prepared to measure. The validity of the questionnaire has been verified through the following:

The Veracity of the Arbitrators "Virtual Honesty": The researchers presented the study tool in its initial form to a group of arbitrators from among the specialists. Among the axes of the study, in addition to suggesting what they deem necessary to amend or delete the wording of the phrases, and based on the observations made by the arbitrators, the researchers made the amendments agreed upon by the arbitrators.

Internal Consistency Validity: It means "the extent to which each paragraph of the questionnaire is consistent with the axis to which this paragraph belongs. It was calculated on the sample of the exploratory study of (20) questionnaires, by calculating the correlation coefficients between each paragraph and the total score of the axis to which it belongs.

A. The Results Of The Validity Of The Internal Consistency Of The Dimensions Of Digital Transformation:

The following table shows the correlation coefficients between each paragraph of all dimensions and the total score of the dimension, which shows the correlation coefficients are statistically significant, as the probability value (Sig) is less than (0.05), and thus it turns out that the paragraphs of the dimension are true.

Table 2: The results of the validity of the internal consistency of the dimensions of Digital transformation

No.	R	SIG.	No.	R	SIG.	No.	R	SIG.	No.	R	SIG.
Senior Management Support			Strategic Directions			Technical Infrastructure Needed For Digital Transformation			Human Resources		
1	0.728	*0.000	1	0.536	*0.000	1	0.745	*0.000	1	0.862	*0.000
2	0.545	*0.000	2	0.839	*0.000	2	0.796	*0.000	2	0.707	*0.000
3	0.766	*0.000	3	0.868	*0.000	3	0.515	*0.000	3	0.601	*0.000
4	0.694	*0.000	4	0.688	*0.000	4	0.450	*0.000	4	0.634	*0.000
5	0.817	*0.000	5	0.578	*0.000	5	0.552	*0.000	5	0.740	*0.000
6	0.662	*0.000	6	0.727	*0.000	6	0.378	*0.000	6	0.378	*0.000
7	0.461	*0.000				7	0.449	*0.000	7	0.849	*0.000
Coordination			Data Privacy And Security			Organizational Structure And Job Description					
1	0.615	*0.000	1	0.734	*0.000	1	0.905	*0.000			
2	0.794	*0.000	2	0.893	*0.000	2	0.656	*0.000			
3	0.758	*0.000	3	0.785	*0.000	3	0.656	*0.000			
4	0.627	*0.000	4	0.403	*0.000						

B. The Results Of The Validity Of The Internal Consistency Of The Dimensions Of Cyber Security:

The following table shows the correlation coefficients between each paragraph of all dimensions and the total score of the dimension, which shows the correlation coefficients are statistically significant, as the probability value (Sig) is less than (0.05), and thus it turns out that the paragraphs of the dimension are true.

Table 3: The results of the validity of the internal consistency of the dimensions of Cyber Security

No.	R	SIG.	No.	R	SIG.	No.	R	SIG.	No.	R	SIG.
Organizational Efforts			Technical Efforts			Threat Monitoring Efforts			Rules And Regulations		
1	0.862	*0.000	1	0.887	*0.000	1	0.829	*0.000	1	0.690	*0.000
2	0.884	*0.000	2	0.950	*0.000	2	0.741	*0.000	2	0.822	*0.000
3	0.907	*0.000	3	0.888	*0.000	3	0.878	*0.000	3	0.609	*0.000

4	0.856	*0.000	4	0.894	*0.000	4	0.923	*0.000	4	0.812	*0.000
5	0.872	*0.000							5	0.663	*0.000
Privacy Protection											
1	0.696	*0.000									
2	0.764	*0.000									
3	0.564	*0.000									
4	0.686	*0.000									

1. **Structural Honesty:** Structural validity is considered one of the measures of the validity of the tool and measures the extent to which the goals are achieved, and it shows the extent to which each axis of the study is related to the total score of the questionnaire items, and the following table shows that the correlation coefficients for each axis are statistically significant, as the probability value (Sig) is less than (0.05), Thus, the axes of the study are considered true in their representation of what was set to be measured.

Table 4: constructive validity of the questionnaire axes

The Hub	Correlation Coefficient	Probability Value
The Reality of Digital Transformation		
Senior Management Support	0.881	*0.000
Strategic Directions	0.793	*0.000
Technical Infrastructure Needed For Digital Transformation	0.725	*0.000
Human Resources	0.702	*0.000
Coordination	0.576	*0.000
Data Privacy And Security	0.801	*0.000
Organizational Structure Job Description	0.534	*0.000
The Reality of Cyber Security		
Organizational Efforts	0.932	*0.000
Technical Efforts	0.969	*0.000
Threat Monitoring Efforts	0.925	*0.000
Rules And Regulations	0.808	*0.000
Privacy Protection	0.552	*0.000

Stability of the Study Tool

"The stability of the questionnaire means that it gives the same result if it is re-applied more than once under the same circumstances, or in other words, the stability of the questionnaire means the stability of the results of the questionnaire and not changing it significantly if it was redistributed several times during certain periods of time, and it has been calculated The stability of the resolution in two ways:

1. **Consistency By Cronbach's Alpha Coefficient:**

The following table shows that all Cronbach's alpha coefficients are high, as the digital transformation axis obtained a coefficient of 0.896, while the cyber security axis obtained a stability coefficient of 0.942, and this indicates that the resolution has a high stability coefficient.

Table 5: Cronbach's Alpha coefficient for measuring the stability of the resolution

The Hub	The Number Of Paragraphs	Cronbach's Alpha Coefficient
The Reality of Digital Transformation	**38**	**0.896**
Senior Management Support	7	0.714
Strategic Directions	6	0.720
Technical Infrastructure Needed For Digital Transformation	7	0.689
Human Resources	7	0.777
Coordination	4	0.691
Data Privacy And Security	4	0.698
Organizational Structure Job Description	3	0.605
The Reality of Cyber Security	**22**	**0.942**
Organizational Efforts	5	0.869
Technical Efforts	4	0.915
Threat Monitoring Efforts	4	0.800
Rules And Regulations	5	0.713
Privacy Protection	4	0.695

2. **Stability By Split-Half Method:**

The test items were divided into two parts, which are the questions with odd numbers and the questions with even numbers, then the correlation coefficient was calculated between the scores of the odd questions and the scores of the even questions, and then the correlation coefficient was corrected by the Spearman Brown equation.

Corrected correlation coefficient = $\frac{2r}{1+r}$ where r is the correlation coefficient between the scores of the odd questions and the scores of the paired questions.

The following table shows that the value of the corrected correlation coefficient (Spearman Brown) is high and statistically significant, and this indicates that the questionnaire has a high stability coefficient.

Table 6: Partition half method to measure the stability of the resolution

The Hub	Correlation Coefficient Before Modification	Corrected Correlation Coefficient
The Reality of Digital Transformation	**0.914**	**0.955**
Senior Management Support	0.490	0.656
Strategic Directions	0.560	0.718
Technical Infrastructure Needed For Digital Transformation	0.720	0.838
Human Resources	0.638	0.780
Coordination	0.443	0.614
Data Privacy And Security	0.713	0.832
Organizational Structure Job Description	0.349	0.527
The Reality of Cyber Security	**0.911**	**0.953**
Organizational Efforts	0.716	0.827
Technical Efforts	0.910	0.953
Threat Monitoring Efforts	0.767	0.868
Rules And Regulations	0.661	0.751
Privacy Protection	0.375	0.545

We note from the previous table that all stability coefficients were high, as the digital transformation axis obtained a theat coefficient of (0.955), while the cyber security axis obtained a stability coefficient of (0.953), and this indicates that the resolution has a high stability coefficient.

Data Analysis, Testing and Discussion of Study Hypotheses

First: Analysis of the questionnaire axes

1. Analysis Of The Pillars Of Digital Transformation:

"The researchers used the appropriate descriptive tests: arithmetic means, standard deviations, relative weights, arrangement of the digital transformation axes and the total score, then the researchers analyzed the data of each dimension of the digital transformation separately."

Table 7: Means, standard deviations, relative weights, and rankings for each dimension of Digital transformation and the total score

#	The Hub	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	Senior Management Support	7.8220	1.51020	78.2	4
2.	Strategic Directions	7.6311	1.55846	76.3	5
3.	Technical Infrastructure Needed For Digital Transformation	7.3044	1.82992	73.0	6
4.	Human Resources	7.2201	1.84475	72.2	7
5.	Coordination	8.2746	1.87456	82.7	1
6.	Data Privacy And Security	8.0738	1.50093	80.7	2
7.	Organizational Structure Job Description	7.9344	1.83668	79.3	3
The Overall Degree Of Digital Transformation		**7.7515**	**1.60349**	**77.5**	

It is clear from the previous table that "the relative weight of the total score of the respondents' responses to the paragraphs of Digital transformation came to a large degree and amounted to (77.5%), as the coordination dimension ranked first with a relative weight of (82.7%), while the data privacy and security dimension came in the second rank with a relative weight of (80.7%) %), while the human resources dimension came last with a relative weight of (72.2%).

The researchers attribute this to the interest of the Ministry of Interior in digital transformation to keep pace with technological developments and the needs of society.

The following tables show an analysis of each dimension of Digital transformation:

A. Paragraph Analysis The Dimension: "Support To Senior Management":

Table 8: Analysis of Paragraphs: "The Dimension the Support of Senior Management"

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The Ministry's administration allocates the appropriate time towards digital transformation efforts in all transactions.	7.90	1.513	79.0	5
2.	The Ministry's administration undertakes the strategic and tactical planning process for digital transformation.	7.67	1.777	76.7	6
3.	The Ministry's administration considers digital transformation in its business and transactions a priority in its future goals.	8.08	1.429	80.8	2
4.	The Ministry's administration provides a special budget to develop the quality of its electronic services as a lever for digital transformation.	6.82	1.803	68.2	7
5.	The Ministry's administration adopts all creative initiatives seeking to implement digital transformation.	7.92	1.763	79.2	3
6.	The Ministry's administration urges all agencies to appreciate and support the building of their information technology work teams as a lever for digital transformation.	7.92	1.838	79.2	3
7.	Supports the Department of the Ministry to participate in the electronic transformation competition, which is carried out by the Ministry of Communications and Information Technology	8.44	1.911	84.4	1
Total Degree		**7.8220**	**1.51020**	**78.2**	

The following is evident from the previous table:

- The paragraph that states: Supports a department for the Ministry to participate in the electronic transformation competition that is carried out by the Ministry of Communications and Information Technology. It got first place among the rest of the paragraphs with a relative weight of (84.4%), and this indicates that there is a large degree of approval for this paragraph."
- The paragraph that states: The Ministry's administration provides a special budget to develop the quality of its electronic services as a lever for digital transformation. It got the last ranking among the rest of the paragraphs with a relative weight of (68.2%), and this indicates a high degree of approval for this paragraph."
- In general, "the relative weight of the dimension: support of senior management reached (78.2%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the fact that the support of senior management for the digital transformation process helps the success of this process, as any process of change and transformation requires support from the senior management of this administration.

B. Analysis Of Paragraphs The Dimension: "Strategic Directions":

Table 9: Analysis of Paragraphs: "The Dimension the Strategic Directions"

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The Ministry's strategic directions include clear goals towards implementing digital transformation.	7.84	1.675	78.4	2
2.	Ministry departments are working to understand their internal environment (strengths and weaknesses) and related to their ability to digital transformation.	7.79	1.694	77.9	4
3.	The Ministry's departments seek to develop their strategic plan to transform threats into opportunities that will be utilized in the future in the digital transformation process.	7.82	1.784	78.2	3
4.	The Ministry's departments seek to study and understand their external environment and the opportunities and threats it may contain if they implement digital transformation.	7.95	1.371	79.5	1
5.	The Ministry's departments are working on adopting the strategic direction based on spreading the culture of electronic excellence at all levels.	7.72	1.724	77.2	5
6.	The Ministry's departments spend sufficient amounts of money on innovation in how they provide their services.	6.67	1.904	66.7	6
Total Degree		**7.6311**	**1.55846**	**76.3**	

The following is evident from the previous table:

- The paragraph that states: The Ministry's departments seek to study and understand their external environment and what it includes of opportunities and threats that may surround them if they implement digital transformation. It got the first place among the rest of the paragraphs with a relative weight of (79.5%), and this indicates that there is a large degree of agreeing to this paragraph.

- The paragraph that states: Ministry departments spend sufficient amounts on innovation in how to provide their services. Got the last ranking among the rest of the paragraphs with a relative weight (66.7%), and this indicates that there is a medium degree of approval for this paragraph."
- In general, "the relative weight of the dimension: strategic directions was (76.3%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the importance of having strategic directions that support the digital transformation process through the presence of a vision and a strategic plan for the transformation process.

C. Analysis Of Paragraphs The Dimension: "The Technical Infrastructure Necessary For Digital Transformation":

Table 10: Analysis of paragraphs: “The Dimension the technical infrastructure necessary for digital transformation”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The Ministry has high-speed internet lines and its services are available without interruption.	5.93	2.040	59.3	7
2.	The Ministry has computers and modern software to benefit from the information.	6.52	1.988	65.2	6
3.	Technical support services are available to all departments on a routine basis.	7.46	2.240	74.6	4
4.	There is an internal and external network connection with government agencies.	8.10	2.300	81.0	2
5.	The software tools needed to build and manage the digital transformation process are available.	7.16	2.043	71.6	5
6.	The Ministry updates all activities and information on the Ministry's website.	8.20	1.948	82.0	1
7.	There are clear mechanisms in the Ministry to ensure the continuity of providing electronic services in crises and emergencies.	7.75	1.963	77.5	3
Total Degree		**7.3044**	**1.82992**	**73.4**	

The following is evident from the previous table:

- The paragraph that states: The Ministry updates all activities and information first-hand on the Ministry's website. It got first place among the rest of the paragraphs with a relative weight of (82.0%), and this indicates a high degree of approval for this paragraph."
- The paragraph that states: The Ministry has high-speed internet lines and its services are available uninterrupted. It got the last ranking among the rest of the paragraphs with a relative weight of (59.3%). This indicates that there is a medium degree of approval for this paragraph."
- In general, "the relative weight of the dimension: the technical infrastructure required for digital transformation reached (73.4%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the importance of having an appropriate technical infrastructure that implements the digital transformation process and achieves its desired goals.

D. Paragraph analysis The Dimension: “Human Resources”:

Table 11: Analysis of Paragraphs: “The Dimension Human Resources”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	A sufficient number of qualified specialized personnel are available to develop the IT infrastructure.	6.89	2.169	68.9	6
2.	Consulting bodies and experts are used to provide advice in the field of implementing digital transformation.	7.28	2.107	72.8	4
3.	The Ministry's administration attaches importance to training employees and developing their capabilities in the field of Digital transformation.	7.33	2.127	73.3	3
4.	Most of the Ministry's employees have academic qualifications that enable them to deal with any digital transformation.	7.34	1.948	73.4	2
5.	Opportunities are available for all employees to learn digital transformation skills.	7.13	2.029	71.3	5

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
6.	The skills and qualifications of the occupants of job titles in computer and information technology departments/units are commensurate with the job requirements mentioned in the job description card.	7.82	1.478	78.2	1
7.	The number of workers in computer and information technology departments and units is commensurate with the volume and quality of work to bridge the gap between the required performance and the actual performance.	6.75	2.126	67.5	7
Total Degree		**7.2201**	**1.84475**	**72.2**	

The following is evident from the previous table:

- The paragraph that states: “The skills and qualifications of the occupants of job titles in computer and information technology departments / units are commensurate with the job requirements mentioned in the job description card” got the first rank among the rest of the paragraphs with a relative weight of (78.2%), and this indicates that there is A large degree of approval for this paragraph.
- The paragraph that states: “The number of workers in computer and information technology departments and units is commensurate with the size and quality of work to bridge the gap between the required performance and the actual performance” got the last rank among the rest of the paragraphs with a relative weight of (67.5%), and this indicates that there is a medium degree of Agree to this paragraph.
- In general, "the relative weight of the human resources dimension was (72.2%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the presence of a sufficient number of workers specialized in information technology and qualified in this field, which supports the process of Digital transformation.

E. Paragraph Analysis The Dimension: “Formatting”:

Table 12: Paragraph Analysis: “The Dimension Formatting”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The Ministry sets a clear methodology for exchanging data and information between the components of the Ministry.	7.87	2.125	78.7	4
2.	The Ministry's administration encourages cooperation between all security agencies.	8.46	2.102	84.6	2
3.	There are some joint projects between government agencies in Gaza Strip.	8.54	2.102	85.4	1
4.	The application of Digital transformation achieves a kind of transparency in the work of the ministry.	8.23	1.755	82.3	3
Total Degree		**8.2746**	**1.87456**	**82.7**	

The following is evident from the previous table:

- The paragraph that states: “There are some joint projects between government agencies in Gaza Strip” ranked first among the rest of the paragraphs with a relative weight of (85.4%), and this indicates that there is a very high degree of approval for this paragraph.
- The paragraph that states: "The Ministry establishes a clear methodology for exchanging data and information between the components of the Ministry" got the last ranking among the rest of the paragraphs with a relative weight of (78.7%), and this indicates that there is a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: coordination was (82.7%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the nature of work in the security institutions and the respect for work sequence and coordination between the various departments. This result agrees with a study....

F. Analysis Of The Paragraphs The Dimension: “Data Privacy And Security:

Table 13: Analysis of Paragraphs: “The Dimension Data Privacy and Security”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	Data security and privacy are among the biggest challenges facing the Ministry of Interior in digital transformation.	8.74	1.425	87.4	1

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
2.	Information security elements are available for uploaded data and files.	7.38	1.872	73.8	4
3.	Customers (citizens - employees - partner institutions) feel reassured about the privacy of their data.	7.67	1.886	76.7	3
4.	There is an information security policy approved by the Ministry.	8.51	1.885	85.1	2
Total Degree		**8.0738**	**1.50093**	**80.7**	

The following is evident from the previous table:

- The paragraph that states: “Data security and privacy is one of the biggest challenges facing the Ministry of Interior in digital transformation” ranked first among the rest of the paragraphs with a relative weight of (87.4%), and this indicates that there is a very high degree of approval for this paragraph. ".
- The paragraph that states: “Information security elements are available for the uploaded data and files” got the last ranking among the rest of the paragraphs with a relative weight of (73.8%), and this indicates a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: data privacy and security reached (80.7%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the great interest that the Ministry attaches to the security and privacy of data, especially as it relates to a government institution of a security nature.

G. Paragraph Analysis The Dimension: “Organizational Structure and Job Description:

Table 14: Analysis of Paragraphs: “The Dimension the Organizational Structure and Job Description”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The existence of an organizational structure in computer and information technology departments/units that includes subsections commensurate with the nature of work.	8.02	1.765	80.2	1
2.	The existence of a suitable placement for the private organizational structure in computer and information technology departments/units in the ministry.	7.92	1.926	79.2	2
3.	There is a clear and specific job description for the main tasks in the departments/units of computer and information technology in the ministry.	7.87	2.069	78.7	3
Total Degree		**7.9344**	**1.83668**	**79.3**	

The following is evident from the previous table:

- The paragraph that states: “The presence of an organizational structure in computer and information technology departments/units that includes subsections commensurate with the nature of the work” got the first rank among the rest of the paragraphs with a relative weight of (80.2%), and this indicates a high degree of approval on this paragraph".
- The paragraph that states: “There is a clear and specific job description for the main tasks in computer and information technology departments/units in the ministry.” It ranked last among the rest of the paragraphs with a relative weight of (78.7%), and this indicates a high degree of approval for this paragraph".
- In general, "the relative weight of the dimension: organizational structure and job description reached (79.3%), which indicates that this axis enjoys a high degree of approval.

The researchers attribute this to the presence of a clear and well-established organizational structure in security institutions, with a specific job description, which helps in the process of Digital transformation.

1. **Analyze The Dimensions Of Cyber Security:** The researchers used the appropriate descriptive tests: arithmetic means, standard deviations, relative weights, rankings for Cyber Security dimensions and the total score, then the researchers analyzed the data of each dimension of Cyber Security separately.

Table 15: Means, standard deviations, relative weights, and ranking for each axis of Cyber Security dimensions and the total score

#	The Dimension	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	Organizational Efforts	7.3410	1.89115	73.4	4
2.	Technical Efforts	7.4795	1.77030	74.8	2
3.	Threat Monitoring Efforts	7.3443	1.85470	73.4	4
4.	Rules And Regulations	7.4098	2.01806	74.1	3
5.	Privacy Protection	7.8443	1.58191	78.4	1
Total Degree		**7.4838**	**1.74337**	**74.8**	

It can be seen from the previous table that "the relative weight of the total score of the respondents' responses to the Cyber Security items came to a large degree and amounted to (74.8%), and the privacy protection dimension ranked first with a relative weight of (78.4%), while the technical efforts dimension came in the second rank with a relative weight of (74.8%). %), then after laws and legislations in the third rank with a relative weight of (74.1%), while after efforts to monitor threats and after organizational efforts came in the fourth and fifth rank with a relative weight of (73.4%).

The researchers attribute this to the interest of the Ministry of Interior in Cyber Security through the availability of all the necessary privacy protection for the data that the ministry deals with and the provision of appropriate technical efforts with the enactment of laws and legislation that protect the privacy of data and the monitoring of any threats that may occur to the data through the organizational efforts available in the ministry.

The following tables illustrate the analysis of each dimension of Cyber Security:

A. Paragraph Analysis After: “Organizational Efforts”:

Table 16: Analysis of paragraphs: “After Organizational Efforts”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	A clear strategy on cyber security is prepared and implemented.	7.46	1.954	74.6	2
2.	The Department of the Interior and Homeland Security develops computer systems periodically to improve cyber security.	7.41	2.077	74.1	3
3.	The Ministry of Interior and National Security follows up developments in everything related to protecting systems and networks.	7.48	1.920	74.8	1
4.	The Ministry of Interior and National Security provides a budget for improving the digital transformation system and activating and improving the Cyber Security system.	7.08	2.155	70.8	5
5.	The Ministry of Interior and National Security organizes specialized training courses related to the cyber security management system to improve skills.	7.28	1.881	72.8	4
Total Degree		**7.3410**	**1.89115**	**73.4**	

The following is evident from the previous table:

- The paragraph stating: The Ministry of Interior and National Security follows up on developments in everything related to the protection of systems and networks” ranked first among the rest of the paragraphs with a relative weight of (74.8%), and this indicates a high degree of approval for this paragraph.
- The paragraph that states: The Ministry of Interior and National Security provides a budget for improving the digital transformation system and activating and improving the Cyber Security system” got the last ranking among the rest of the paragraphs with a relative weight of (70.8%), and this indicates that there is a high degree of approval for this paragraph ".
- In general, "the relative weight of the dimension: organizational efforts reached (73.4%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the workers' feeling of satisfaction with the ministry's organizational efforts towards enhancing Cyber Security.

B. Paragraph Analysis After: "Technical Efforts":

Table 17: Paragraph Analysis: “After Technical Efforts”

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The Ministry of Interior and National Security uses a protection network capable of detecting all threats.	7.31	1.962	73.1	4
2.	The Ministry of Interior and National Security updates protection systems periodically to reduce crimes related to Cyber Security.	7.49	1.850	74.9	3
3.	Software to protect systems and networks is commensurate with the nature of the work in the ministry.	7.56	1.766	75.6	1
4.	The Ministry of Interior and National Security develops the database and protection systems related to security and protection on a regular basis.	7.56	1.812	75.6	1
Total Degree		**7.4795**	**1.77030**	**74.8**	

The following is evident from the previous table:

- The paragraph that states: Systems and network protection software is commensurate with the nature of the work in the ministry, and the paragraph "The Ministry of Interior and National Security develops the database and protection systems related to security and protection on a regular basis" ranked first among the rest of the paragraphs with a relative weight of (75.6%), This indicates that there is a large degree of approval for this paragraph."
- The paragraph stating: The Ministry of Interior and National Security uses a protection network capable of detecting all threats" got the last ranking among the rest of the paragraphs with a relative weight of (73.1%), and this indicates a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: technical efforts reached (74.8%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the workers' feeling that the ministry is making great technical efforts to implement cyber security by providing appropriate and advanced devices and software that protect data and prevent hacking.

C. Analysis Of Paragraphs After: "Efforts To Monitor Threats":

Table 18: Analysis of paragraphs: "After Efforts to Monitor Threats"

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	The Ministry of Interior and National Security develops the infrastructure in order to facilitate digital transformation and develop the Cyber Security management system.	7.49	1.955	74.9	1
2.	The information network used by the Ministry of Interior and National Security is able to reduce crimes related to the Department of Cyber Security.	7.43	1.901	74.3	2
3.	The Ministry of Interior and National Security uses all that is new in terms of protection systems.	7.31	2.029	73.1	3
4.	The Department of the Interior and Homeland Security cooperates with outside organizations to reduce penetration of network systems.	7.15	2.136	71.5	4
Total Degree		**7.3443**	**1.85470**	**73.4**	

The following is evident from the previous table:

- The paragraph that states: The Ministry of Interior and National Security develops the infrastructure in order to facilitate digital transformation and develop the Cyber Security management system." It ranks first among the rest of the paragraphs with a relative weight of (74.9%), and this indicates a high degree of approval for this paragraph. ".
- The paragraph that states: The Ministry of Interior and National Security cooperates with external institutions to limit penetration of network systems" got the last ranking among the rest of the paragraphs with a relative weight (71.5%), and this indicates that there is a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: Efforts to monitor threats was (73.4%), which indicates that this axis enjoys a high degree of approval."

The researchers attribute this to the Ministry's relentless endeavor to monitor the threats that the information system in the Ministry may be exposed to, as it contains sensitive and important parameters related to the Ministry's work.

D. Analysis Of The Paragraphs After: "Laws And Legislations":

Table 19: Analysis of paragraphs: "After Laws and Legislations"

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	There are laws and regulations at the Ministry of Interior and National Security that allow the improvement and development of Cyber Security management.	7.38	2.001	73.8	4
2.	There are legislations and regulations at the Ministry of Interior and National Security that facilitate the process of exchanging information regarding cyber security management with public and private sector institutions.	7.48	2.241	74.8	2
3.	There are specific instructions and laws on the basis of which citizens and institutions are directed.	7.57	1.945	75.7	1
4.	The current laws, legislation and regulations of the Ministry of Interior facilitate the management of cyber security.	7.41	2.124	74.1	3

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
5.	The laws and legislations of the Ministry of Interior are continuously developed in line with the development of cyber security.	7.21	2.222	72.1	5
Total Degree		**7.4098**	**2.01806**	**74.1**	

The following is evident from the previous table:

- The paragraph that states: There are specific laws and instructions on which citizens and institutions are directed." It got the first rank among the rest of the paragraphs with a relative weight of (75.7%), and this indicates a high degree of approval for this paragraph.
- The paragraph that states: The laws and legislations of the Ministry of the Interior are being developed continuously in line with the development of Cyber Security." It got the last ranking among the rest of the paragraphs with a relative weight of (72.1%), and this indicates that there is a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: laws and legislation was (74.1%), which indicates that this dimension enjoys a high degree of approval."

The researchers attribute this to the ministry's efforts to issue clear laws and regulations to help workers maintain the security of data and information in a way that prevents them from being hacked.

E. Analysis Of The Paragraphs After: "Privacy Protection":

Table 20: Analysis of Paragraphs: "After Privacy Protection"

#	Item	SMA	Standard Deviation	Relative Weight(%)	Rank
1.	Security gaps in the field of Cyber Security are due to the lack of experience of the public who benefit from the ministry's electronic services.	7.59	1.657	75.9	4
2.	The inclusion of scientific courses in schools and universities in the field of Cyber Security contributes to the reduction of electronic threats.	8.10	1.609	81.0	1
3.	Presenting programs through various media to enlighten the public about the most important developments in the field of information security protection.	7.90	1.777	79.0	2
4.	Review the programs used and the protection at the Ministry on an ongoing basis to ensure the required protection and fill security gaps	7.79	1.993	77.9	3
Total Degree		**7.8443**	**1.58191**	**78.4**	

The following is evident from the previous table:

- The paragraph "Including scientific courses in schools and universities in the field of Cyber Security contributes to reducing electronic threats" ranked first among the rest of the paragraphs with a relative weight of (81.0%), and this indicates a high degree of approval for this paragraph.
- The paragraph "Security gaps in the field of Cyber Security due to the lack of experience of the public who benefit from the Ministry's e-services" ranked last among the rest of the paragraphs with a relative weight of (75.9%), and this indicates a high degree of approval for this paragraph.
- In general, "the relative weight of the dimension: protection of privacy was (78.4%), which indicates that this dimension enjoys a high degree of approval."

The researchers attribute this to the ministry's endeavor to provide and protect privacy by providing a username and password for each user, while defining specific access rights to the system that cannot be bypassed.

Second: Testing the Study Hypotheses

Ho$_1$: There is a statistically significant relationship at the level of significance ($\alpha \leq 0.05$) between digital transformation and the application of Cyber Security in the Ministry of Interior in the southern governorates.

To test this hypothesis, a "Pearson correlation coefficient was established to study the relationship between digital transformation and the application of Cyber Security in the Ministry of Interior in the southern governorates. The results are shown in the following table:

Table 21: Correlation coefficient between "digital transformation and the application of Cyber Security"

Variable	Statement	Organizational Efforts	Technical Efforts	Threat Monitoring Efforts	Rules And Regulations	Privacy Protection	Cyber Security

Senior Management Support	Correlation Coefficient	.822	.709	.739	.818	.585	.775
	Probability Value	*0.000	*0.000	*0.000	*0.000	*0.000	*0.000
Strategic Directions	Correlation Coefficient	.893	.835	.850	.882	.741	.883
	Probability Value	*0.000	*0.000	*0.000	*0.000	*0.000	*0.000
Technical Infrastructure Needed For Digital Transformation	Correlation Coefficient	.920	.868	.882	.912	.794	.919
	Probability Value	*0.000	*0.000	*0.000	*0.000	*0.000	*0.000
Human Resources	Correlation Coefficient	.890	.862	.880	.895	.732	.896
	Probability Value	*0.000	*0.000	*0.000	*0.000	*0.000	*0.000
Coordination	Correlation Coefficient	.821	.823	.822	.842	.771	.855
	Probability Value	*0.000	*0.000	*0.000	*0.000	*0.000	*0.000
Data Privacy And Security	Correlation Coefficient	.846	.860	.855	.838	.812	.881
	Probability Value	*0.000	*0.000	*0.000	*0.000	*0.000	*0.000
Organizational Structure And Job Description	Correlation Coefficient	.929	.894	.893	.918	.817	.934
	Probability Value	*0.000	*0.000	*0.000	*0.000	*0.000	*0.000
Digital Transformation	Correlation Coefficient	.933	.893	.904	.931	.803	.937
	Probability Value	*0.000	*0.000	*0.000	*0.000	*0.000	*0.000

* The correlation is statistically significant at ($\alpha \leq 0.05$).

From the results shown in the previous table, it was found that "the probability value of the Pearson correlation coefficient is less than the significance level (0.05), and this indicates that: There is a correlation between digital transformation and the application of Cyber Security and its dimensions in the Ministry of Interior in the southern governorates," and thus the hypothesis can be accepted.The researchers attribute this to the fact that the application of Digital transformation necessarily requires data privacy and data protection from intrusion, penetration and tampering through the application of data cyber security.

Ho$_2$: There is a statistically significant effect at the level of significance ($\alpha \leq 0.05$) of the digital transformation in its dimensions on the application of Cyber Security in the Ministry of Interior and National Security in the governorates of Gaza.

The multiple regression model was used to test the impact of the independent variables "top management support, strategic directions, technical infrastructure needed for digital transformation, human resources, coordination, data privacy and security, organizational structure and job description" on the dependent variable "cyber security application", and to find an equation that connects between them.

Table 22: The effect of the independent variables on the dependent variable

Variable	**Coefficient Value**	**(T) Value**	**Probability Value**	**(F) Test Value Of The Model**	**R^2 Of The Model**
Fixed Amount	-.122-	-.294-	.770	*164.867	0.947
Organizational Structure Job Description	.414	2.983	.004		
Data Privacy And Security	.265	2.466	.017		
Technical Infrastructure Needed For Digital Transformation	.299	2.445	.018		

* The probability value is statistically significant at ($\alpha \leq 0.05$)

Through the previous table, the stepwise method was used to find the best equation for the multiple regression line. It was found that the dimensions of Digital transformation (organizational structure, job description, data privacy and security, technical infrastructure required for digital transformation), in order, have a substantial effect on (Cyber Security) according to the method. stepwise, where it was noted that the probability value is less than the significance level of 0.05, while it was noted that the axes (senior management support, strategic directions, human resources, coordination) do not affect (the application of Cyber Security) as the probability value of these axes is greater than 0.05.

The previous table shows "the value of (F-test), where it is noted that it is statistically significant, which indicates the explanatory power of the multiple linear regression model from a statistical point of view."

Also, the "determination coefficient (R²) is equal to 0.897, and this means that the following digital transformation dimensions (organizational structure, job description, data privacy and security, technical infrastructure required for digital transformation) explained 89.7% of the total variation in (Cyber Security application) and the rest is due to other factors The regression equation can be formulated in the following form:

$$Y = \alpha + \beta_1 X_1 + \beta_2 X_2 + \cdots + e$$

Cyber Security application = 0.122 - + (0.414 x organizational structure and job description) + (0.265 x data privacy and security + (0.299 x technical infrastructure needed for digital transformation)

The researchers attribute this to the critical importance of implementing digital transformation

Conclusions

The following Results and recommendations were reached:

1. **Results Related To The Study Variables:**

    A. **Results Related To The Independent Variable (Digital Transformation):**

- The results of the study showed that there is a significant application of Digital transformation in the Ministry of Interior and National Security, and its value reached (77.5%).
- The results of the study showed that the support of senior management received a high degree of approval with a relative weight of (78.2%).
- The results of the study indicated that the strategic directions dimension received a high degree of approval with a relative weight of (76.3%).
- The results of the study indicated that the technical infrastructure dimension needed for digital transformation received a high degree of approval with a relative weight of (73.4%).
- The results of the study indicated that the human resources dimension had a high approval rating with a relative weight of (72.2%).
- The results of the study indicated that the coordination dimension received a high approval rating with a relative weight of (82.7%).
- The results of the study indicated that the dimension of data privacy and security received a high approval rating with a relative weight of (80.7%).
- The results of the study indicated that the organizational structure and job description dimension received a high approval rating with a relative weight of (79.3%).

    B. **Results Related To The Dependent Variable (Cyber Security):**

- The results of the study showed that there was a high degree of agreement on the degree of cyber security application, which amounted to (74.8%).
- The results of the study showed that the organizational efforts dimension received a high approval rating with a relative weight of (73.4%).
- The results of the study indicated that the technical efforts dimension received a high approval rating with a relative weight of (74.8%).
- The results of the study indicated that the threat monitoring dimension received a high degree of approval with a relative weight of (73.4%).
- The results of the study indicated that the dimension of laws and legislations received a high approval rating with a relative weight of (74.1%).
- The results of the study indicated that the privacy protection dimension received a high approval rating with a relative weight of (78.4%).

2. Results Related To Hypothesis Testing:

A. Results Related To The First Main Hypothesis And Its Sub-Hypotheses:

The results of the study showed that there is a statistically significant correlation between all dimensions of Digital transformation and the application of Cyber Security in the Ministry of Interior and National Security.

B. Results Related To The Second Main Hypothesis:

- The results of the study showed that there is an impact of Digital transformation on the application of security in the Ministry of Interior and National Security in the governorates of Gaza, and the impact coefficient was (0.897).
- It was found that the dimensions affecting the dependent variable of Cyber Security are dimensions (organizational structure, job description, data privacy and security, technical infrastructure required for digital transformation), as these dimensions affect (89.7%) of the variation in the application of Cyber Security.

Recommendations

Recommendations Related To The Independent Variable (Digital Transformation):

- The need for the Ministry's administration to provide a special budget to develop the quality of its electronic services as a lever for digital transformation.
- The Ministry's administration should spend sufficient amounts of money on innovation in how to provide its services.
- The Ministry provides high-speed internet lines and its services are available without interruption.
- The need for the number of workers in computer and information technology departments and units to be commensurate with the volume and quality of work to bridge the gap between the required performance and the actual performance.
- The ministry should develop a clear methodology for exchanging data and information between the components of the ministry.
- A Information security elements are available for the uploaded data and files.
- The Ministry provides a clear and specific job description for the main tasks in computer and information technology departments/units in the Ministry.

Recommendations Related To The Dependent Variable (Cyber Security):

- Interest in providing the Ministry of Interior and National Security with a budget in order to improve the digital transformation system and activate and improve the Cyber Security system.
- The Ministry of Interior and National Security should use a protection network capable of detecting all threats.
- The cooperation of the Ministry of Interior and National Security with external institutions to reduce penetration of network systems.
- Enhancing and developing the laws and legislations of the Ministry of Interior continuously in line with the development of cyber security.
- Enhancing the experiences of the public beneficiaries of the Ministry's e-services to reduce security gaps in the field of cyber security.

Acknowledgment

The authors extend their sincere thanks and appreciation to all who enriched the current study with valuable information, without which the study would not have appeared in its present elegant form.

References

[1]Abdalmenem, S. A., et al. (2019). "Relationship between e-Learning Strategies and Educational Performance Efficiency in Universities from Senior Management Point of View." International Journal of Academic Information Systems Research (IJAISR) 3(6): 1-7.

[2]Abu Amuna, Y. M., et al. (2017). "Strategic Environmental Scanning: an Approach for Crises Management." International Journal of Information Technology and Electrical Engineering 6(3): 28-34.

[3]Abu Amuna, Y. M., et al. (2017). "The Reality of Electronic Human Resources Management in Palestinian Universities-Gaza Strip." International Journal of Engineering and Information Systems (IJEAIS) 1(3): 37-57.

[4]Abu Naser, S. S. and M. J. Al Shobaki (2017). "The Impact of Senior Management Support in the Success of the e-DMS." International Journal of Engineering and Information Systems (IJEAIS) 1(4): 47-63.

[5]Abu Naser, S. S., et al. (2017). "The Reality of Electronic Human Resources Management in Palestinian Universities from the Perspective of the Staff in IT Centers." International Journal of Engineering and Information Systems (IJEAIS) 1(2): 74-96.

[6]Abu-Nahel, Z. O., et al. (2020). "Quality of Services and Its Role in Enhancing Strategic Flexibility in Non-Governmental Hospitals." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(10): 38-56.

[7]Abu-Nahel, Z. O., et al. (2020). "Strategic Flexibility and Its Relationship to the Level of Quality of Services Provided in Non-Governmental Hospitals." International Journal of Academic Multidisciplinary Research (IJAMR) 4(10): 57-84.

[8]Abu-Nahel, Z. O., et al. (2020). "The Reality of Applying Strategic Flexibility in Non-Governmental Hospitals." International Journal of Academic Management Science Research (IJAMSR) 4(7): 144-170.

[9]Abusharekh, N. H., et al. (2020). "The Impact of Modern Strategic Planning on Smart Infrastructure in Universities." International Journal of Academic Management Science Research (IJAMSR) 4(8): 146-157.

[10]Al Najjar, Mahmoud T., Al Shobaki, Mazen J. and El Talla, Suliman A. (2022). The Reality of Digital Transformation in the Palestinian Ministry of Interior and National Security, International Journal of Academic Management Science Research (IJAMSR), 6(11), 1-1

[11]Al Najjar, Mahmoud T., Al Shobaki, Mazen J. and El Talla, Suliman A. (2022). The Extent of Cyber Security Application at the Ministry Of Interior and National Security in Palestine, International Journal of Academic Information Systems Research (IJAISR), 6 (11), 1-1

[12]Al Shobaki, M. J. and S. S. Abu Naser (2016). "Decision support systems and its role in developing the universities strategic management: Islamic university in Gaza as a case study." International Journal of Advanced Research and Development 1(10): 33-47.

[13]Al Shobaki, M. J., et al. (2016). "The impact of top management support for strategic planning on crisis management: Case study on UNRWA-Gaza Strip." International Journal of Academic Research and Development 1(10): 20-25.

[14]Al Shobaki, M. J., et al. (2016). The Impact of the Strategic Orientations on Crisis Management Agency, International Relief in Gaza. First Scientific Conference for Community Development, 5-6 November, Faculty of Economics and Administrative Sciences Al-Azhar University of Gaza.

[15]Al Shobaki, M. J., et al. (2017). "Impact of Electronic Human Resources Management on the Development of Electronic Educational Services in the Universities." International Journal of Engineering and Information Systems 1(1): 1-19.

[16]Al Shobaki, M. J., et al. (2017). "Strategic and Operational Planning As Approach for Crises Management Field Study on UNRWA." International Journal of Information Technology and Electrical Engineering 5(6): 43-47.

[17]Al Shobaki, M. J., et al. (2017). "The Reality of the Application of Electronic Document Management System in Governmental Institutions-an Empirical Study on the Palestinian Pension Agency." International Journal of Engineering and Information Systems 1(2): 1-14.

[18]Al Shobaki, M. J., et al. (2018). "Availability of Crowdfunding Elements among Palestinian University Students." International Journal of Academic Management Science Research (IJAMSR) 2(2): 1-15.

[19]Al Shobaki, M. J., et al. (2018). "Support Extent Provided by Universities Senior Management in Assisting the Transition to e-Management." International Journal of Academic Management Science Research (IJAMSR) 2(5): 1-26.

[20]Al Shobaki, M. J., et al. (2018). "The Entrepreneurial Creativity Reality among Palestinian Universities Students." International Journal of Academic Management Science Research (IJAMSR) 2(3): 1-13.

[21]Al Shobaki, M. J., et al. (2018). "The Extent to Which Technical Colleges Are Committed To Applying Lean Management." International Journal of Engineering and Information Systems (IJEAIS) 2(1): 23-42.

[22]Al Shobaki, M. J., et al. (2019). "The Role of Human Resources in Interpreting the Relation between the Emphases on the Operations Standard and Improving the Overall Performance of the Palestinian Universities." International Journal of Academic Management Science Research (IJAMSR) 3(5): 60-75.

[23]Al Shobaki, M. J., et al. (2020). "Digital Repositories and Their Relationship to the Modern Strategic Planning of the Universities' Smart Infrastructure." International Journal of Academic Information Systems Research (IJAISR) 4(9): 1-18.

[24]Al Shobaki, M. J., et al. (2020). "Digital Reputation in the University Of Palestine: An Analytical Perspective of Employees' Point Of View." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(9): 22-37.

[25]Al Shobaki, M. J., et al. (2020). "Measuring the E-Content of the Digital Repositories in the University of Palestine." International Journal of Academic Information Systems Research (IJAISR) 4(10): 34-50.

[26]Al Shobaki, M. J., et al. (2020). "The Reality of Using Digital Repositories at the University of Palestine." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(8): 115-134.

[27]Alayoubi, M. M., et al. (2020). "Requirements for Applying the Strategic Entrepreneurship as an Entry Point to Enhance Technical Innovation: Case Study-Palestine Technical College-Deir al-Balah." International Journal of Business and Management Invention (IJBMI) 9(3): 1-17.

[28]Alayoubi, M. M., et al. (2020). "Strategic Leadership Practices and their Relationship to Improving the Quality of Educational Service in Palestinian Universities." International Journal of Business Marketing and Management (IJBMM) 5(3): 11-26.

[29]Almasri, A., et al. (2018). "The Organizational Structure and its Role in Applying the Information Technology Used In the Palestinian Universities-Comparative Study between Al-Azhar and the Islamic Universities." International Journal of Academic and Applied Research (IJAAR) 2(6): 1-22.

[30]Arqawi, S. M., et al. (2019). "Strategic Orientation and Its Relation to the Development of the Pharmaceutical Industry for Companies Operating in the Field of Medicine in Palestine." International Journal of Academic Management Science Research (IJAMSR) 3(1): 61-70.

[31]El Talla, S. A., et al. (2018). "Organizational Structure and its Relation to the Prevailing Pattern of Communication in Palestinian Universities." International Journal of Engineering and Information Systems (IJEAIS) 2(5): 22-43.

[32]El Talla, S. A., et al. (2018). "The Availability of the Focus Standards on Human Resources and Processes as a Potential for Excellence in Palestinian Universities According to the European Model." International Journal of Academic Management Science Research (IJAMSR) 2(11): 58-69.

[33]El Talla, S. A., et al. (2018). "The Nature of the Organizational Structure in the Palestinian Governmental Universities-Al-Aqsa University as A Model." International Journal of Academic Multidisciplinary Research (IJAMR) 2(5): 15-31.

[34]El Talla, S. A., et al. (2019). "Intermediate Role of the Focus Standard on Human Resources in the Relationship between Adopting the Criterion of Leadership and Achieving Job Satisfaction in the Palestinian Universities." International Journal of Academic Management Science Research (IJAMSR) 3(3): 48-60.

[35]FarajAllah, A. M., et al. (2018). "The Reality of Adopting the Strategic Orientation in the Palestinian Industrial Companies." International Journal of Academic Management Science Research (IJAMSR) 2(9): 50-60.

[36]Hamdan, M. K., et al. (2020). "Strategic Sensitivity and Its Impact on Boosting the Creative Behavior of Palestinian NGOs." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(5): 80-102.

[37]Hamdan, M. K., et al. (2020). "The Effect of Choosing Strategic Goals and Core Capabilities on the Creative Behavior of Organizations." International Journal of Academic Information Systems Research (IJAISR) 4(4): 56-75.

[38]Hamdan, M. K., et al. (2020). "The Reality of Applying Strategic Agility in Palestinian NGOs." International Journal of Academic Multidisciplinary Research (IJAMR) 4(4): 76-103.

[39]Keshta, M. S., et al. (2020). "Perceived Organizational Reputation and Its Impact on Achieving Strategic Innovation." International Journal of Academic Information Systems Research (IJAISR) 4(6): 34-60.

[40]Keshta, M. S., et al. (2020). "Strategic Creativity and Influence in Enhancing the Perceived Organizational Reputation in Islamic Banks." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(7): 13-33.

[41]Keshta, M. S., et al. (2020). "Strategic Creativity in Islamic Banks in Palestine between Reality and Implementation." International Journal of Academic Accounting, Finance & Management Research (IJAAFMR) 4(3): 79-98.

[42]Madi, S. A., et al. (2018). "The Organizational Structure and its Impact on the Pattern of Leadership in Palestinian Universities." International Journal of Academic Management Science Research (IJAMSR) 2(6): 1-26.

[43]Kennedy, C., (2017). The internet of things: The cyber security risks and how to protect against them.

[44]Kuzu. Omur Hakan (2020): Digital Transformation in Higher Education – A case Study on Strategic Plans. Higher Education in Russia.29 (3). 923.

[45]Lanzolla, G., Lorenz, A., Spektor, E. M., Schilling, M., Solinas, G., & Tucci, Ch. (2018). Academy of Management Discoveries (AMD) SPECIAL ISSUE – CALL FOR PAPERS "Digital Transformation: What Is New If Anything?" Academy of Management Discoveries, 4 (3), 378–38.

[46]Loudon, C, & Laudon P. (2017). Management information system. Managing the Digithl form. (14th Edition). Pearson.

[47]Catota. Frankie. Morgan. Granger. & Sicker Douglasmar. (2019): Cyber Security education in developing nation: the Ecuadorian environment. Journal of CYBER SECURITY. 119

[48] Maranga Mayieka. & Nelson Masese (2019): Emerging Issues in- Cyber Security for Initiutions of Higher Education. International Journal of Computer Science & Network. 8(4). August 2019.2277-5420.

[49]Menesini. Ersilia & Nocentini. Annalaura (2009): Cyber bullying Definition and Measurement- Some Critical Considerations Zeitschrift fur psychologue. 217(4).

[50]Moskal, E. (2020). A model for establishing a cyber-security center of excellence. Information systems education journal. 13 (6), 97- 108

[51]Nathanael J. Fast. Yeri Cho (2012): Power defensive denigration and the assuaging effect of gratitude expression. Journal of Experimental Social Psychology. 48(3). 778 – 782

[52]Ninkeu, N., Anye, D., Kwededu, L. & Buttler, W. (2018). Cyber education outside the cyber space: the Case of catholic university institute of Buea. International journal of technology in teaching and learning. 14 (2), 90-101.

[53]R, S. (2011). Cloud computing effect on enterprises in terms of Cost and Security. London: LUND UNIVERSITY.

[54]Richardson. M... Lemoine. P... Stephens W... & Waller. R. (2020). Planning for Cyber Security in Schools -The Human Factor. Educational planning.27 (2). 23-39.

[55]Tiwari. Soumya. Bhalla. Anshika. & Rawat. Ritu (2016): Cyber- Crime and Security. International Journal of advanced research in Computer Science and Software engineering. 6(4). 46- 52

[56]Vayansky. Ike & Kumar SathishA.p (2018): phishing – Challenges and Solutions. Computer Fraud & Security. (1). 15- 20.

Arabic References in Roman Scripts:

[1]Abdullah, Nawal (2019). Digital transformation in the Sultanate of Oman and the factors affecting it from the point of view of decision makers in the Sultanate of Aan. Sultan Qaboos university. Muscat.

[2]Abu Al-Hasani, Abdullah Mansour (2017). The role of organizational and functional factors in the successful management of NGO projects in Gaza Strip. (Unpublished master's thesis) The Islamic University, Gaza.

[3]Al-Arishi, Jibril, Al-Dosari, Salma (2018). The role of higher education institutions in promoting a culture of Cyber Security in society. King Fahd National Library Journal. Riyadh. (24)2.

[4]Al-Assaf, Saleh bin Hamad. (2000). Handbook for Researchers in the Behavioral Sciences. Riyadh: Obeikan Library.

[5]Al-Bahi, Raghda. (2017). Cyber deterrence concept, problems and requirements. Journal of Political Science. . https://democraticac.de

[6]Al-Balochi Nawal Bint Ali, Al Harasi Nabhan Bin Harith, Al Awfi Ali Bin Saif. 2020. The Reality of Digital transformation in Omani institutions. Sultan Qaboos University Journal - Oman - Fourth Edition - March - 2020. Oman.

[7]Al-Halabi, Mahmoud, Abu Odeh Saleh, Al-Hayek Omar, (2022). Transformational leadership and its role in managing digital transformation at the Ministry of Interior and National Security. Gaza, Palestine.

[8]Al-Janabi, Lily (2017). The effectiveness of national and international laws in combating cybercrime, research published on https://www.ssrcaw.org on 5/9/2017.

[9]Al-Jifnawi, Khaled. (2021). Digital transformation of national institutions and Cyber Security challenges from the point of view of academic police officers in Kuwait. Arab Journal of Arts and Humanities, Arab Foundation for Education, Science and Arts. Volume (5). Issue 19, pg. 75.

[10]Al-Jundi, Alia, Hassan, Nahair Taha (2019). The role of the applied practice of Cyber Security in developing the skills and accuracy of the practical application of information security among university students, Journal of the World of Education. Cairo. The Arab Foundation for Scientific Consultation and Human Resources Development. (67) 3. pp. 14-84.

[11]Al-Manthari, Fatima Yousef (2020) The role of school leadership in enhancing Cyber Security in government schools for girls in Jeddah from the point of view of female teachers, The Arab Journal of Educational and Psychological Sciences, (17) July 4. 48-95, 2020

[12]Al-Manthari, Fatima Youssef, and Hariri, Randa (2020) The degree of awareness of middle school teachers about Cyber Security in public schools in Jeddah from the point of view of female teachers, The Arab Journal for Specific Education, (13), 4 July 2020.

[13]Al-Qahtani, Noura Nasser (2019). The availability of cyber security awareness among male and female Saudi university students from a social perspective. Social Affairs Journal. Sharjah. (36) 144, pp. 85-120.

[14]Al-Sanea, Nora, Suleiman, Enas, Asran, Awatef, Al-Sawat, Hamad, Abu-Aisha, Zahda (2020). Teachers' awareness of Cyber Security and methods of protecting students from the dangers of the Internet and promoting their national values and identity. Journal of the Faculty of Education in Assiut. (26) 6, 41-90.

[15]Al-Shoubri, Noha Muhammad (2020). Analytical visions of the possibility of applying digital transformation in non-governmental organizations, "a study from the perspective of how society is organized." Journal of the Faculty of Social Work for Social Studies and Research, Faculty of Social Work, Fayoum University. Issue eighteen. 2020, pg. 716.

[16]Al-Wakil, Sami (2017). Cyber Security is a national protection for the security of the individual and society in the Kingdom of Saudi Arabia. Research published on 10/1/2017. https://www.spa.gov.sa.

[17]Bahour, Khaled (2016). The availability of factors affecting the adoption and application of cloud computing in government institutions from the point of view of senior management. (Unpublished master's thesis) The Islamic University, Gaza.

[18]Faraj, Alia (2021). The reasons for enhancing the culture of Cyber Security in light of the digital transformation - Prince Sattam bin Abdulaziz University as a model. Sohag University. Faculty of Education. Part (1).

[19]Hajjaj, Ibrahim (2021). The role of some emerging crises in promoting digital transformation as a mechanism for achieving development goals in civil organizations in contemporary society. Al-Azhar University Journal of Social Sciences. Issue 27, June 2021.

[20]Information and Decision Support Center (2020). The Most Important Cyber Security Breakthroughs for 2020 Cabinet, Arab Republic of Egypt, December 2020

[21]Jarbou, Haitham (2018) Availability of factors influencing the success of re-engineering administrative processes, a case study of the Palestine Red Crescent Society, Gaza. Islamic University of Gaza.

[22]Madi, Khalil, Abu Hajeer, Tareq Mufleh (2020). The readiness of Palestinian private universities towards digital transformation. The First International Conference on Information Technology ICITB. Gaza. Palestine.

[23]Qari, Reem Abdel-Rahim and Al-Sani, Reem Alawi and Allam, Nouf Khaled (2019). Keys to Cyber Security in Education, Jeddah.

[24]http://www.moi.gov.ps