

The strategy of the Algerian state for information security
- risks and challenges-

Kassaa Khadidja ^{1,*}, Benzerouk Djamel ²

¹ **University of Salah Boubendir, Constantine 03 (Algeria), khadidja.kassaa@univ-constanline3.dz**

² Media and Communication Studies Laboratory; University of 20 August 1955 in Skikda (Algeria), d.benzerouk@univ-skikda.dz

Received: 09/06/02025

Accepted: 17/09/2025

Abstract:

This study tackles the mechanisms of implementing the information security strategy in Algeria by showing its features, vision, elements, fields of application, and the challenges and obstacles that face it. In this regard, we conducted an analytical study on the Army Magazine and used a purposive sample that included 16 issues from 2020 to 2023. Besides, we used the content analysis and found out that the information security in Algeria is one of the new challenges the state aims at developing to combat the cyber risks. Besides, in presenting the army strategy for information security, the Army Magazine insists on increasing awareness about the importance of protecting the electronic devices because the citizens are vital for the success of the strategy. Finally, it is necessary to develop the army, invest in the youths, and secure the social media.

Keywords: *information security, risks, The strategy*

*Corresponding Author

I. INTRODUCTION

Information security is one of the most demanded modern fields in the local and international markets because it is a strategic weapon that aims at ensuring the availability and continuity of the cyber systems, and at securing the secrecy and privacy of the personal information against the cyber attacks. Lately, the interest in information security has increased, mainly with the shift towards the digital governments, what raised the states' worries about how to protect their cyber systems amid the increasing electronic threats. In this regard, Algeria aims at protecting its cyber system through different security entities, such as the National Popular Army, which has shown high interest in the information security in the last 05 years. The Army redoubled its efforts to face the electronic crimes committed by different people or organizations by promoting the laws that foster the information security in the state.

The new generation wars became a reality and raise different challenges and threats. In this regard, many thoughtful and multilateral plans target different states to weaken and divide them. Therefore, Algeria is careful and is consolidating its information security. In 2020, the Algerian President signed a decree that provided for setting a strong strategy for information security and for founding the Information Security Agency, which works with other entities to develop the strategy based on a vigilance system that deters the new threats with their ramifications. Based on what was said, we raise the following problematic, "how is the Algerian strategy of information security implemented?" From this, sub-questions arise as follows:

1. What are the electronic threats that face the state institutions under the wide spread of internet?
2. What are the measures adopted by the Algerian National Popular Army to achieve information security?
3. What are the security strategies adopted by the Army to face the cyber attacks?
4. What are the challenges that face the institutions in achieving the information security?

Aims of the study:

This study aims at:

- Identifying the main electronic risks that face the institutions, and the role of the Army in protecting them.
- Identifying the main techniques used by the state to protect the institutions and states from information insecurity.
- Raising awareness of people and institutions about the importance of information security.
- Identifying the challenges that face the Army in its mission to fight the cyber crimes.
- Identifying the security policy against the cyber insecurity.

The study concepts:

1.1 The information security:

It is a set of tools and procedures that must be provided to protect the information from the internal and external risks, and to protect the secrecy, privacy, and integrity of information against its violation and illegal use for the commission of crimes (Al Arabia, 2018). The information security covers the administrative and technical measures and procedures to protect the sources of information (i.e., devices and software) and the people from the illegal interventions and violations that happen indeliberately or deliberately through hacks, or as a result of wrong procedures or insufficient protection. Thus, the information security covers the following axes:

- The indeliberate mistakes when uploading information.
- The incidents of losing or modifying the information due to errors in the devices or programs.
- Theft, capture, authorized adjustment, or misuse of information.
- Loss of the information management skills due to some natural catastrophes (al Qattal, 2008).

1.2 Cyber security:

It can be defined based on its goals as the activity that protects the human and financial resources used in communication and information. It is about limiting the losses and damages that may result from the threats and risks. Besides, it allows restoring the situation as fast as possible so as not to stop production and to avoid permanent losses. In addition, it is the protection of the information of the telecommunication systems from any damage, illicit use, modification, or exploitation (Samira, 2017). Besides, it is protecting the systems, data, communications, nets, and internet from the digital attacks, which are usually referred to as the cyber attacks, that aim at violating, modifying, damaging, logging in, or using the systems. The attacks may include the installation of harmful software on the device or the destruction of the whole infrastructure of a state (The National Cyber Security Center).

1.3 Electronic piracy:

It is illegally copying or distributing copy rights materials. It negatively affects innovation, including the production of films, TV shows, music, and games. Besides, it has negative economic consequences because it affects the sources of governmental incomes, subjects the consumers to potential financial losses, and raises security threats, such as the theft of identity or broadcasting unsuitable content for children (<https://www.interpol.int/ar/4/13/8/5>).

1.4 The electronic crime:

It is any illicit act where high knowledge about computers is needed for its commission, investigation, and prosecution. Besides, it is the illicit act where the computer is used, or is the criminal act where computer is a main tool (Aggoune, 2012).

1.5 The electronic attacks:

They are attacks from one or a set of computers against one or a set of computers or nets. The attacks may aim at breaking the system of a computer, accessing its data, or getting the prerogatives of its user.

1.6 The information security policy:

It is a mixture of principles, systems, methods, and tools to protect the organization from the threats (Tryfonas et al., 2001). Alnatheer (2015) sees that it is a strategic document that is established before any activity of information security. It includes the goals, trends, and rules that must be followed by the others that deal with the organization. Therefore, it must be clear and show clear goals, roles, and responsibilities of the employees and the other parties. Moreover, it must be comprehensive and cover all the sides, requirements, and regulations of information security, and be compatible with the organization policy and vision.

2. A historical background on information security:

Alexander Klimburg pointed that information security is in an infirm frame, as confirmed by NATO in 2013 when discussing the side effects of information security on the security of states due to the increasing technical innovations at that time. In 1943, Thomas Watson, the CEO of IBM Company, predicted the status quo of technology and information and the emergence of an international market for their products. Then in 1977, Ken Oslen, the head of the digital tools company, recognized that there was no cause for people to have computers at home. In the 1960s, the world witnessed successes in the digital cycles, intranet, and personal computers. In the 1970s, the audiovisual telecommunication nets and the cell phones appeared, and were followed by the Graphical User Interfaces in 1984. Later in 1990, Windows system appeared. As for internet, it appeared in 1991, and Google was founded in 1998. As for the 1st model of Apple I Phone, it was in 2007 and was followed by the Ipad in 2010.

People who invested in these techniques turned very rich; however, there were big losses in the products. Due to the failure of these techniques, the expression “information security” lost its position. The massive wave of innovations, known as Technami, brought about negative effects and harmful consequences, mainly the information insecurity, which raised worries about the possibility of controlling the modern innovations and techniques.

3. The requirements of information security:

The protection of information security requires raising awareness of the organization workers about the risks that threaten the information. The requirements include the following:

Hamed & al Hamoud (2009) see that the risks of information security are all deliberate and indeliberate human practices, political events, and environmental effects inside or outside the organization that lead to the deterioration, devastation, theft, or falsification of some or all the accounting information and to losses in time, effort, and money.

The electronic information systems face many risks and threats, including the manipulation, to destroy them through their deletion, wrong integration with each other, mixing them with unreal data, and wrongly classifying them. The manipulation dissociates the data from their facts and takes place during inputting, operation, storing, or outputting. Besides, the threats may be a theft of the computer time, using the computer for personal purposes, illicitly accessing the systems and nets, destroying files and communication net, natural catastrophes such as fires and floods, arsons, viruses, unauthorized presentation of data on screens or on paper, and their distribution by unauthorized people (Moussa, 2020).

4. The importance of information security:

The importance of information security lies within the following:

- The security and military sectors rely on the exactness and validity of information.
- The states need security measures that face the risks of dealing with other parties.
- There is an increasing need to establish a safe electronic environment that serves the private and public sectors.
- The electronic applications are rapidly increasing and need a safe environment.
- The electronic crimes increased with the development of the cyber techniques.
- It is necessary to protect the infrastructure of internet for the sustainability of the commercial activities (Al Arichi, p. 10).

5. The dimensions of information security:

The dimensions of information security are:

1. The secrecy of information: This implies it is not possible to access or modify the information stored on computers or transferable online.
2. The integrity of information: This is about not changing the information stored on computers or transferable online.
3. The quality of information: It is about no deleting the information stored on the computers unless by the authorized people (Amina, 2016).

6. The risks of information security:

Information security faces different risks and threats that negatively affect the sources of information. Such threats are not only electronic, as they may be from one of the employees or the outcome of an incident that leads to the loss of information. In this regard, we shall mention the following types:

First: Violating the material protection:

This takes place through 04 techniques, as follows:

1. Looking in the technical waste: The criminal relies on the garbage of the organization, such as CDs and flash drivers, and tries to find information in it.
2. The wiretapping: The criminal makes a wire communication with the net.
3. Eavesdropping: The criminal uses captors to receive the bands released from the systems.

4. Service cancellation: This is about harming and hindering the delivery of the service (al Qahtani, n.d.).

Second: The cyber threats:

They are the most widespread and include the malware, such as viruses, spams, and other techniques that highly harm the information and devices of the organization. This pushed many organizations to specialize in producing protection tools, such as the fire walls, anti-viruses, etc. The methods that harm the software and devices include:

- Storage devices: The viruses may move from one computer to another through the storage devices that transmit the files and programs, such as CDs, USB drivers, etc.
- Email: Email is one of the most important tools in transferring viruses because it is very widespread. The email may include viruses or links to hacking sites or to downloading malware.
- Suspicious websites: Internet servers show different security gaps that are generally ignored by the users. Some suspicious websites take advantage of such gaps to access the computers and download malware.
- Downloading programs from internet: Some programs are not protected from viruses (Hanan, 2014).

Third: The internal threats:

The employees are the main source of internal risks that may face any government or organization because they know the information systems and have high knowledge about the internal controls and the weaknesses or strengths of the system. Besides, they can deal with and access the information thanks to the authorization they have. Therefore, the dishonest employees may destroy or modify the information (Aicha, 2021).

Fourth: The external threats:**How to face the risks when they happen:**

Despite the security measures, risks may happen. Therefore, it is necessary to think about a plan that includes the technical and legal measures to limit the losses and secure the work continuity with alternative tools. Moreover, the plan should show the measures of analyzing the nature and causes of the risks that happened to suggest reforms and ensure the risks will not reoccur (Amina, op. cit.)

2. The analytical study:**2.2 The study population:**

The identification of the study population is one of the main methodological steps in the human and social sciences because it requires exactness and focus. The study population is defined as the environment where the study phenomenon takes place because it starts from it and goes back to it. Thus, it is a set of views or items within a given frame, which have common features (Al Tuwissi, 2001). In our study, it is the issues of the Army Magazine of

the Algerian Ministry of National Defense. It is a monthly electronic and paper magazine in Arabic and French.

2.2 The sample:

It is part of the study population from which we collect data. It is part of the whole on which the study will be conducted to allow generalizing the results, later, on the whole population (Zerouati, n.d., the National Cyber Security Center). In this study, we used a purposive sample that covers 15 issues of the Magazine in 2020, 2021, 2022, and 2023, which tackled the question of information security, as follows:

2020	Issue 685	Issue 683	Issue 680	Issue 681	Issue 679
2021	Issue 691	Issue 693	Issue 694	Issue 701	
2022	Issue 702	Issue 703	Issue 705	Issue 708	
2023	Issue 714	Issue 715			

2.3 Method of the study:

The method is the set of general rules and systems used to achieve acceptable results about the study phenomenon. The study uses the analytical descriptive method in collecting data and facts on the topic. This method is good for studying the natural social phenomena because the descriptive study is qualitative and shows the features of the phenomenon while the quantitative shows the size, changes, and correlation with other phenomena.

4.2 Analysis and interpretation of the data:

1. The category of “how it was said”

Table 01:

Category of journalistic arts	Frequency	Percentage
Reportage	00	00
Report	08	50
Investigation	00	00
Interview	01	06.25
Comment	00	00
News	03	18.75
File	04	25
Total	16	100

Table 01 shows the journalistic arts used by the Magazine in treating the question of information security. In this regard, the report ranks first with a percentage of 50%. It is used in the study issues to show the concepts of information security, electronic crime, cyber security, and others. Besides, it shows statistics and the activity of the Army for the information security. It is followed by the file, which is very important and has been used during the 04 last years to present a detailed description of the issue of information security. It helps cover the topic from all its sides. Then, we find the journalistic news with a percentage

of 18.75%. This type covers the activities of the Army for the information security. After that, we find the interview with a percentage of 6.25. However, the other types are not used despite their importance in covering such topics.

Table 02:

The category of the content language	Frequency	Percentage
Journalistic language	12	75
Scientific language	04	25
Total	16	100

The table shows the language used by the Army Magazine to make the journalistic arts used in covering the question of information security. In this context, 75% are written in a journalistic language that relies on the writer's personal style while 25% are in a scientific language based on different scientific references.

Table 03:

The category of the presentation style	Frequency	Percentage
Text	03	18.75
Image	00	00
Text+ image	13	81.25
Total	16	100

The table shows the presentation styles used by the Magazine in treating the issue of information security. In this context, the text+image is the most used, with a percentage of 81.75%, followed by the text, with a percentage of 18.75%

Table 04:

The category of the number of pages	Frequency	Percentage
Less than 01 page	03	18.75
01page	07	43.75
02 to 04 pages	02	12.5
More than 04 pages	04	25
Total	16	100

The table shows the number of pages used by the Magazine in discussing the information security. In this context, 43.75% of the articles are in one page, 25% are in 04 pages, 18.75% are in less than one page, while 12.5% are in 02 to 04 pages. Usually, the number of pages differs according to the journalistic style used to treat the topic.

Table 05:

The category of headings	Frequency	Percentage
Headline	04	25
Subheading	12	75
Subtitle	00	00
Total	16	100

The table shows the types of headings used by the Magazine in treating the topic of information security. Findings show that 75% of the headings are subheadings while 25% are headlines.

2. The category of “what is said”:

Table 06:

The category of the target audience	Frequency	Percentage
Individuals: workers+ employees	00	00
Security institutions	03	18.75
Private and public companies	00	00
Public audience	13	81.25
Total	16	100

The table shows the target audience for the Magazine. Most of the articles, 81.25%, are meant for the public audience while 18.75 are for the security institutions.

Table 07:

The category of the goal of discussing the question of information security	Frequency	Percentage
Introducing the question of information security	05	20.83
Providing statistics on the information security crimes	04	
The policy adopted by the Army for the information security	08	50
Raising awareness about the importance and sensitivity of the information security	03	18.75
Showing the challenges faced by the Army in deterring the information security risks	05	20.83
Total	24	100

The table shows the goals behind tackling the information security question. In this context, 50% aim at showing the policy adopted by the Army for the information security, 20.83% aim at showing the challenges faced by the Army in deterring the information security risks, while 18.75% aim at raising awareness about the importance and sensitivity of the information security.

Table 08:

The category of the aspects of information security focused on by the Magazine	Frequency	Percentage
The theft of and access to information	10	40
Hacking the official websites	06	24
Spying on the official websites	06	24
Assault, defamation, libel, threatening, etc	03	12
Total	25	100

The table shows the aspects of information security focused on by the Magazine. In this regard, 40% are the theft of and access to information, 24% are hacking and spying on the official websites, and 12% are the issues of insult, libel, defamation, and threatening.

Table 09:

The category of the methods used by the Magazine to cover the question of information security	Frequency	Percentage
Presenting statistics on the topic	04	17.39
Testimonies, experiences, and real events in the field of information security	02	8.70
Enacting laws and regulations on information security	03	13.04
The activity of the Army in the field of information security	09	39.13
The training sessions for the soldiers on information security	02	8.70
Advice, guidelines, and instructions on how to achieve information security and avoid its risks	03	13.04
Total	23	100

The table shows the methods used by the Magazine to cover the question of information security. In this context, 39.13% are about the activity of the Army in the field of information security, 17.39% are about presenting statistics on the topic, and 13.04% are about advice, guidelines, and instructions on how to achieve information security and avoid its risks, and the same for enacting laws and regulations on information security. Finally, 8.70% of the methods are the training sessions for the soldiers on information security.

Table 10:

The category of the dimensions of the information security focused on by the Magazine	Frequency	Percentage
The need to be aware about the sensitivity of the issue	07	46.67
The application of the necessary precautions and measures to protect the electronic devices (information secrecy and privacy)	05	33.33
How to deal with the different forms of electronic piracy	03	20
Total	15	100

Table 11:

The tasks presented by the Magazine regarding the information security	Frequency	Percentage
Making investigations in case of electronic attacks	01	2.70
Evaluating, collecting, and presenting different information on information security	14	37.83
Discussing the different issues of information security	11	29.72
Developing an efficient and effective security strategy	09	24.32
International cooperation to develop the information security	02	5.40
Total	37	100

The study results:

1. The Army Magazine uses different journalistic arts in treating the question of cyber security depending on the content, method, and space devoted. In this regard, the report is the most used to treat the topic from a given angle and provides a general description about the topic and its risks by presenting all the relevant points that may build the attitude of the reader or the target audience. In addition, the file ranks second. The one file may include different

journalistic types and helps tackle the topic in a detailed and thorough way to link it to the different variables. Thus, the writer can provide definitions, statistics, and experiences of the institution in the field and in the other variables thanks to the space devoted, which is about 05 pages.

2. The Magazine uses Arabic and French and relies on the journalistic and scientific styles. In some journalistic arts, the writer uses books and scientific papers written in Arabic and French to give an objective vision, detail the concept of information security, and identify its risks because he uses a reliable scientific content.

3. The Magazine uses the Text+image in the different journalistic types. The images are usually about the electronic devices, the social media, and the soldiers assigned with the cyber security to show their tasks and activities in the field. The use of images adds meaning and fosters the information, as some studies confirm that the image is more influential on the brain than the text, and helps even digest the text.

4. The Army Magazine devotes a special space for the information security because the study issues covered the topic and its related points many times. Sometimes the issues are successive, what confirms the interest of the Army in information security. In this regard, the space devoted for the topic depends on the journalistic type as we already said. Most are in one page and take the form of news or reports. On the other hand, the interviews with the stakeholders, including the Head of the Department of Cyber Security and Controlling the Systems, were in 02 to 04 pages. As for the articles that exceed 04 pages, they were files made by the Magazine from one time to another, with long intervals, and discussed the topic in details.

5. Most of the headings used by the Magazine for the information security are subheadings about telecommunications. The Magazine divides its content according to different fields that cover the Army activities; the question of information security is usually part of the telecommunication field. As for the headlines, they are usually in red and confirm the importance and sensitivity of the topic; these headlines usually take a wide space.

6. The Magazine targets the public audience, including the individuals and the private and public institutions, through providing paper formats for the locals and electronic formats for the audience abroad. The information security is very sensitive and affects the security of states and individuals. Therefore, people must be aware about the topic and its risks. The Magazine tackled different topics to define the topic, increase awareness, and suggest solutions and preventive measures under the Army's strategy for the cyber security.

7. The study showed that the main goal of the Magazine behind discussing the information security is showing the policy of the Army in the field. The Army considers information security as a new war and challenge due to the illegal use of modern ICTs. This war is different than the military armed ones because it takes place behind the screens and may destabilize states and cause conflicts through electronic attacks via nets against the main vital infrastructure, the energy stations, the transportation means, and the ministerial departments. Therefore, the states in general, and Algeria in particular, must deeply focus on the topic by identifying the tools, needs, and strategies that allow preventing the risks. The attacks may be by the hackers or cyber units of other states.

According to the Magazine, the strategy of the Algerian army for information security is as follows:

- Investment in the human resources by promoting the requirements of the modern war, mainly in the units that secure the borders with the 07 neighboring states, by reinforcing the protection and tools, mainly the electronic ones, for the early detection of any threats.
- Fostering the defense capacities in the field of cyber security to face the threats of the new wars. In this context, the board of detecting and monitoring the cyber threats is equipped with the necessary forces and tools.
- Increasing the soldiers' awareness about the risks of the misuse of the communication and information devices through organizing open days, publications, and announcements on the Army intranet.
- Showing interest in the information and communication cell because of the sensitivity of its tasks to face the tools used in the 04th generation wars by facing all the rumors and misleading, informing the public opinion, and using the artificial intelligence AI in defense and security. In this context, AI with machine learning help the military forces cope with the military development in wars based on the personal experiences and the data the computers deal with. Besides, AI systems can easily identify the type of the electronic attacks and develop tools to face the counter attacks and identify the location of the targets.
- Securing the cyber systems and updating the legal frame of using modern ICTs.
- From the legal side, the strategy focuses on the organizational aspect based on the premise that the cyber defense operations are part of a functional and organizational series for the interaction and harmony of the activities.
- Due to the importance of the cyber space and the new challenges of the modern war, the higher leadership highly focuses on developing the technical and operational cyber defense to efficiently intervene and deter any violation of the national sovereignty and the nationals' safety.

The Magazine focused on different aspects, mainly the theft of and access to information and data. It confirms that the information insecurity is not limited to piracy, spying, or electronic crime; rather, it may take simple aspects but with high risks, such as the access to, modification, or deletion of information without leaving a trace because the threats against the cyber systems witness technical and practical developments. Therefore, the individuals must be aware and follow special measures to deter any threat and protect the secrecy of their personal information.

In addition, the Magazine discussed the piracy and spying on the official websites in the last years. As for the electronic crime issues, the Magazine focused on it in collaboration with the National Gendarmeries. Statistics show that in 2019 the treated cases were 71%, mainly regarding impersonation to commit libel and defamation, and intimidation through haggling and insults. The expert in criminal proofs states that this type of crimes is generally related to the personal and social relations built in traditional environments.

8. The Magazine relies on different styles that support the public policy of the Army by showing the main activities in the field of information security to insist on the high importance of topic for the Army, which allocated all the material and moral capacities and considered it as strategic challenge and a political defensive priority to protect the state from any threats against its stability. The magazine shed light on the activity of the cyber defense department and the training sessions to the soldiers to develop performance and control the modern technology, in addition to the meetings and scientific seminars to raise awareness about the risks of cyber security and the challenges faced to increase protection and prevention and manage the potential cyber crises and threats. According to the head of the department of Cyber Defense and Control of Information Systems, these sessions aim at:

- Promoting intelligence activities to detect the security threats and the malware.
- Evaluating the risks of the different cyber threats and their consequences on the systems.
- Predicting the cyber threats that affect the work of the systems by detecting the new weakness centers.
- Revealing the techniques, motives, and tools used by the perpetrators of the electronic attacks to take the necessary measures that protect the systems of the National Popular Army.

Moreover, the main activities and exercises of the army departments are presented, such as the 1st session of high quality cyber exercise “5+5 defense”, which simulated a wide range cyber crisis that targets the infrastructure. The session was held on 12-14 December 2022 to test the readiness of facing the cyber systems that threaten the space and evaluate the plans of managing the cyber crises. Furthermore, the Magazine presents statistics on the topic to increase understanding and awareness about the risk and sensitivity of the topic. The statistics help convince the audience with the topic, add credibility, and identify the risks for the target audience. These statistics show the number of internet and social media users in Algeria and the issues of electronic crimes.

Internationally speaking, 2021 witnessed different electronic incidents that led to losses in all the sectors estimated at 6000 billion USD. Therefore, the dependence on the modern ICTs is a source of cyber threats against the international security. Moreover, about 4.9 billion people all over the world are connected to internet. Therefore, the world is weak in front of the cyber activities. Issue 705

Regarding the cyber crimes in Algeria, it witnessed a remarkable development in the last years due to the increase and spread of modern ICTS, mainly internet and social media. The cyber investigations of the National Gendarmeries recorded an increase from 18 cases in 2008, 102 in 2013, to 1659 in 2019. The number of cases in 2018 was 1245 with 1004 victims; 307 were females and 737 were males. Most of the cases, 64%, were about attacks on people while the rest were about fraud, deception, violation of the automatic procession systems, and violations of properties. Issue 681

As for the enactment of laws and rules, the Magazine linked the information security and its aspects with the Algerian and international legal frames. It confirmed that the information security crimes are related to the activities that affect all the systems that automatically

process data, such as the cyber attacks that aim at hindering access to websites or the personal files. Besides, it is about the acts that harm the properties, individuals, and minors. Issue 685.

7. The Magazine focused on different dimensions that confirm the need to increase awareness of people and institutions about the sensitivity and risks of cyber security on people, institutions, and the state, and considered cyber security an integral part of the national strategy. The Magazine presented the different activities and the contents of the scientific meetings and study days that introduced information security and its sides and raised awareness about the good use of modern ICTs and how to deal with the potential threats. Besides, it discussed some previous issues on cyber crime to increase people awareness about the potential risks.

The implementation of the strategy of information security in Algeria depends on the people's and institutions' awareness because it is necessary to know how to protect the personal devices and face the different threats. Thus, people must have good knowledge about the elements of information security, the potential threats, and the laws and regulations to protect themselves.

According to the Army Magazine, the Army's tasks to achieve information security revolved around evaluating, collecting, and presenting the different information on the topic. The Magazine presents the concept of information security and the different relevant variables to clarify the image to the readers and increase their awareness on how to deal with its risks based on scientific books and references. Moreover, the Magazine shed light on the local and international activities of the Army and tried to discuss the topic from different angles. In addition, it presented the different policies and measures adopted by the Army for information security, and the US and Russian experiences to confirm the Army's continuous efforts to develop its policy and foster its readiness to face the information insecurity.

- **Referrals and references:**
- Bara Samira (July 2017), cyber security in Algeria: policies and institutions, the Algerian journal for human security (issue 04), p. 257.
- Ben Kara Mostefa Aicha (January 2021), the strategy of achieving information security for the electronic government in Algeria, the inclusive international forum on the theoretical issues and the methods of their practical treatment, Vol. 02, p. 30, Al Rafed house.
- Dalal Sadek, Hamid Nacer al Qattal (2008), information security, Jordan, technical education board, al Yazouri house for publication and distribution.
- Dr. Ghanim technical company for computers (n.d.), definition of the electronic attacks, paper published on <http://www.it.pillars.com>, accessed on 25.04.2023.
- Hamza Ben Aggoune (2011/2012), the criminal behavior of the information criminal, Batna, Magister thesis in legal sciences, major of criminology, Algeria: University of Batna.
- <https://www.interpol.int/ar/4/13/8/5>, (n.d), <https://www.interpol.int/ar/4/13/8/5>, accessed on 31.03.2023.
- Kedaifia Amina (30.06.2016), the strategy of information security: economic dimensions, Vol. 06 (issue 01), p. 166.
- Khaled Ben Salman al Ghouthir, Mohamed Ben Abdellah al Qahtani (n.d.), the information security, Ryad, King Fahd national library for publication.
- Mohamed Abidat, Mohamed Abu Nassar et al. (1999), writing the research methodology (rules, phases, and applications) (p. 135), Oman, Wail house for publication.
- Noufil Hadid, Karbit Hanan (2014), information security and its role in facing the electronic attacks on the company, journal of the institution (issue 03), p. 190.
- Rachid Zarouati (n.d.), writing the methods and tools of the scientific research in sociology (p. 267), Algeria: Houda house.
- Rida Ibrahim Saleh, Ahmed Abdessalam Abu Moussa (2020), study of the effect of information security on the success of the program of accounting information security system: field study on the Egyptian nets, journal of the contemporary commercial studies, Vol. 06, issue 10, p. 111.
- Selma Abderrahman al Dussari, Djibril Hassan Mohamed al Awichi (n.d.), the role of the higher education institutions in fostering the culture of information security in the society (p. 10), KSA, University of Queen Noura Bint Salma Abderrahman, URL: <http://www.pnu.edu.sa>.
- The National Center for Cyber Security (n.d.), accessed on 05.03.2023 from <http://www.ncsc.gov.bh>.
- The union of the Arab banks (04.09.2018), the information security: risks and future challenges, accessed on 29.03.2023 from a paper on <http://www.uabonline.org>.
- Tryfonas, T. K. (2001). "Embedding Security Practices in Contemporary Information Systems Development Approaches. Information Management& Computer Securit, vol 06 (n 04).
- Ziyad Ahmed al Tuwissi (2001), the study population and samples, Amman, Jordan, Education Directorate for Al Petra province.