The Role Of Cybersecurity Awareness in the Era Of Digital Transformation

دور التوعية حول الأمن السيبراني في عصر التحول الرقمي

[1]-MOUISSI Maroua * [2]- Abdellatif Messaitfa [2], [3]-Nader Mahmoud Fawaz

[1]- University of Ghardaia, Ghardaia (Algeria), mouissi.maroua@univ-ghardaia.edu.dz

[2]- University of Ghardaia, Ghardaia (Algeria), Messaitfa.abdellatif@univ-ghardaia.edu.dz

[3] -University of tanta (Egypt), PG8_166429@commerce.tanta.edu.eg

Received: 30/07 /2025 **Accepted**: 18/11 /2025 **Published**: 15/12 /*2025*

Abstract:

With the development of technologies, institutions must move towards implementing cyber security. If it is exploited in a positive way, it affects the performance of these institutions. Our study aims to clarify the concepts of cyber security and seeks to raise awareness by knowing its importance and reality in institutions in light of the digital transformation by investigating the views of a sample of Algerian society using a questionnaire tool, through the Statistical Package for Social Sciences (SPSS) program and using appropriate statistical methods. After analyzing the outputs, we concluded that there is a strong statistically significant relationship at a significance level of 0.05 between the opinions of sample members about the perception of the dimensions of cyber security and its reality attributed to demographic variables.

Keywords Knowledge, Cybercrime, Artificial Intelligence, Safety, Protection, Cyber security.

- Résumé:

Avec le développement des technologies, les institutions doivent s'orienter vers la mise en œuvre de la cyber sécurité. Si elle est exploitée de manière positive, elle affecte la

* المؤلف(ة) المرسل(ة): مروة مويسي، الإيميل: mouissi.maroua@univ-ghardaia.edu.dz

performance de ces institutions. Notre étude vise à clarifier les concepts de la cyber sécurité et à sensibiliser le public en connaissant son importance et sa réalité au sein des institutions à la lumière de la transformation numérique. Elle s'appuie sur l'analyse des opinions d'un échantillon de la société algérienne à l'aide d'un questionnaire, du logiciel SPSS (Statistiques Package for Social Sciences) et de méthodes statistiques appropriées. Après analyse des résultats, nous avons conclu à l'existence d'une forte relation statistiquement significative (seuil de signification de 0,05) entre les opinions des membres de l'échantillon sur la perception des dimensions de la cyber sécurité et sa réalité attribuée à des variables démographiques.

Mots clés : Connaissance, cybercriminalité, intelligence artificielle, sécurité, protection, cyber sécurité.

الملخص:

مع تطوّر التِقنيّات، على المُؤسسات التوّجُهُ نحو تطبيق الأمّن السيبرانيcyber Securityإذْا ما تمّ استغلاله بطريقةٍ إيجابيةٍ يُؤثر على أداء تِلك المُؤسسات، تهْدِف دراستنا لِتَوضِيح مفاهيم الأمّن السيبراني كما تسعى إلى التوعية من خلال معرفة أهميّته و واقعه بِالمُؤسسات في ظل التحول الرقمي عن طريق تقصيّ وُجهات نَظر عيّنة للمُجتمع الجزائري باستخدام أداة الإستبيان، بِواسِطة بَرْنَامَجِ الحُزم الإحصائية للعلوم الإجتماعية spss وبِاستعمال الأساليب الإحصائية المُناسبة، و بعد تحليل المُخرجات، تَوّصلنا إلى أنّ هُناك علاقة ذات دلالة إحصائية قويّة عِند مُستوى معنويّة 0.05 بيّن آراء أفراد العيّنة حول إدراك أبعاد الأمّن السيبراني مع واقعه يُعزى لمُتغيرات الديمغرافيّة.

الكلمات المفتاحية: معرفة، جرائم إلكترونية، ذكاء اصطناعي، سلامة، حماية، أمن سيبراني.

- Introduction:

Both individuals and institutions rely heavily on information and communication technologies. As some departments transition to digitalization, cyber security offers better defense against online threats. In addition to safeguarding people from dangers and threats, it also involves making sure that all types of devices smart, computer, and networks are safe by utilizing antivirus software and protection programs. Cyber security is defined as "the ability of the information system to resist hacking attempts targeting data" in the European Declaration, and according to the American National Institute of Standards and Technology, "it provides protection from damage, the restoration of computer systems and electronic and wired communications services.

Research question: How well-informed are the participants in the study about the aspects of cyber security?

Research inquiries:

- ✓ Is there an effect on addressing the difficulties of cyber security?
- ✓ To what extent does cyber security actually exist in Algerian institutions?
- ✓ Describe the significance of cyber security and the challenges associated with its implementation ?

Study hypotheses:

H0 At a significance level of 0.05, there is no statistically significant correlation between the study sample's participants' perceptions of the reality of cyber security as it is perceived in Algerian institutions based on the variables (gender, age, educational background, experience, and current employment).

H1 At a significance level of 0.05, there is a statistically significant correlation between the study sample's participants' perceptions of the reality of cyber security in Algerian institutions based on its dimensions and the variables (gender, age, educational background, work experience, and current employment).

The purpose and significance of the research:

- ✓ Filling up the research gap by providing definitions for the key terminology in cyber security.
- ✓ Emphasizing the advantages of utilizing cyber security.
- ✓ Understanding the opinions of the research sample regarding the level of knowledge regarding the various facets and dimensions of cyber security.
- ✓ The reality of cyber security in Algerian institutions is examined.

Study Methodology: In the theoretical section, we employed the deductive technique, whose instrument is description and analysis, to describe the numerous concepts that govern the research variable's operation in order to comprehend the study's elements. We used the inductive approach to examine SPSS outputs and offer an interpretation of the findings in order to apply the study's circumstances to the applicable portion.

1- First Title: Learn the following terms:

Cybercrime: The Algerian lawmaker has taken notice of it, particularly in light of the increase in security data indicating the proliferation of this kind. He enacted legislation to deter crimes involving information and communication technology (TIC). However, the texts provided room for judicial adaptation rather than categorizing cybercrimes. Therefore, in contrast to the European Convention on Cybercrime, which mentioned crimes like insulting and cursing and required the judicial police to intervene whenever they occur using information and communication technologies, all crimes under the Penal Code committed through these technologies are classified as cybercrimes. Due to its widespread distribution on the Internet, this is still not feasible, despite data indicating that many. (ALACHACH, 2018, p. 186 _187)

Artificial Intelligence: Through this area of computer science, computer programs that mimic human intelligence can be developed and designed to enable the computer to carry out certain tasks in place of a human that call for rational, well-organized thought, understanding, hearing, speaking, and movement. The term's origins can be traced to the shift from conventional programming systems following World War II to computer programs that mimicked human intelligence by utilizing the developer's acquired expertise in a particular field, comprehension of various languages, image recognition, and speech. This resulted in the development of methods for creating programs that turn computers into artificially intelligent machines or carry out tasks. (KADIM, 2012, p. 98)

2- Second Title: Earlier research:

First study: Houria Ben Sidhom, Rokia Awashria (2020) entitled: Cyberspace Security (Challenges and Solutions), Algerian Journal of Human Security at the University, Volume 05, Issue 02, The study's goal is to draw attention to the national and international initiatives, whether they involve institutional or legal measures, to address the threats to cyber security. According to the study's findings, cybercrimes have catastrophic social and economic repercussions, and everyone has a responsibility to defend cyberspace security, which calls for international cooperation.

The second study: Samir Bara (2017) entitled: Cyber security in Algeria Policies and Institutions, Algerian Journal of Human Security, Volume 04, Issue 04, Given the existing and upcoming national and international difficulties posed by cyberspace, the study examined the role of national defense in achieving cyber security in Algeria. In order to ensure that the plan is integrated and consistent with what those concerned with the security of the information society can be expected to commit to, the study recommends the following: Develop a strategy to spread and build awareness among various segments of society, whether they are professionals, decision-makers, or ordinary users; and take into account all aspects of cyber security when developing any strategy or policy, including the needs of citizens and institutions as well as their rights and duties.

3- third Title: Research methodology:

3.1- The nature of cyber security: A combination of the terms "security" and "cyber."

In terms of language, security is safety and security and is the opposite of fear.

The Penguin Dictionary of International Relations defined it as a term that refers to the absence of what threatens rare values.

The word security is mentioned in the Holy Quran in several Surahs: Al-Baqarah, Al-Imran, An-Nisa, Al-An'am, and Al-Qasas.

God says in Surat AL-Nahl بسم الله الرحمن الرحيم ﴿وَضَرَبَ اللَّهُ مَثَلًا قَرْيَةً كَانَتْ آمِنَةً مُطْمَئِنَّةً يَأْتِيهَا
رِزْقُهَا رَغَدًا مِنْ كُلِّ مَكَانٍ فَكَفَرَتْ بِأَنْعُمِ اللَّهِ فَأَذَاقَهَا اللَّهُ لِبَاسَ الْجُوعِ وَالْخَوْفِ بِمَا كَانُوا يَصْنَعُونَ﴾
الآية 112.صدق الله العظيم

The Messenger of God says { مَّنْ أَصْبَحَ مِنْكُم آمِنًا فِيّ سِرْبِهِ مُعَافى فِيّ جَسَدِهِ عِنْدَهُ قُوتُ يَومِهِ فَكَأنمّا
حُيِزَتْ لَهُ الدُنْيا بحِذَافِيرِهَا} صدق رسول الله صلى الله عليه وسلم رواه الترمذي.

There have been numerous references to the word security. Security refers to both physical and psychological comfort, and it encompasses both societal and personal security. (AL_TORKI , 2021)

Among the most commonly used terms nowadays, "cyber" is also the one that appears the most frequently in the international security lexicon. The Greek word for direction and control, Cybernetic, is where the word "cyber" originates. (MOHAMED ABDEBASET AYOUB , 2020) The term "governor" was used by American mathematician Norbert Wieners (1894–1964) to refer to the person in charge of steering the ship. Through his well-known work Cybernetics or Control and Communication in the Animal and the Machine, he is regarded as the founding spiritual father of cybernetics. According to his book, cybernetics is the study of control and communication in humans, machines, and animals; as a result, the term "machine" was substituted with "computer" following World War.

Cyber security as defined by Edward Amorso: "Means of reducing the risk of attack on software, computers or networks, including tools used to combat hacking, detect and stop viruses, and provide encrypted communications."

In the 2010–2011 International Telecommunication Union report on trends in telecommunications reform, cyber security was described as "a set of tasks such as the collection of security tools, policies, procedures, guidelines, approaches to risk management, training, and techniques that can be used to protect the cyber environment and the assets of institutions and users."

Cyber security is precisely defined by the US Department of Defense's "Pentagon" as "All organizational measures necessary to ensure the protection of information in all its physical and electronic forms, from various crimes, attacks, hijacking, spying, and accidents." (Cyber Security, 2022)

3-2- The significance of cyber security (ALHIARY , 2019) :

- ✓ Providing exceptional privacy and confidentiality protection for information and preventing unauthorized individuals from accessing or using it.
- ✓ Reaching data readiness and plenty as required.
- ✓ As a safeguard for data and information, devices and networks should be protected from breaches.
- ✓ Finding weaknesses and vulnerabilities in systems and fixing them.
- ✓ To implement cyber security principles, open source technologies are being developed and used.

3-3- Cyber threat types:

Theft of credit card numbers, bank account information, or personal identity numbers are examples of confidentiality attacks. After stealing the data, many attackers sell it on the Dark Web for others to purchase and use unlawfully.

Attacks on Integrity: These include institutional or personal sabotage, often known as leaks, in which a cybercriminal obtains private data and then makes it public with the intention of exposing it and making the public lose faith in that organization or individual.

The purpose of availability attacks is to keep users from accessing their personal information unless they pay a fee or a certain ransom.

3-4- The process of achieving cyber security:

Reliability: When supplying personal information, only use websites you can trust. The fundamental guideline is to verify the URL address. It indicates that the website is secure if it starts with https. But if the URL address starts with http instead of s, don't enter any personal data like your social security number or credit card number.

Scam Email: Emails posing as correspondence from someone you trust are the most frequent way that people are robbed or compromised.

Updates (Always current): Ensure that your gadgets are up to date. Successful hacker assaults are mostly directed at older devices since they lack the most recent security software, and software upgrades frequently include crucial patches to address security flaws.

Backup: Creating frequent backup copies of your data also helps to keep your contents in a secure location and facilitates the process of formatting your device following a previous cyber attack.

3-5- Cyber security advantages: (ATTALAH, 2020)

Business Protection: Since it lets workers access the Internet whenever they want without worrying about getting caught in a network of possible threats, it is the greatest option for organizations looking for complete digital protection.

Protecting personal data: In the digital age, personal data is the most crucial thing. A virus can manipulate, sell, or even steal money from businesses and employees if it manages to get hold of personal information belonging to consumers or employees.

Maintaining Productivity and Working Safely: Any time a cyber attack could occur, the organization's gadgets could be vulnerable. Any type of virus infection will cause the computer systems to operate more slowly or even stop altogether, which reduces productivity and results in time wasted. The administrator will then have to replace the equipment. All of this hassle and anxiety about hacking and business disruption is avoided with the help of cyber security.

Website security: is the protection of the business owner who runs the company. If the information system is compromised by a virus or something similar, the owner may have to shut down the website, lose money from transactions he can't reply to, and lose the trust of his clients.

Blocking Spyware : is a type of cybercrime in which a cybercriminal creates a program to spy on computer activities and send data to the computer. The best course of action in this case is cyber security. For example, Fortine's FortiGate Firewall keeps data private and stops spyware from getting inside and influencing it.

Adware is a type of computer infection that clogs your computer with advertisements, which reduces productivity and can let other viruses in if you click on them by mistake.

Assistance from the IT specialist at your company: Since most cybercriminals have greater experience with cybercrime than the typical employee, IT security aids the technical staff in combating any cybercriminals.

Building Customer Trust: A company that is successfully safeguarded against all forms of cyber attacks will encourage customers to have faith in it and be happy with the things they buy.

4- Results Analysis:

where we created a survey tool in the form of a questionnaire and disseminated it to the study population electronically by utilizing email, paper, and social media platforms including Facebook, WhatsApp, and Telegram.

4-1- Study community and sample: A variety of job titles, a group of professors, physicians, and people employed by the State of Algeria's institutions and agencies, security agencies, and even the private secto such as marketing offices and travel agencies, for instance made up the study community.

Table N°1. Data for the distribution of questionnaires.

	number	percentage
The Distributeur	60	100%
Not refundable	01	1,67%

The Acquired	**The canceled**	01	1,67%
	The lost	08	13,33%
	Adaptable to analysis	50	83,33 %

Source: From the researchers based on the results of the questionnaire.

A study aid: We relied on the questionnaire tool as a key source for gathering the data required to carry out the field study in order to determine the degree of the study sample's awareness of the significance of cyber security and its actuality. It was created (beginning with an introduction that clarifies the purpose of the study and attests to the confidentiality of the responses), and the closed questionnaire questions covered the primary facets of the investigation since the research instrument was separated into:

First Section: comprises general and functional data about the study sample members (who responded to the questionnaire) based on five variables: age, gender, job title, number of years of experience, and academic background.

Second Section: There are two axes used for the questionnaire's twelve questions, which are related to the study data. You may see the questionnaire axes in Table No. (3).

In order to verify the apparent correctness and dependability of the questionnaire's content, we showed the list of questions to a panel of academic arbitrators. The necessary adjustments were made after taking the arbitrators' instructions and feedback into consideration.

Tools and techniques for statistical data processing and analysis: A collection of descriptive statistical techniques that are suitable for the sample type and study nature were employed in order to address the study's issue and evaluate its hypotheses. These techniques include:

- Frequencies and percentages were used in descriptive statistical studies to characterize the study sample's demographic factors, arithmetic means, and standard deviation.
- The Cronbach's alpha test assesses the validity and stability of the measurement instrument "questionnaire"; Table 3 shows that the Cronbach's alpha stability coefficient for sample participants ranged from 0.723 to 0.858.
- Arithmetic mean: If the answers' arithmetic mean is higher than (3), this indicates that the neutral opinion is represented by score (3).

- The purpose of the T Test (One Sample T-Test) is to determine the differences between the community mean and the single sample mean; that is, a 95% confidence level is represented by a significance level of 5%.

- **Arithmetic mean and degree:** The arithmetic mean was used in the fields displayed in Table No. 2 in order to determine the values of the arithmetic mean.

Coefficient of correlation (R).

- The magnitude of study that was employed: To gauge how the members of the descriptive study sample responded to the statements on the questionnaire and to make sense of the sequence in which we responded, we employed a five-point Likert scale:

Table N°2. Descriptive responses are converted into numerical form using a five-point Likert scale and the associated percentages.

The scale	**Strongly disagree**	**Disagree**	**neutral**	**Agreed**	**Strongly agree**
Quantitative Formula	1	2	3	4	5
%	1-20	21-40	41-60	61-80	80-100
Average	1-1.79	1.8-2.59	2.6-3.4	3.5-4.3	4.4-5
Degree of approval	Very weak	weak consent	Medium	High approval	too high

Source: From the researchers based on previous studies.

The statistical packages for social sciences program: After the questionnaire was filled out, we used the results to evaluate the data, determine the trends and scope of the research sample participants responses, and determine whether the hypotheses were valid.

- **Validity and reliability of the questionnaire:** We used Cronbach's alpha to calculate the reliability coefficient and the reliability coefficient that is derived from taking the reliability coefficient's root. The results of entering the responses we received into the SPSS software were as follows:

Table N°3 Cronbach's alpha (reliability coefficient) results.

Study data	Number of paragraphs	Honesty factor
First: The role that media attention has in spreading awareness about cyber security in Algeria.	05	0.723
Second: Information technology's function in defending security institutions against intrusion and hacking.	07	0.773
Total number of questionnaire	12	0.858

Source: From the researchers based on the results of the questionnaire.

The Cronbach's alpha coefficient values for each of the questionnaire's axes varied from 0.723 to 0.773, respectively, which is high and strong and greater than 0.70, according to the table. The reliability coefficient and degree of validity are both high, as indicated by the Cronbach's alpha score of 0.858 for the questionnaire's axes taken together. Because we have verified the questionnaire's appropriateness for the study and its capacity for analysis, interpretation, and hypothesis testing, we are thus confident in its validity.

Examination of the study sample participants' responses: Features of the study sample's demographics: Five categories of variables are used to describe the sample members who took part in the study, including gender, age, educational background, experience, and present employment.

Table N°4. Title (Source: Name of author (year), page)

Demographic variables		**number**	**Percentage %**
Sex	Male	40	80%
	Feminine	10	20%

	the total	50	100%
the age	Less than 25 years	07	14%
	From 26 years to 30 years	10	20%
	From 31 years to 35 years	16	32%
	From 36 years to 40 years	09	18%
	More than 41 years	08	16%
	the total	50	100%
got a certificate	Bachelor's degree	17	34%
	Master	13	26%
	PhD	20	40%
	the total	50	100%
Your current role	Professor	20	40%
	Bank employee	13	26%
	Head of department at the institution	17	34%
	the total	50	100%

Years of expertise	From 1 to 5 years	08	16%
	6 to 10 years	19	38%
	More than 11 years	23	46%
	the total	50	100%

Source: From the researchers based on the results of the questionnaire.

We examined the study sample's characteristics to determine how they affected the accomplishment of the study's goals. Males made up 40% of the sample, or 80%, according to the data in the preceding table, indicating that they are more interested in this field. Given that Algeria is a conservative country ruled by traditions and beliefs, this makes sense, particularly in Arab societies generally. On the other hand, universities in the Kingdom of Saudi Arabia, for instance, have established a full specialization in this area. With a proportion of 32%, the age group between 31 and 35 years old leads, with 16 people falling into the young category. This makes sense because it is a generation that grew up on computers, smartphones, electronic games, and the relative availability of the Internet. We find it interested in everything new in the field of TIC. As for the educational level, we see that most of them have a high level of PhD holders and those who are preparing To get it by 40%, their number reached 20. This category is educated and cultured and is considered the elite of society. Their specialization may be electronic and interested in the field of computers, given that their work requires the presence of a computer and the Internet. It is followed by PhD holders by 40%, their number is 20, and this is acceptable. Regarding the job, we see that there is diversity in the job titles of the responding individuals, and from there, diversity in viewpoints on the subject of the study, which contributes to enriching it and increasing the accuracy of information. The majority of them are professors who are leaving the teaching profession at Algerian universities with administration and management at times. Their number reached 20% by 40%, given that their knowledge requires the Internet using e-mail. With the transition to distance education through e-learning platforms, for example, in light of the global outbreak of the Corona virus (Covid 19), it has become necessary to protect programs and computers from any danger that may occur. It is followed by heads of departments and those who hold sensitive positions in state institutions, so it is mandatory to maintain confidentiality. Their information, and their need to protect themselves and their country, and most of the study sample members have worked for more than 11 years, with a percentage of 46, their number reached 23, they have sufficient experience, according to their experience in their field of work, they realize the importance of protecting themselves and their phones, so the need for cyber security has become certain compared to countries keeping pace with the developments taking place, due to the culture of individuals and societies.

The significance of media attention in advancing the idea of cyber security is the first axis.

Table N°5. The first axis phrases are analyzed.

Algeria's actual cybersecurity practices	Iteration	%	The assessment of cyber security is challenging.	Iteration	%
excellent	12	24%	Yes	22	44%
Good	09	18%	I don't know	10	20%
acceptable	05	10%	No	18	36%
superficial	24	48%			
the total	50	100%	the total	50	100%
The person who gains from cyber security	Iteration	%	Methods for Assessing Cybersecurity	Iteration	%

The State	28	56%	Good	17	34%
Universities	10	20%	Middle	16	32%
Economic institutions	09	18%	Weak	13	26%
I don't know	03	6%	I don't know	04	8%
the total	50	100%	the total	50	100%
Are you familiar with the idea of cyber security?				Iteration	%
Yes				23	46%
No				11	22%
Maybe				09	18%
I don't know				07	14%
the total				50	100%

Source: From the researchers based on the results of the questionnaire.

The table above for the statements of the first axis, which are questions that were answered according to the opinions of the study sample members, shows that they are diverse. We notice that 48%, 24 in number, say that the reality of cyber security in Algeria is superficial. In their opinion, it is a relative effort in the field of combating cybercrime with the emergence of a special cell for it located in the capital and headquartered in Bab Ezzouar. There is a great need to activate it due to the large number of crimes in this field, which has become a danger. The points of view agreed regarding the difficulties facing cyber security, as there is a group that answered yes, there is a difficulty, with a percentage of 44%, 22 in number. The unexpected difficulties lie in the technologies and software that are constantly evolving. Algeria has brains and competencies in addition to energies capable of facing the difficulties and challenges of the fields of information and communication technology (TIC) and finding Solutions, as for the category that does not know and does not have any idea about cyber security or its difficulty, it is the majority, as its percentage reached 11.6, their number is 2, the party benefiting from activating cyber security according to the opinions of the respondents, the state is the big winner, their percentage reached 50, their number is 25, by virtue of the fact that it protects it from any threat or enemy, whether in relation to individuals or security agencies, and with a percentage of 22, their number is 11, they said that the universities benefit from activating cyber security because they rely on computers in relation to the information of students and professors, so they need continuous protection, and as for the institutions of an economic nature, with a percentage of 10, their number is 5, according to their opinion, they benefit from cyber security, especially those that practice network marketing, their dealings via the Internet, customers and local clients, across the countries of the world, they need protection in order to gain the trust of the dealers, and the category that The beneficiary does not know the same number and percentage, as for the evaluation of cyber security, the percentage is 18, their number is 9, as for the question, do you have information about the concept of cyber security, the opinions varied between yes, no, maybe, and I don't know, so the percentages differed due to the fact that the term is relatively new in appearance and use.

Table N°6. Examine the second axis's paragraphs and ascertain their orientation.

The paragraphs	1	2	3	4	5	The arithmetic mean	The standard deviation	Level of approval
	%	%	%	%	%			
Employing cyber security services is crucial for businesses.	11.1%	_	16.7%	_	72.2%	4.217	1.312	too high
Communication and the media play a significant part in	40 %	_	60 %	_	_	3.087	1.411	Medium

increasing public knowledge about cyber security.								
The function and significance of cyber security are explained on certain blogs or social media pages.	27.8%	_	22.2%	_	50%	3.260	1.601	Medium
Every precaution is made to shield consumers and citizens from the risks associated with internet.	5.6%	_	80	5%	9.4%	4.565	1.036	too high
Since cyber security is a key component of contemporary war and attack strategies, it is regarded as a strategic weapon in both the hands of the government and the individual.	10%	7%	14%	3%	66%	4.087	1.311	High
Cyber security guarantees the privacy, confidentiality, and protection of personal information.	27.8%	_	16.7%	_	55.5%	4.043	1.186	High
Cyber defense shields citizens and the country against the perils of the Internet.	30%	4%	37%	9%	20%	4.043	1.106	High
The sum of the second axis scores						4.007	1.003	High

Source: From the researchers based on the results of the questionnaire.

The table displays the findings for understanding cyber security and how it is reflected in the opinions of the survey participants. With an arithmetic mean of 4.007 and a standard deviation of 1.003, we deduce that the second axis had a high degree of general approval. We see that, with an arithmetic mean of 4.565 and a standard deviation of 1.036, the paragraph that read, "All necessary measures are taken to protect the citizen and consumer from the risks of cyberspace," came in first place with a very high degree of approval. This suggests that awareness and a culture of reporting cybercrime to safeguard oneself and one's property are beginning to emerge According to their assessment, the paragraph "Using cyber security services is of great importance to institutions" came in second place with an arithmetic mean of 4.217 and a standard deviation of 1.312. The significance is in preserving Regarding its worth and standing in addition to its ability to endure and continue, the paragraph comes in third. Because it is a crucial component of contemporary strategies for international conflicts and attacks, cyber security is regarded as a strategic weapon by both the government and individuals. It has a high degree of approval with an arithmetic mean of 4.087 and a standard deviation of 1.311. With an arithmetic mean of 4.043 and a standard deviation of 1.186, indicating a high degree of approval, the fourth rank paragraph, "Cyber security," guarantees protection and secrecy in addition to the privacy of personal data. The paragraph that follows, "Cyber defense protects the homeland and the citizens alike from the dangers of the Internet," came in fifth place with a high degree of approval and an arithmetic mean of 4.043 and a standard deviation of 1.106. The sixth ranking is the paragraph that states that communication and the media play a significant role in increasing public knowledge of cyber security. Finally, the paragraph in the seventh rank, which reads: There are special pages on social media or blogs that explain the role and importance of cyber security, has an average degree of agreement, arithmetic mean of 3.260, standard deviation of 1.601, and a standard deviation of 1.411. and an average degree of agreement, and finally, in the seventh rank, the paragraph: There are special pages on social media or blogs that explain the role and importance of cyber security, with an arithmetic mean of 3.260, a standard deviation of 1.601, and an average degree of agreement.

5- Discussion and analysis of results:

The parametric test (T for one sample), which is deemed appropriate if the data follow a normal distribution, was employed to evaluate the data and assess the study hypotheses. The null hypothesis cannot be rejected if Sig is more than 0.05 based on the SPSS outputs, and the average opinions of the study sample members on the phenomenon under investigation do not significantly deviate from the average degree of agreement, which is (3).

On the other hand, if Sig is less than 0.05, the alternative hypothesis is accepted and the null hypothesis is rejected, and the average degree of agreement is significantly different from the average opinions of the study sample members. As a result, by using the T value to increase or decrease the average degree of agreement, the average response may be found. A positive value indicates that the answer's arithmetic mean is higher than the average degree of agreement, and vice versa.

Table N°7. One sample T test results.

Number of paragraphs	T	Sig	R	Variance analysis
01	17.855	0.000	1.000	1.948
02	12.836	0.000	0.167	2.000
03	10.000	0.000	0.167	2.824
04	8.416	0.000	0.000	-0.195
05	19.241	0.000	-0.167	1.912
06	20.283	0.000	0.612	0.801
07	16.299	0.000	0.000	1.114
Every paragraph in the second axis	12.785	0.000	A significance score of 0.05 indicates that the correlation is statistically significant.	

Source: From the researchers based on the results of the questionnaire.

The aforementioned table shows that the significance value, sig 0.000, is less than 0.05 and that the value of t reached 12.785 degrees of freedom. Thus, we conclude that the average responses of the sample members and the significance value have a statistically significant relationship.

Hypothesis testing: As seen in Table 7, we computed Sig to evaluate the hypothesis's validity. According to the correlation outputs R approaching and equaling 1, which demonstrate the internal coherence with the second axis paragraphs, we can observe a very strong direct relationship and strong correlation. The computed T value, as we can see, was 12.785, This is less than 5% and smaller. Thus, we deny the null hypothesis, H0. We accept the alternative hypothesis H1 because there are no statistically significant differences, at a significance level of 0.05, between the opinions of the study sample participants regarding how they perceive the reality of cyber security according to its dimensions attributed to the variables (gender, age, educational qualification, experience, and your current job). At a significance level of 0.05, there are statistically significant differences between the study sample's participants' perceptions of the reality of cyber security based on the dimensions assigned to the variables (gender, age, educational background, work experience, and current employment).

6- CONCLUSION :

The study helped clarify the theoretical aspects of the cyber security literature. Understanding the realities of cyber security in Algerian security agencies and organizations allowed us to apply the study in the field as well. After addressing the issue and testing the hypothesis, we conducted a random sample study and came to several conclusions and suggestions.

7- Results:

- ✓ In Algerian institutions, the study sample had a high level of awareness regarding the actuality and significance of cyber security.
- ✓ Computers and information are the targets of cyber security, which serves the dual purposes of establishing confidentiality and integrity for data as well as safeguarding it.
- ✓ Like road safety, cyber security is everyone's duty; thus, because of its catastrophic economic, social, and moral ramifications, everyone must cooperate and collaborate.
- ✓ When working online, cyber security helps to create a very safe working environment.
- ✓ Because it helps manage risks and dangers, cyber security is a means to a goal that guarantees the safety of both individuals and institutions.
- ✓ All aspects of cyber security are necessary for many facets of society, and Algerian institutions in particular, both now and in the future.
- ✓ Cyber security is always changing and is important because it keeps information safe and intact by avoiding manipulation.

8- Prospects and suggestions:

- ✓ The necessity of raising cyber maturity and knowledge across the board, including in the areas of education, the economy, banking and finance, industry, communications, military, justice, and transportation, among many others.
- ✓ Promoting the usage of cyber security aspects since they are the best information and communication technology practices.
- ✓ Establishing procedures for institutions and government organizations to control cyber security governance.
- ✓ The greatest method to help safeguard yourself and your work online is to stay informed and exercise caution.
- ✓ Laws and regulations must be developed to combat the threats to cyber security.

9- References:

1) AL_TORKI , A. (2021, 01 18). *security in the Quran*. Consulté le 04 15, 2021, sur Glory towards a safe society: https://almajid.ps/news620/
2) ALACHACH, I. (2018). Cyber terrorism and the challenges of countries: a comparative study with international agreements. *Research ISSUE 12*, p. 186_ 187.
3) ATTALAH, S. (2020, 09 04). *arageek mojtamea*. Consulté le 03 27, 2021, sur What is cyber security and what are its benefits: https://www.arageek.com
4) *Cyber Security*. (2022, 02 12). Consulté le 04 04, 2021, sur Political Encylopedia: https://political-encyclo peadia.org
5) KADIM, A. (2012). *Artificial intelligence.* IRAQ: Imam Jaafar AL_Sadiq university.
6) MOHAMED ABDEBASET AYOUB , A. (2020, 07 03). *ARID*. Consulté le 03 27, 2021, sur The concept of cyber security and its relationship to information security and electronic security: https://portal.arid.my/ar-LY/Posts/Details/94edf980-c7a4-4f30-afcb-5bc393af018c.