***Dirasat*:** Human and Social Sciences, Volume 52, No. 5, 2025, 6562

Deanship of Scientific Research

Challenges of Iraqi National Security in Confronting cyber terrorism and ways to strengthen it

Zeyad Samir Al-Dabbagh [1]*, *Arshed Adil Rashed* [2], *Ghufran Younus Hussein*[1]

[1] College of Political Science, University of Mosul, Mosul, Iraq

[2] Mosul Technical Institute, Northern Technical University, Mosul, Iraq

Received: 5/1/2024
Revised: 17/3/2024
Accepted: 16/5/2024
Published online: 1/5/2025

* *Corresponding author:*
z-psc@uomosul.edu.iq

Citation: Al-Dabbagh, Z. S., Rashed, A. A., & Hussein, G. Y. (2025). Challenges of Iraqi National Security in Confronting Cyber Terrorism and Ways to Strengthen it. *Dirasat: Human and Social Sciences*, *52*(5), 6562. https://doi.org/10.35516/hum.v52i5.6562

Abstract

Objectives: The study aimed to identify and understand the challenges of Iraqi national security in confronting cyber terrorism and work to provide the most important ways to enhance cyber security in Iraq.

Methodology: To understand the research hypothesis and answer the questions raised in the problem, the study used systems analysis and inductive approaches.

Results: The study explained many results were reached, including Iraq's measures in enhancing cyber security are still below the required level, especially at the level of national legislation. The existence of a national cyber security strategy represents the first positive step to improving Iraqi national cyber security, but there is a need for regular updates and reviews of that strategy.

Conclusions: The technological and information development that the world is witnessing today has led to the dominance of open space in the absence of centralization responsible for organizing power within cyberspace, which has made society subject to many digital threats. Therefore, urgent and thoughtful mechanisms must be found to preserve society's security and the state's national security from aggressive actions and espionage carried out by terrorist groups.

Keywords: National security; Iraq; cyberterrorism; challenges; solutions.

تحديات الأمن الوطني العراقي في مواجهة الإرهاب السيبر اني وسبل تعزيزه

زياد سمير الدباغ [1]*، ***أرشد عادل راشد*** [2]، ***غفران يونس حسين*** [1]

[1] كلية العلوم السياسية، جامعة الموصل، الموصل، العراق.

[2] المعهد التقني الموصل، الجامعة التقنية الشمالية، الموصل، العراق.

ملخّص

الأهداف: هدفت الدراسة إلى تحديد وفهم تحديات الأمن الوطني العراقي في مواجهة الإرهاب السيبراني والعمل على توفير أهم السبل لتعزيز الأمن السيبراني في العراق.

المنهجية: لفهم فرضية البحث والإجابة عن التساؤلات المطروحة في المشكلة، استخدمت الدراسة منهج تحليل النظم والمنهج الاستقرائي.

النتائج: بينت الدراسة العديد من النتائج، من بينها أن إجراءات العراق في تعزيز الأمن السيبراني لا تزال دون المستوى المطلوب، وخاصة على مستوى التشريعات الوطنية. يمثل وجود استراتيجية وطنية للأمن السيبراني الخطوة الإيجابية الأولى لتحسين الأمن السيبراني الوطني العراقي، ولكن هناك حاجة إلى تحديثات ومراجعة منتظمة لتلك الاستراتيجية.

الخلاصة: إن التطور التكنولوجي والمعلوماتي الذي يشهده العالم اليوم أدى إلى هيمنة الفضاء المفتوح في ظل غياب المركزية المسؤولة عن تنظيم السلطة داخل الفضاء السيبراني، وهو ما جعل المجتمع عرضة للعديد من التهديدات الرقمية. لذلك لا بد من إيجاد آليات عاجلة ومدروسة للحفاظ على أمن المجتمع والأمن القومي للدولة من الأعمال العدوانية والتجسسية التي تقوم بها الجماعات الإرهابية.

الكلمات الدالة: الأمن الوطني، العراق، الإرهاب السيبراني، التحديات، المعالجات.

1. Introduction:

Cyberspace and security are not exclusively concerned with Telecommunications, Information and Internet services, but in many different areas, such as community and government infrastructures and services; however, each has different characteristics and challenges. This Cyberspace deals with data and information in a way that is preserved, modified and exchanged through private, controlled network systems. It is managed by the concepts of cybersecurity, which has become a universal character with national dimensions embodied in an electronic capacity in the economic, social and security aspects of the State, as well as the international dimensions. This advance is accompanied by electronic, technological, and digital Threats that cause significant damage to national security, which are beginning to rise across national borders, making it a complex challenge. Given these threats and risks, Strategies must be built to organize an integrated security framework that ensures adequate protection of the telecommunications and information technology sector and enhances its role in achieving Iraq's development objectives.Importance of Research: The research aims to identify the most significant challenges to Iraqi national security, as cyber risks spread to the security and safety of countries worldwide, with researching appropriate solutions to address and contain these risks.

2. General Framework of the Study:

2.1. Problem of the study: Iraq's national security challenges in the face of cyberterrorism are complex problems that require real solutions and treatments, which a set of questions can summarize:

1. How can Iraq protect its government institutions and critical infrastructure from cyberattacks?
2. What are the main challenges of cyberterrorism?
3. What are the most important ways and mechanisms to achieve and enhance cybersecurity?

2.2. Hypothesis of the study: The rise of cyber threats and cyberattacks poses a real challenge to Iraqi national security. Therefore, it is necessary to adopt coordinated and organized effective means and mechanisms to enhance its capabilities in the field of cybersecurity.

2.3. Objectives of the study: The study aims to identify and understand the challenges of Iraqi national security in confronting cyberterrorism and work to provide the most important ways to enhance cybersecurity in Iraq.

2.4. Methodology of Research: To understand the research hypothesis and answer the questions raised in the problem, we relied on the systems analysis and inductive approaches.

2.5. Significance of the study: The importance of the study comes from the recognition to identify the most significant challenges to Iraqi national security, as cyber risks spread to the security and safety of countries worldwide, with researching appropriate solutions to address and contain these risks.

2.6. Limitations of the study: The spatial limitations of the study are limited to Iraq, while the temporal limitations are limited to the period from the occupation of Iraq in 2003 until now.

2.7. Structures of the study: The study was divided into three topics, as well as the introduction and conclusion; the first researched what Iraqi national security is, the second researched the challenges of cyberterrorism on national security, and the third researched ways to enhance Iraqi cybersecurity.

3. Theoretical framework:

Technological development has led to the growth of cybercrimes across borders through the poor use of technology, the internet, and modern technologies, which have produced cyber risks and real crimes that increase the dominance of information and communications technology over life. These crimes are represented in the erection, fraud, and theft of funds, data, and information belonging to the political system or person, as well as planning terrorist operations and promoting false news, this is more common in the digital world.

3.1 cybersecurity

Cybersecurity is defined as the security of information systems, networks, information, connected devices, and data, an area related to the protection procedures, measures, and standards to be adopted and adhered to to counter threats and prevent and mitigate breaches. Therefore, Frichard Kammer defined cybersecurity as "reducing the risk of attacking software, computers or networks, and these include tools used to counter hacking, detecting and stopping viruses... etc.". According to the International Telecommunications Union, it is a set of tasks used to manage risk, namely the compilation of methods, policies, security procedures, guidelines, and approaches used in risk management, as well as techniques and best practices that can be used to protect cyber architecture, institutions and users from aggressors and hackers, through the development of a set of plans adapted to the technical, human, regulatory and legal environment. (Zarrouqa, 2019, pp. 1021-1022).

There are several main ways that cybersecurity, in general, is threatened (Al-Aoudi, 2022, pp. 8-9):

1. Denial of Service: This is through the launch of large requests against a website in a way that exceeds the ability of the device or site to process or respond to them, which partially or completely stops it and slows its operation in a way that harms the user. This is considered a computer attack to disrupt the objective of providing the usual services. This is usually against websites, banks, and institutions to affect them and take a physical ransom.

2. Modification or destruction of information: By accessing the victim's information through the Internet or private network, important data is modified without the victim's knowledge, as it remains present but is shaded and often results in disaster-like outcomes if military plans or secret maps are made.

3. Network espionage: Illegal or unauthorized access to the victim's network, but without destroying, destroying, or making changes to data, the aim is to obtain information often related to the national security and national security of the target country.

4. Destruction of Information: This way, information and data on networks are destroyed and deleted completely; this is called a content integrity threat and means changing data by deletion or destruction.

As for the most important types of cybersecurity threats, they are as follows (Cisco, 2023):

1. Malware: A type of program designed for unauthorized access to a computer or causing damage to it.

2. Phishing: The process of sending a fraudulent e-mail message similar to a reliable e-mail message, the goal of which is often to steal sensitive information such as login information and credit card numbers. This type is the most common type of electronic attack.

3. Ransomware: A type of malicious software designed to extort people financially by preventing access to files or the computer system until the ransom is paid.

4. Deception using social engineering: "Social engineering" represents a method used by the adversary to lure the target person to reveal private or sensitive information. The adversary can request a cash payment or access confidential data through this. "Social engineering" can also be combined with Any of the previously mentioned threats to increase the chance of clicking and entering electronic links, downloading unknown programs that may be harmful, or trusting a malicious source.

Cybersecurity has contributed, through many interaction mechanisms, to changing the boundaries of space and time, as well as the rules of democratic debate, and creating a distinct space characterized by the following (Qasimi, 2016, pp. 69-70):

1. Reshaping the boundaries between private and public.
2. New forms of social action.
3. Forms that appear in users' expressive methods, such as images, texts, and videos.
4. Individuals in cyberspace have become an audience that creates content, and the production of speeches is no longer the monopoly of a specific elite.
5. A new group of bloggers and page moderators on Facebook, controlling and managing the discussion.

3.2 cyberspace

Cyberspace is a virtual field created by humans that relies in its work on the computer system and the Internet in particular, and a huge amount of information, data, and devices in general. It serves as the basic arm of the modern army, and the French Agency for Media Systems Security (ANSS) defined it as "the communication space formed by... Global interconnection of automated processing equipment for digital data." The International Telecommunication Union" describes cyberspace as a material and non-material field resulting from elements represented in computers, software, networks, information computing, control data, and transmission. Therefore, cyberspace is an environment of modern interactions that include physical elements. An intangible group of digital devices, network systems, software, operators, and users (Zarrouqa, 2019, p. 1017).

Cyberspace is related to cybernetics, which represents the science that studies how information flows and monitors it among people, within social and economic systems, and automated devices. Therefore, it can be said that cyberspace is a new world that does not belong to history or geography. It is a homeland with no borders or heritage because it was built with Electronic communication and information networks. Countries rely on it in banking, military, and governmental information infrastructure in addition to public and private companies and institutions, until cyberspace today has become a vital and geo-strategic field that is relied upon even in wars and digital attacks. The issue of understanding depends on the nature of countries' awareness and understanding of their national security (Farhat, 2019, pp. 90-91).

The cyber virtual space consists of the following elements (Qasimi, 2016, p. 68):

1. Data on the social phenomenon via the Internet, interaction and communication in its various natural forms between people, in modern and traditional institutions and systems such as law, trade, administration, society, etc.

2. The Internet is the new digitized society and cyberspace with endless openness and characteristics with unlimited qualities and directions.

3. The individual user of the Internet, his virtual characteristics and forms of appearance, and the emergence of new electronic human personalities.

4. The electronic mind as a group for the interaction of virtual individual minds, with a comprehensive orientation to the information movement within the electronic network in a way that works towards an integrated embodiment of the electronic village.

3.3 cyberterrorism

"According to The Global Terrorism Database (GTD, 2015), terrorism (in general) is: an intentional act of violence or threat of violence by a non-state actor to achieve a certain goal through actions, including the use of violence, or to carry out a threat involving coercion that is contrary to international law". (Mohammed Torki Bani Salameh, 2022, p. 642)

The use of the term cyberterrorism goes back to the writer "Collin Barry" in the 1980s (Ismail, 2020, p. 281), who defined it as every electronic attack whose purpose is to threaten the governments of countries in particular and attack them and to seek to achieve religious, political, and ideological goals, and this attack has destructive effects similarly. Terrorism, which uses modern technological methods that include technical capabilities based on information networks to intimidate members of society, threaten them, and inflict actual harm on them through the use of modern methods represented by information resources and electronic means, so the goal of electronic terrorism revolves around electronic systems and information infrastructure (Al-Aoudi, 2022, pp. 5-6).

Cyberterrorism is also defined as any act that undermines or impairs the functions and capabilities of the Internet for political or national purposes by exploiting the vulnerability to manipulate the system to steal information, breach its confidentiality, modify it, or prevent access to it (Al-Bahi, 2018, p. 209).

With the IT revolution, various terrorist groups quickly owned websites, especially social networks. They may have more than locations and in more than languages. For example, the terrorist "ISIS" worked to support its cyber capabilities by integrating its cyber army (e.g., the Caliphate's cyber army. ghost caliphate, and the army of the Caliphate Klachinkov Cybersecurity) and he called this (United Cyber Caliphate Pirate Group). It was able to hack and disrupt some of the websites and spread its extreme publicity. Such as the Malaysian police site, the UK Ministry of Health location, US Central Military Command... etc (Al-Aoudi, 2022, pp. 3-4).

Cyberterrorism is quick and easy to implement. It facilitates the agreement, meeting, and implementation over information networks and the ease of gathering advocates for them by publishing their ideas and principles on websites, rooms, and online forums. Therefore, computer networks are used to disrupt and destroy national infrastructures, such as transportation and energy, government systems, and public institutions, and intimidate civilians and the government (Al-Aoudi, 2022, pp. 6-7).

2. Challenges of cyber terrorism to national security

Cyberterrorism is one of the most powerful types of terrorism that poses a threat to the national security of countries. Terrorist cyber attacks are increasing day after day, generating many security, political and social problems. Cyberterrorism attacks take many forms, including (Al-Bahi, 2018, p. 209):

1. Confidential Cyber Attacks: It is one of the most important types of high-tech espionage, often carried out by criminal groups. This is where it is difficult to respond to these attacks with a devastating and overwhelming attack, no matter how much it has to do with national security due to its confidentiality. At the same time, a large-scale response is threatened to maintain the basic pillar of deterrence and to successfully prevent the recurrence of attacks.

2. Tactical Attacks: These attacks are designed to achieve strategic and tactical objectives by sabotaging opponent-critical civil and military information systems, manipulating data within the information system, and distorting enemy awareness by spreading false information within intelligence systems or concealing specific activities that may be under surveillance.

3. Long-term attacks: These attacks aim to shut down information systems and cause devastating damage to the enemy's economy by affecting electricity or the telecommunications network.... etc., so these attacks must be deterred and prevented by all means to avoid harm.

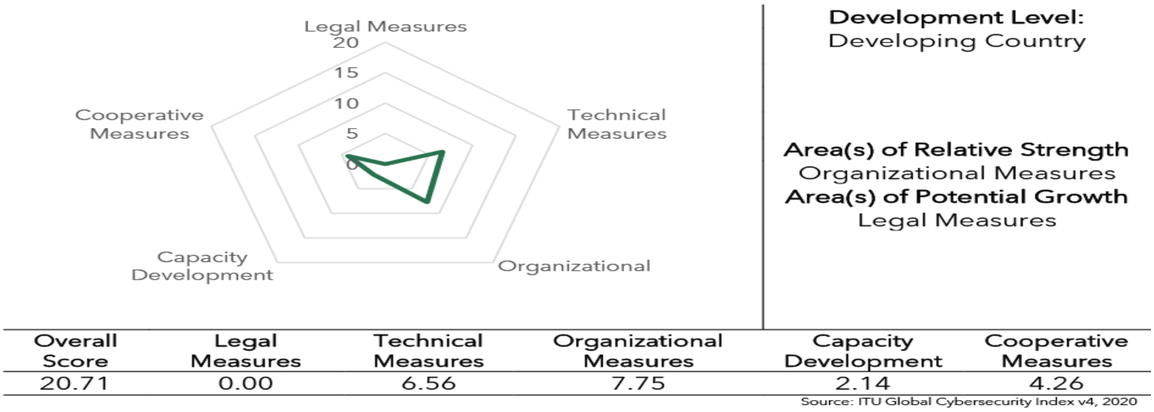
Since 2003, Iraq has witnessed remarkable progress and openness at the information and technical levels, which has made its official and unofficial institutions highly vulnerable to cyber attacks and breaches as trade and illegal routes have grown through it, which has created new challenges that have greatly affected its national security and safety system (Al-Shammari, 2021, p. 150).

Cybersecurity challenges are increasing in Iraq and the world with the development of technological means, especially with the advancement of artificial intelligence (AI). This is because the latter contributes to developing and strengthening cyberattacks and makes them more advanced and complex; simultaneously, it can be used to increase cybersecurity capabilities. Facing these threats, on the other hand, is a double-edged sword (Arabia, 2023).

With the increasing number of devices connected to the Internet system (the so-called Internet of Things), the security of these devices becomes a very important issue, and given the issue of negative issues, attackers can exploit artificial intelligence technology to modernize and develop more complex attacks, and this technology can also allow them to use techniques and means Machine learning to analyze and organize data and discover unusual patterns and vulnerabilities in cyber systems, which makes it difficult to know and detect attacks due to the complexity and sophistication of the methods used (Arabia, 2023).

According to the International Telecommunications Union of the United Nations, published in Geneva (Switzerland) in 2023, Iraq ranked in the late places globally and Arab, ranking (129) globally out of (182) countries and ranking (17) out of (22) Arab countries, with (20.71) degrees. This indicator shows (82) questions about the cybersecurity obligations of the member states across five pillars: The legal, technical, organizational, and capacity development measures, as well as the cooperation. Iraq's measures were substandard, with a score of (0) in terms of legal measures and low scores at the level of the rest of the measures (2023, 2023), as shown in the figure below.

Figures: (Explains Iraq's indicators in the field of cybersecurity)



Development Level:
Developing Country

Area(s) of Relative Strength
Organizational Measures
Area(s) of Potential Growth
Legal Measures

Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
20.71	0.00	6.56	7.75	2.14	4.26

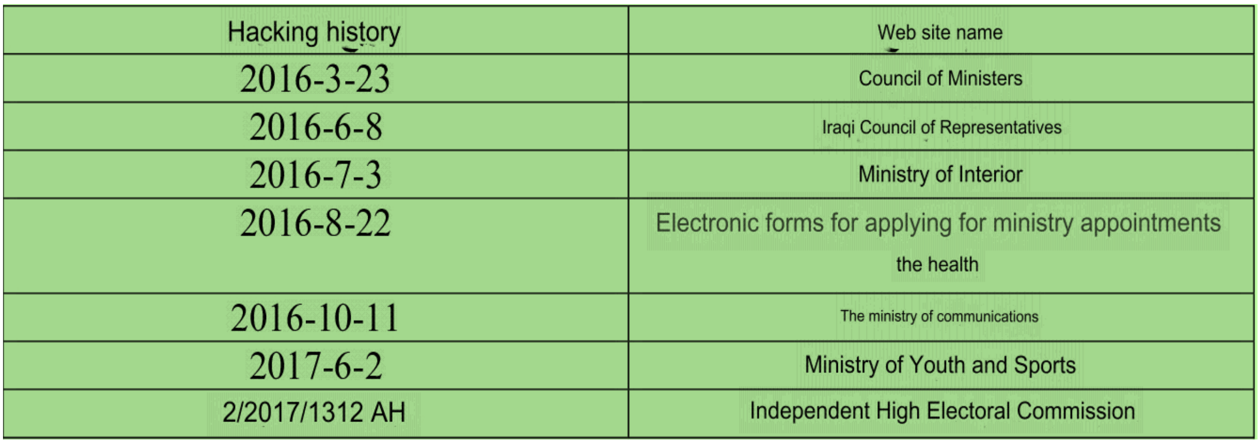
Source: ITU Global Cybersecurity Index v4, 2020

Source: (2023, 2023)

Therefore, it is unsurprising that Iraq has witnessed cyber security breaches of several important government institutions during the past few years. For example, on September 28, 2016, the official website of the "National Security Advisory" was hacked, and the group that hacked the site then published a "caricature" of an advisor. National Security Director "Falih Al-Fayyad," and they wrote the phrase: "You did not protect your position, so how do you maintain the security of the people?" (Ismail, 2020, pp. 279-280).

During 2016-2017, several official Iraqi websites were also subjected to cyber breaches, as shown in the table below.

Table: (Shows some of the official Iraqi websites that were hacked during the years 2016-2017)



Hacking history	Web site name
2016-3-23	Council of Ministers
2016-6-8	Iraqi Council of Representatives
2016-7-3	Ministry of Interior
2016-8-22	Electronic forms for applying for ministry appointments the health
2016-10-11	The ministry of communications
2017-6-2	Ministry of Youth and Sports
2/2017/1312 AH	Independent High Electoral Commission

Source: (Ismail, 2020, p. 280)

In late 2019, an unidentified group of hackers, “pirates”, was able to launch a major hacking campaign that affected “the official website of the cleric Muqtada al-Sadr” and some government websites, including the Prime Minister’s website, as one of the hackers claimed that he was able to seize “8 gigabytes of secret messages.” of the Ministry of Oil.” In October 2021, state agencies were able to thwart a dangerous cyber plan to rig the Iraqi parliamentary elections, as then Prime Minister “Mustafa Al-Kadhimi” revealed that this plan sought to “stir information chaos in Iraq.” In 2022, an unidentified hacker team An Iraqi carried out some cyber attacks on some Iraqi websites, such as the website of the Supreme Judicial Council, the personal website of the head of the Wisdom Movement, Ammar al-Hakim, and the websites of Afaq, Al-Ahed, and Al-Ghadeer channels (Today, 2023).

As for the year 2023, the case of the hacking that took place in the center of the capital, Baghdad, on a public screen is considered one of the most prominent cases, as the Iraqi authorities were forced at that time to stop all electronic billboards after an Iraqi hacker managed to penetrate its electronic system and broadcast a “pornographic film” in front of people in the streets. This operation is added to the record of numerous breaches on several official and unofficial Iraqi websites, reflecting the low levels of Iraqi cybersecurity (Today, 2023).

In general, many factors have contributed to the growth of cyber threats to countries and their interests, leading to the possibility of the emergence of cyber wars. These factors include the following (Klaa, 2022, pp. 299-300):

1. The widening risk of the global information infrastructure being exposed to electronic attacks has increased as the world is connected to cyberspace.

2. The state’s role as an influential actor in cyberspace has declined in light of globalization and its withdrawal from some strategic sectors in light of the growing role of multinational companies, especially those working in the technology field.

3. Increasing reliance on electronic systems in all vital state facilities has made them vulnerable to harming their interests due to aggressive electronic attacks.

4. The possibility of launching an attack at any time due to the low cost of cyberwarfare compared to traditional war, as

its implementation requires only a limited time.

5- Transforming cyber warfare into one of the tools for influencing information used at the level and stages of electronic combat and various conflicts, whether at the strategic or operational-tactical level, to negatively affect this information and its work systems.

6- Maximizing the power of states by exploiting cyberspace, creating advantages or effects in different environments, which produced the state's cyber strategy.

7- The widening risks of hostile activities practiced by states or non-state states in cyber wars, as they launch electronic attacks through the state's defensive security agencies, and may also recruit hackers to launch attacks on opponents without any official connection.

Therefore, it can be said that all cyber attacks work to disrupt security and order within societies and generate a set of risks to members of society and the security of the state, in addition to other political, social, and economic effects, which necessitate the need to develop the necessary solutions to them.

3. Ways to enhance Iraqi cybersecurity

The issue of cybersecurity concerns the individual, society, and state security. This issue has become a necessity that the National Security Service must address, as it is central to national security. Therefore, specialists in the field of national security in Iraq and the world must deal with it as a technological problem that must be solved as quickly as possible and with high accuracy. Because what cyberattacks target are the political values of the state in the first place, they are a potential threat at any time and place and result in destruction, tension, and risks, which makes this issue a matter of great importance to decision-makers in the National Security Apparatus, which requires coordinated and interconnected strategic plans. They are integrated within an appropriate legal framework, and the proper implementation of these plans will protect the state's national security and individuals, ensuring the sound development of all society (Al-Shammari, 2021, pp. 165-166).

In this context, there are many mechanisms and means that work to strengthen the investigative agencies of the national security of the countries of the world in general, and Iraq in particular, and the agencies concerned with arresting cybercrime perpetrators and thwarting their terrorist plans and operations, and among these means are the following (Asaad Tarish Abdel-Rida, 2018, pp. 180-182):

First: Technical resistance:

This method carries out its tasks by locking or encrypting important data that is transmitted over the Internet, providing an integrated security system that works to protect data and information, and creating or developing a program to detect viruses and protect the computer and not use it in the circulation of security information, and creating a difficult code to enter and maintain information.

Second: Electronic signature:

This method was used to keep pace with the increasing development in the use of communications and information technology in all activities and fields due to its importance in maintaining the security and privacy of transactions and the confidentiality of transmitted information and protecting it from any modification, identification, or even access to it from any party, where the sender and recipient are identified, and the person is verified electronically. This prevents tampering with information.

Third: Internet access technology:

The countries of the world, in general, are witnessing rapid technical development accompanied by economic, social, and security impacts, which has made them live in close interconnection through communications and information technologies and other applications that have contributed to the flow of goods, money, information, and ideas. Therefore, the security of the state, society, its institutions, and civilizations must be protected from the effects that are generated by This technical development by blocking harmful websites used by terrorist groups that incite terrorism and contribute to its spread.

Fourth: Walls of fire:

This method secures the ports through which applications obtain Internet service. These ports are determined programmatically within the operating systems or applications used. Hence, the work of firewalls acts as a filter that prevents suspicious requests from reaching any device equipped with them through policies through which network administrators determine The nature of the information to which access is permitted, that is, identifying the secure services and communications and knowing the protocols assigned to it within the network. Thus, it prevents unauthorized users from entering the network and protects public services in the event of entry and exit to and from the network, in addition to general protection from all Attacks.

Fifth: Securing user accounts and identity verification systems:

Using verification techniques, including biological verification of identity, through personality traits and the physical characteristics of the person, but the password and user name remain among the most widely used means of verifying identity, and for this method to succeed, it requires a lot of skill and conscious planning before the actual application for it to be successful. Preventing hackers from hacking and revealing their methods.

Sixth: Electronic encryption:

The encryption protection process is the most important means of achieving security functions (confidentiality, integrity, and provision of parameters). This mechanism is a technology included in the various technical means intended to achieve the protection of elements by protecting and ensuring the confidentiality of information through encryption and coding of all files and data and encryption of passwords and means of installation, which is what it relies on. Content protection and safety policy through data encryption to prevent hacking, modification, change, or eavesdropping and spying.

The Iraqi National Security Service has developed its vision to protect cybersecurity, and this vision came to meet Iraq's priorities and aspirations to enhance the protection of operational and technical systems and sensitive infrastructure and to increase the ability to confront all cyber threats and limit their negatives and damages, as well as to enhance the confidence of national institutions, individuals and investors in cyberspace. Iraq and contribute to Iraq's economic and social growth, and the Iraqi National Security Service has developed a national road map that includes coordinated mechanisms within an executive framework to achieve its vision and goals related to cybersecurity, including (National Security Advisory):

1. Develop comprehensive legislation to surround and combat cybercrimes by taking countermeasures for all cyber threats to national, social, regional, and global security relevant to securing the country's cyberspace.

2. Protecting vital information infrastructure by developing thoughtful measures to reduce national vulnerabilities and gaps within the cybersecurity framework.

3. Providing effective mechanisms to respond to emergencies in all electronic devices.

4. Improving and developing the capabilities of the emergency response team in computers inside Iraq.

5. Achieving an effective and rapid response to cyber-attacks through capacity building, public awareness, empowerment, and skills.

6. Coordinating cybersecurity in a way that includes all levels of government within Iraq.

7. Establishing reliable national mechanisms to involve stakeholders, national and international, to collectively address cyber attacks.

8. Working to create departments with university curricula concerned with cybersecurity, digital forensics, and methods of proving and investigating information crimes.

9. Employing cybersecurity graduates in state institutions.

10. Monitoring the correct implementation of mechanisms and plans in a way that serves national and cyber security.

To confront cyber attacks, whether hacking or espionage etc., Iraq took the initiative to work with its international partners to develop and improve cyber security performance and benefit from their expertise. For example, it coordinated with the North Atlantic Treaty Organization (NATO) to train workers in the team. Responding to cyber events in 2016. The program included practical laboratory and theoretical training sessions on the basics of cyber defense, protecting all data from hacking, leakage, and code analysis, as well as electronic evidence, and raising the level of technical expertise to protect the national network and preserve the state's national security by limiting these attacks and reducing their damage and risks on society and the state (Al-Shammari, 2021, p. 173).

One of the matters that must be dealt with extreme caution by Iraqi individuals or institutions is what can be called “social engineering” or “the art of hacking minds,” which means “a set of techniques used to make people do something or divulge confidential information.” Social engineering is Sometimes used within Internet fraud to achieve the desired goal of the victim, as the primary goal of social engineering is to ask simple or trivial questions (by phone or e-mail while impersonating an authority figure or someone with a job that allows him to ask such questions without raising suspicion)” (Service).

In this regard, the Iraqi National Intelligence Service provided some observations and instructions to people and workers in the private and public sectors to avoid the dangers of “social engineering,” which are: (Service):

1. Do not try to trust anyone anonymous: The Internet is not a place to receive gifts or invitations, as no one seeks to give you something for free.

2. Avoid opening any anonymous link sent to you via email, especially if it appears to be from your bank or any other financial institution. If you think the message appears correct, login to the sender's website instead of using the link in the message sent.

3. It is necessary to ensure that all applications and programs are constantly updated, with the need to use the best browsers, such as Firefox and Google Chrome.

4. Do not provide any information about yourself or your organization, whether confidential or not, over the phone, the Internet, or even in person unless you can verify the identity of the person requesting the information.

5. Always remember that the original providers of your information technology and financial services will not attempt to request your passwords or other information via your phone or personal computer.

6. The phone or computer must be set up to lock after a short period of not being used, and it must be set up with a strong password.

7. It is necessary to be careful when trying to install and use applications, especially those permissions that they request during the installation process, as it is unreasonable for a weather application, for example, to ask you for permission to access your stored images.

8. It is necessary to verify the files and programs downloaded from the Internet, with the importance of asking about the site from which they are downloaded. While there are many reliable sites, there are, on the other hand, thousands of fake sites with harmful content and malicious programs specifically designed to steal personal data and banking for users.

9. Anti-virus protection programs must be constantly updated, and these programs must be downloaded from the official websites of their makers. If you cannot purchase these programs, there are many free applications in this regard, such as AVIRA, AVAST, etc.

10. Do not trust free technical programs of unknown origin, as they often have a price, so it is recommended to read all notes and agreements while installing programs and not to download or upload them from an unknown or suspicious source.

11. You must use constantly updated software browsers, as security vulnerabilities and breaches are an infection or disease that is increasing daily.

In addition to the above, there are several requirements and priorities that Iraqi National Security must take into account to achieve and protect cybersecurity, which can be summarized as follows (Al-Kuwaiti, 2023):

1. Cybersecurity awareness: In light of the spread of cybersecurity threats on a large scale, national security efforts must invest in training and educational programs for citizens and workers in state institutions and the private sector about protecting sensitive data to prevent unwanted access to networks and information systems.

2. Cybersecurity Governance and Risk Management: Here, the various threats to a country must be identified while maintaining an inventory of all assets of industrial control systems, from supporting hardware, technology, and software to the development of cybersecurity policies, programs, training, and educational guidance that apply to industrial control systems, and the development and practice of incident response procedures that integrate IT and operational technology.

3. Establishing new legal rules and legislation: The significant growth in the level of cyber attacks and threats requires the necessity of continuing to prepare new legislation and legal regulations to achieve and ensure cyber security

requirements, as well as keeping pace with the increasing developments in the field of cyber security threats.

4. Strengthening capacity development measures: According to estimates by the World Economic Forum, about one million people access the Internet for the first time every day, and two-thirds of the world's population owns a mobile device. While digital technology brings enormous economic and societal benefits, cyber risks can offset the benefits of digitization, so securing cyberspace through capacity-building activities in cybersecurity is important, as it will contribute to reducing technical problems such as the digital divide and cyber risks (2023, 2023).

5- International cooperation: Effective cyber deterrence requires broad programs and plans of defensive and offensive cyber capabilities, supported by an effective international legal framework, with the ability to attribute a cyber attack to an attacker without a doubt. One of the main issues for international legal coordination and cooperation is facilitating the prosecution of cybercrime perpetrators.

In general, the issue of the complexities of modern cybersecurity requires the speed and necessity of cooperation between the various security agencies concerned, especially the national security agencies of countries, to combat electronic threats to which countries and individuals alike may be exposed. Collective international action represents the best way to reach the results desired to confront and combat cybersecurity risks and threats. In other words, it is necessary to build a strong cybersecurity alliance in which various countries, organizations, and multilateral companies participate, as the human element still represents the weakest link in this field, as some research in this field revealed that 88% of Security breaches may occur as a result of human errors. Therefore, a top priority must be given to raising cybersecurity awareness, enhancing educational and training programs intended for users and specialists, and improving the security culture within government institutions and private companies. Focus must also be placed on strengthening and supporting young people's cybersecurity capabilities, as it is one of the main components necessary for business development. In light of the increasing demand and reliance on digital technologies (2023, 2023).

4. Conclusion:

The technological and information development that the world is witnessing today has led to the dominance of open space and the dismantling of spatial boundaries in light of the absence of centralization responsible for organizing power within cyberspace and the presence of gaps in information security, which has made society subject to many digital threats. Therefore, it is necessary to find Urgent and deliberate mechanisms to preserve the security of society and the national security of the state from aggressive actions and espionage carried out by terrorist groups and the poor use of communications and information technology.

The study was able to answer its questions, in addition to that it was able to test the hypothesis and achieve its aims as well.

4.1 Results:

- Iraq's measures in enhancing cybersecurity are still below the required level, especially at the level of national legislation.
- The existence of a national cybersecurity strategy represents the first positive step to improving Iraqi national cybersecurity, but there is a need for regular updates and reviews of that strategy.
- The technical-informational openness in Iraq since 2003 has made governmental and non-governmental institutions vulnerable to cyber breaches and attacks, resulting in challenges and breaches that negatively affected its security system and national integrity.
- The presence of effective mechanisms and institutional structures at the Iraqi national level is necessary to deal with cyber risks and incidents.

4.1 Recommendations:

- It is necessary to find and develop a legal and regulatory framework to protect society and promote a safe digital environment so that this must be at the forefront of any national efforts in the field of cybersecurity.
- Developing legislation that defines illegal activities in cyberspace.

- The necessity of taking regulatory measures that address cybersecurity at the highest level by the Iraqi executive authority, assigning relevant roles and responsibilities to various national entities and making them responsible for the national cybersecurity situation, including ensuring the sustainability of Iraqi cybersecurity.
- It is necessary to develop capabilities in the field of cybersecurity in order to enhance and develop processes, skills, resources, and research aimed at strengthening national capabilities.
- The capabilities of Iraqi cybersecurity specialists must be strengthened at the level of collective governmental and non-governmental capabilities.
- The need to activate and facilitate international cooperation and partnerships to effectively respond to digital security challenges related to Iraqi cybersecurity.
- The need to increase effective cybersecurity awareness to keep citizens, companies, governments, youth, and organizations prepared and alert to the risks of terrorism and cyber targeting.
- Governments must ensure that all users are aware of the risks they may face while carrying out digital activities, as this constitutes citizen protection and support for government efforts in enhancing efforts to achieve effective cybersecurity.

REFERENCES

Al-Aoudi, J. F. (2022). *The Impact of the Cyber Terrorist on National Security.*

Al-Bahi, R. (2018). Cyber deterrence: concept, problems, and requirements. *Journal of Media Studies - Arab Democratic Center,* (1).

Al-Kuwaiti, M. (2023). *Cybersecurity in 2023: Transformations and Challenges of the Age of Artificial Intelligence.* Retrieved from Trends Research and Consulting: https://marsaddaily.com/Article_Detail.aspx?authorid=6&Articleid=409

Al-Shammari, M. I. (2021). Cybersecurity and its impact on Iraqi national security. *Journal of Legal and Political Sciences,* (1).

Arabia, S. N. (2023, 8 20). *What are the most prominent cybersecurity challenges with the advancement of artificial intelligence?* Retrieved from Sky News Arabia: https://www.skynewsarabia.com/business/1646519

Asaad Tarish Abdel-Rida, A. I. M. (2018). cybersecurity and its role in the spread of the phenomenon of terrorism in Iraq after 2003. *Journal of International Studies,* (80).

Cisco. (2023). *What is Cybersecurity.* Retrieved from Cisco: https://www.cisco.com/c/ar_ae/products/security/what-is-cybersecurity.html.

Global Cybersecurity Index 2020. (2023). Retrieved from ITU: https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

Farhat, A. (2019). Cyberspace: Shaping the Battlefield in the 21st Century. *Journal of Legal and Political Sciences,* (3).

Ismail, S. M.S.Z. (2020). Cybersecurity as a New Foundation in the Iraqi Strategy. *Political Issues Magazine,* (62).

Klaa, S. (2022). Cybersecurity and the challenges of espionage and electronic intrusions of countries through cyberspace. *Journal of Law, Science and Humanity,* (1).

Mohammed Torki Bani Salameh, I. H. (2022). The Impact of Terrorism on Tourism: Pilot Study 2007–2017: Case Study of Jordan, Egypt, Spain and France. *Dirasat: Human and Social Sciences,* (49), 642.

National Security Advisory, S. (n.d). *Iraqi Cybersecurity Strategy.* Retrieved from https://www.itu.int/en/ITUD/Cybersecurity/Documents/National_Strategies_Repository/00056_06_iraqi-cybersecurity-strategy.pdf

Qasimi, S. (2016). *Cyberspace and the Electronic Valley: The Problem of Creating a Virtual Public Space according to the Habermasian Perspective.* Algeria: Dar Al-Manduma.

Service, I. N. (n.d.). *Information Security Tips.* Retrieved 10 28, 2023

Today, B. (2023). *A review of global hacking cases carried out by Iraqi hackers.. Why is piracy active in Iraq?* Retrieved from Baghdad Today: https://baghdadtoday.news/22988

Zarrouqa, I. (2019). Cyberspace and the Transformation in Concepts of Power and Conflict. *Journal of Legal and Political Sciences, 1*.