Sys Rev Pharm 2020;11(12):469-476
A multifaceted review journal in the field of pharmacy

Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study

Lect. Asmaa Khalid Jarjees Al-Tae, Ass. Prof. Hameeda Abdul-Hussain Al-Dhalimi[1], Prof. Adnan Kadhum Jabbar Al-Shaibani[1]

College of Education for Humanities, University of Mosul, Iraq.
[1]College of Education for Humanities, Al-Muthanna University, Iraq.
Email: a_alshabani@yahoo.com

ABSTRACT

Cyberspace is the fourth area of the state in addition to the third areas, air, land, and sea. The issue of his protection and defense has become a concern of many decision makers in the country because of his connection to national security, the challenge posed by cyberspace is a major challenge, represented by the dangers surrounding this use on state institutions and individuals, because of the large increase in the number of dealers with the computer, the diversity of their uses and their workplaces, and their different cultures, their goals and affiliation. In addition to the expansion in the use of the international information network on the Internet. Cyber insecurity and its vulnerability to persistent hacking, an effective tool capable of contributing to the destruction of the state politically, security, socially and economically in light of the development of technologies, methods of penetration are in continuous development and at the same time their negative impact is greatly increasing, which threatens the national security of the state. Thus, states should seriously consider finding defensive means to verify cybersecurity, until stability is achieved at all levels. Iraq entered the cyberspace strongly, especially after 2003, due to the expansion in the use of smart mobile devices and computers, but still lacks how he handles quick entry, as a result, cybersecurity in Iraq has become permanently compromised. It can be inferred that the Iraqi ministries have been compromised, Iraq lags behind in the global cybersecurity index, ranked 107th internationally in 2018, the lack of relationship between the Ministry of Communications, which is supposed to be concerned with cyberspace, and other ministries. All these facts strongly indicate the necessity of adopting realistic solutions to achieve cybersecurity.

Keywords: Cybersecurity, National Security, Iraq Case Study

Correspondence:
Prof. Adnan Kadhum Jabbar Al-Shaibani
College of Education for Humanities, Al-Muthanna University, Iraq.
Email: a_alshabani@yahoo.com

INTRODUCTION

The expansion has led to the use of the information revolution and the associated precision devices, to change many concepts related to the state, sovereignty and security. Cyberspace has become of great importance, whether in the military, financial, and administrative fields ..... etc. So it has become the most prominent characteristic of modern life and cannot be dispensed with in any way. Despite cyberspace, it was found to serve man and his welfare, however, it carries a lot of risks to state institutions and individuals alike, which threatens the security and stability of the state at all levels, especially since those risks differ in nature from the traditional risks, it has necessitated the many dangers posed by cyberspace. Countries take a set of measures and measures to protect their cybersecurity, infrastructure was protected from malware called cybersecurity. Many developed and even developing countries have begun to establish supreme bodies and councils concerned with cybersecurity. Strategies were taken place that aim to explain how its cyberspace can be secured. The correlation is clear between cybersecurity and the nation's national security.

Based on the foregoing, researchers took from (Relationship of cybersecurity and the national security of the state: Iraq case study), a topic for research with the intent to unveil the relationship between cybersecurity as a new concept that has great dangers and the nation's national security, Iraq taking a case study to identify the challenges facing cybersecurity, highlight the most important ways to secure, for the purpose of studying the subject with a scientific methodology, the researchers divided the research into two main requirements preceded by a general introduction. The first requirement focused on the relationship between cybersecurity and the nation's national security, while the second requirement addressed cybersecurity in Iraq, challenges of reality and solutions. The research concluded with a set of results and a list of sources adopted by the research.

The first requirement: the relationship between cyber security and the national security of the state

First: theoretical rooting for cyber security:

Cyberspace is the origin of cyberspace from the Greek word (CYBER NETICS), means the guide, ruler, or captain, Nurburt was the first to use this term in the early 1940's, whereas the English dictionary (CYBER NETICS) has translated as cybernetics, automatic control, or cybernetics, and communication, as for the United Nations, it has been translated Saber. This word became popular in the early nineties and specifically since 1990, when the use of the Internet, networks and digital communications increased dramatically, the term cyberspace was able to represent many new ideas and phenomena that appeared at that time (1). Cyberspace was defined by many definitions, it is the field characterized by the use of electronics and the electromagnetic field, to store, modify or change data via connected systems, associated with natural infrastructure, includes the process of merging between the Internet and mobile devices, communications and satellites (2).

The Oxford Dictionary defines cyberspace as the virtual environment, through which communication is completed via computer networks, also known as the metaphorical field for them computer data and electronic networks, where the information is stored electronically and direct communications are made on the network, so

it is an intangible world that includes topics such as personal information, electronic transactions, intellectual property and other related topics (3).

As for the International Organization for Standardization and Metrology, it made its role regarding the definition of cyberspace, defined him as a complex environment resulting from the interaction between people, software and services on the Internet, through technology devices and networks connected to it that are not found in any physical form (4).

We move away from the many views in the definition of cyberspace, we'll get to the definition of the International Telecommunication Union, because all the adopted definitions were launched from it, cyberspace has been defined as the tangible and intangible space that arises or consists of a group of parts that include computers, network equipment and mechanization, computerized information, software, content, and audit data (5).

Second: relationship of cybersecurity and the national security of the state:

Cyberspace represents the sum of computer networks in the world and all that is connected to them and directly controls these networks. It includes the Internet and other computer networks that are indirectly connected, or networks that cannot be accessed online, they were similar to the Internet but separate from it. Cyberspace also includes commercial networks, it performs certain tasks such as data on financial flows, financial transactions in the markets, and credit card transactions, some of these networks have the same control system, allow devices to address other devices such as control panels that address pumps, generators, and elevators (6).

The risks of cyberattacks have become one of the most important systemic risks, facing economic, financial and military systems, because of increasing global technological convergence, which led to the dissipation of physical or digital separations between countries of the world, for example, and not limited to, the World Economic Forum (WEF) mentioned in its report on international risks, increased fears of technology risks, especially cyberattacks and data distortion, these risks appeared in the list of the top five potential international risks in 2018, likewise, cyber threats have topped the global list of risks to the global financial system in 2018 and beyond. According to a poll conducted by a number of other international bodies such as the Bank of England and the American DTCC, at 2017, the intensity and severity of malicious cyberattacks have increased recently, except from the side of proliferation or its ability to destroy and harm economic institutions, the number of cyber breakthroughs recorded in the global business sector has doubled over the past five years, from (68) breakthroughs for each mentor for each facility in 2012 to (130) breakthroughs in 2017, besides, the malware market has again returned, after being tightened down with the force of law, it released about 357 million varieties of different types of malware in 2016, the price of the malware used to steal bank account data has decreased to about (500) dollars per program. Cyber Criminals have also multiplied the number of victims targeted by cyber criminals, thanks to the higher usage of Cloud Services, the Internet of things expanded, from about (8.4) billion devices used in 2017 to about (20.4) billion devices by 2020, even the cyberattacks, which were previously considered huge, have become very ordinary today. The global corporate sector revealed in 2016 more than (4) billion cases of data records breach, more than twice the sum of breakthroughs in the past two years, deprivation of Distributed Denial of Services globally increased by 140% in 2016 alone. The financial cost of cyberattacks increased, as one of the global studies conducted in 2017 estimated (254) companies in seven international countries, the average cost of dealing with these attacks in one company has reached (11.7) million euros, with an annual increase of (27.4%), it was expected that the cost of electronic crime in the business sector will increase within the next five years to about (8) trillion dollars. The Council of American Economic Advisors has estimated the amount of losses resulting from malicious cyber activities in the United States of America in 2016 at an amount ranging from (57 - 109) billion dollars (7).

These facts show that the world is in a new kind of war, it was the cyber warfare that is inside the internet and the digital medium, don't need massive amounts of resources like weapons and equipment, armies, money, only need limited people who are distinguished by the ability to cause damage to systems or penetration of systems of remote devices using the Internet or other communication networks, therefore, it can be that the orientation of states towards this war is the end of conventional wars and the beginning of new wars that will be witnessed in the near future, the subject of the research requires a reference to the definition of electronic (cyber) war, known several definitions, including the penetration of computer networks in one country by another country, and this breach is not authorized by or on behalf of or on behalf of a government, or any other activity that affects the computer system, for the purpose of adding, changing or falsifying data, or causing a computer device to be damaged, damaged, disabled, or damaged by a device connected to a network or things controlled by the computer system, this definition must be the computer that was attacked by a state computer, also, the perpetrator of the attack must be another country or a body on its behalf or supportive of it, in addition to this definition, electronic espionage excludes from the purposes for which the attack was carried out. Paul Robinson has called cyber warfare several names, including digital warfare, electronic warfare, email warfare, or virtual warfare, adding that the Internet war is the most direct and simple of these designations, because it is a war over the Internet, defined as a war and it is being waged through the computer and the internet, includes both offensive measures to damage opponent information systems and defensive systems to protect the attacker's systems to protect their systems from being attacked (8).

Interferes with the concept of cyber warfare, intended to use deliberate activities to change, spoil, deceive, multiply, or destroy computer systems or computer networks of opponents, information, or programs included in these systems and networks or send through them, these activities may also affect entities associated with these systems and networks, cyberattack may be used to prevent authorized users from accessing a computer, services, or information service (denial of service attack), or to destroy computer-controlled machines or to destroy or change vital data such as (use schedules for military logistical operations), the direct effects of a cyberattack (computer damage) are less important than indirect effects (damage to the system to which the computer is attached) (9).

In 2007 the US Strategic Command knew cyberattacks, adapt computer system operations to prevent opponents

from actually using them, as well as infiltration into information systems and communication networks in order to collect, possess and analyze the data they contain (10).

Cyberattacks can be defined as an act that undermines the capabilities of computer network functions, for a national or political purpose, by exploiting a weakness, the attacker can manipulate the system (11).

The risks to cyberspace can be listed as follows (12):

First: breach of physical protection

This will be by one of the following means:

1. Inspection (Dumpster diving) in the technical waste, which means the days of the attacker searching for the establishment's waste from garbage and materials expected in search of anything that might help in penetrating the system.
2. Wiretapping, which means physical connection to the network and then penetration of the system.
3. Eavesdropping on Emanation, using technical patches to collect the waves emitted from the system of different types.
4. Denial or degradation of Serice, meaning material damage to the system to prevent service provision.

Second: Violating the protection related to people or personnel affairs

This shall be done through one of the following means:

1. Concealment of impersonating the powers of an authorized person (Masquerading), and here the unauthorized access to the system is through the use of other user identification methods.
2. Social Engineering refers to activities for obtaining information that prepares intrusions through social relationships.
3. Harassment, which is a threat that includes many forms of aggression and methods, and combines the transmission of messages, harassment and harassment.
4. Software piracy (Soft war Piracy) by using it without permission or using it financially without permission or copying and simulating.

Third: Protection breach related to communications and data

This is as follows:

1. Data attacks, which include:

A. Unauthorized Copying of Data, which is a common process that often comes after unauthorized entry into the system.

B. Traffic Analysis, which is an attack focused on studying the system's performance at the dealing stage and following up on communications and connections that are used to determine the behavior of users and identify weaknesses at the appropriate attack time.

C. Covert Channals, which is one of the attacks of the storage unit, where the intruders conceal data, software, or information that they seized. They had credit cards in a specific matter of the system.

2. Software Attacks:

A. Trap Doors, which means a loophole that is implemented in a program that allows the hacker to gain access to the system.

B. Theft, misappropriation of information, and instant use (Session Hijacking) means that the person exploits a legitimate use by someone other than the system, so he steals the view, or he may use the system when he has the opportunity.

C. Attacks The muscles of the data transfer players are the tunneling energy.

D- Timing Atctaks are attacks in which sophisticated technology is used to gain unauthorized access to programs or data.

E. Malicious Code, which is malicious software that is used to destroy whether to destroy the system, software, data, or files.

3. Attacks and risks related to protection operations:

A. Did Data Diddling means attacking by changing or modifying data or creating fake data whether it is in the input or output stages.

B. IP Spoofing, which means deception, fraud, or delusion, but the common use now is related to Internet virus attacks.

C- Scanning and used specifically regarding the possibilities of a password, modem phone number, or the like.

D. Passwords collected and captured (Password Sniffing).

E. Excess Privileges.

The most prominent harmful malware that is used as a weapon in cyberspace is as follows (13):

1. Viruses:

Viruses dating back to the beginning of the seventies of the last century, and the virus is an application program but it is distinguished from other programs that it was designed by one of the saboteurs and aims to cause certain damage to the computer system.

2. Worms:

It is a standalone program and has a file of its own. The worm is an integrated application program that can work on its own and does not need to add itself to another file as is the case in viruses. It can also work on its own and carry itself to the computer's memory and start working automatically.

3. Trojan horse:

They are destructive programs disguised as useful programs that are desirable by information technology users, but when these viruses are implemented or run, they destroy and erase data and in many cases they work as a means to steal data, that is, they provide access to data by unauthorized people.

There is a growing crime of attacking information and data systems, whose consequences have become more dangerous, especially when it affects human lives, especially in cases of attacks on hospital information systems, medical research laboratories and airports, security concerns have become more acute, the severity of the issues related to it has grown to the extent that it is considered a national security priority for some countries, especially the countries that dominate cyberspace, for example, in this context what the United States considered sabotaging its information network infrastructure, as a kind of mass destruction that leads the country to complete paralysis, George Tenet, the former director of the CIA, responded in an expression of the gravity of an information systems violation, the complexity of tracing offenders is saying that we have based our future on technology capabilities that we have not learned how to protect (14).

The threats facing cyberspace have compelled states to protect and secure them, find what is known as cybersecurity, which many countries took a lot of attention, known by many definitions, some were defined in the report of the International Telecommunication Union, about "Trends in Telecom Reform 2010-2011", it is a set of tasks, such as grouping methods, policies, security procedures, guidelines, risk management approaches, training, best practices, techniques, it can be used to protect cyber environment, enterprise assets, and users (15).

The World Telecommunication Union has identified several key elements of information security, it can be restricted to seven main elements: identity verification, access control, confidentiality, integrity and integrity of information, non-denial, availability and permanence of information, and follow-up or verification (16).

To the relationship between cybersecurity and national security is complete, the need to refer to the concept of national security, Amin Howaidi has known is the actions that the state takes within its capacity to preserve its existence in the future, taking into account the local, regional and international variables that may arise in the future, Robert McNamara's definition is one of the modern definitions, knows about development and its economic, social or political aspects under guaranteed protection (17).

Globalization has provided mechanisms and tools to improve communications and facilitate the movement of people, money, weapons and ideas, all of these variables had repercussions for the national security of individual nations and for international security as a whole.

The concept of national security is no longer only related to that physical entity, which relates to the protection of resources, population, and borders, and the preservation of elements of the state's strength and national capabilities, the military force has been linked to the control of four areas that comprise the ability to control land, sea, air, and outer space. Security thought was linked to the issue of defense and attack by conventional armies, or support the allies and that security was achieved through several political, economic, diplomatic, technological, and military components, those elements were related to each other as they supported each other, weakness in one of them may lead to weakness of other elements and vice versa, previously, countries were more isolated from each other, defending its national borders was an important part of protecting the elements of its national power, the cyberspace came with distinctive features and elements, to have an impact on international security and the economy (18).

National security means protecting the fundamental values of society, the absence of fear of the danger of these values being attacked, cyberspace has forced a rethink of the concept of security, that relates to the degree that enables the state to be safe from the risk of military or terrorist attack, measures to protect against exposures critical infrastructure for administrative work through misuse of communication and information technology.

National interests associated with vital infrastructure have become vulnerable to attack danger, that includes energy, communications, transportation, government services, e-commerce, banks and financial institutions, the cyberspace has made these interests interconnected in one working environment known as the national information infrastructure, any attack on one or all of those interests, represents a reason for a strategic imbalance that reveals at the same time a new form of conflict (19).

Security gave many definitions, builds on military capabilities, through maintaining system stability, to protect the fundamental values of a society, regardless of the convergence or difference of philosophical and political views on the subject, the firm is the fear that most countries now show, whoever exposes its national security, as a result of cyberattacks, especially since information and communication technologies, had raised the level of danger, by making available new sources, manifold and multiple, and enormous potentials, to achieve this risk, in exchange for a decrease in the percentage of risks and the possibilities of exposure, on the side of the aggressor, the evidence for this is the increased coordination between security and economic departments, in addition to the interconnectedness that world leaders see between Siberian space security and national security.

A former US National Security official, Michael McConnall, explained, the Internet has raised the level of threats to the system, in an unprecedented way, reference to new threats to national security, can take unexpected shapes, and cover basic and vital areas. also, the current American President, Barack Obama, announced that Siberian space security is at the forefront of his concerns, considering the threat emanating from the Siberian space, one of the most serious issues that arises at the economic level, as well as at the level of national security. has been translated into practice, with the appointment of a Siberian space security official, constant contact and coordination, shall be a member of the National Security and of the National Economic Council (20).

The effects of the conflict in cyberspace on the nation's national security can be illustrated in the following (21):

1. Cyber Conflict is characterized by destruction that is not necessarily accompanied by blood and body parts, Includes espionage, infiltration, and then blasting, but no smoke, debris, or dust, parties were characterized by lack of clarity and its repercussions are dangerous, whether by destroying, blasting, and bombing websites on the Internet with viruses or by working to use multiple cyber weapons, to undermine the integrity of those sites, weapons that are easily obtained through the Internet as well and learn to use them. The proliferation of cyberspace and easy access to it can expand the circle of site targeting in addition to increasing the number of attackers, for these mutual attacks to take place in a manner of hit-and-run to express the state of an extended conflict related to the different nature of cyberspace.
2. Cyberspace is used as a method of conflict within the state Inte – State Conflict, among its components on sectarian, economic or religious grounds, helps expose the dynamics of internal interaction to the outside, thereby facilitating the process of external penetration through communication networks by supporting a party to the conflict with non-combat tools.
3. The conflicts spread across cyberspace (It is characterized by the occurrence of frequent cases of mutual piracy) without necessarily resulting in a conventional war, especially with the rise of the "individual" role in international relations, like the case of the Arab-Israeli conflict, between Pakistan and India, between China and the United States, between China and Taiwan or Kosovo or other conflict areas.
4. The electronic conflict takes on a competitive nature over the acquisition of technological advances and theft of economic and scientific secrets, until that conflict extends to trying to gain control of the Internet, by seeking to control domain names and URLs, and control information, penetrate the national security of countries without using planes or explosives or even violating the sovereign borders, like hacker attacks, site destruction, and espionage, it has an impact on destroying the economy and infrastructure with the same strength that a devastating conventional bombing may cause.

5. Difficulty separating activity related to intelligence, information gathering, and cyberspace war, or distinguishing between political and criminal use, this ideal environment for cyberspace contributes to the work of different groups, support the ability to form a global network without direct control, in addition to the cheap cost, ease of communication and weak traditional control, this is an attraction to use and employ to achieve political and military goals.
6. There is an electronic conflict that is politically motivated and takes a military form, it uses offensive and defensive capabilities across cyberspace, this is aimed at spoiling information systems, networks, and infrastructure, including the use of electronic weapons and tools by actors within the information society or through cooperation among other powers to achieve political goals.
7. There is a soft electronic struggle by the struggle for access to information, influencing feelings and thoughts, and launching a psychological and media war, it is also by leaking information and using it through media platforms, this affects the nature of international relations, such as the role WikiLeaks played in international diplomacy.
8. Cyberspace is used to wage psychological warfare on the population
   In what affects the degree of community stability with its widespread use, increased dependence and availability to all users without discrimination, this type has an impact on the population, making them feel helpless, mistrustful in state institutions, and sheltering from traditional primary loyalties, including the beginning of the use of religion, tribe and ethnicity as drivers of the conflict, that can undermine the authority of the state and prolong the conflict.
9. The role of cyberspace has also emerged through social media networks in managing the political conflict between major technology companies and countries on the one hand, between the ruling regimes and the movements opposing them, on the other hand, perhaps the Arab Spring countries are an example of this, as a disparity has emerged in the use of cyberspace, according to the nature of technical development and the ability of the system to manage media conflict, influence public opinion, and mobilize and mobilize the public, there was a difference between the position of the Syrian regime, which conducted its battles with counter-ideas and mutual breakthroughs, while the Egyptian regime failed to use cyberspace to manage the protests crisis, especially after cutting off the internet and communications, while it did not exist in the crisis in countries that did not rise to the level of technology such as Libya and Yemen, the confrontations were more bloody by moving the hard force, not the soft force, reflected in the conflict situation, its extent and parties, and the nature of international intervention.

The second requirement: cybersecurity in Iraq, challenges of reality and solutions

First: The challenges facing cybersecurity in Iraq:

That all countries of the world have taken great care of cyberspace, because of the great effects on the state as a result of cyberattacks that affect its governmental and non-governmental institutions as well as individuals, therefore, these countries have been developing a set of visions, perceptions and laws, to secure itself from the dangers of cyberspace.

Iraq is one of these countries that entered strongly into cyberspace with great randomness, this is evidenced by the large number of electronic devices, especially the number of mobile phones that reached in 2017 (40) million lines, with a telephone density of 107.7 per 100 inhabitants, the number of mobile Internet service lines (19.2) million (22), the availability of the Internet and a large percentage of the population despite its poor quality, besides the lack of experience of the government in the process of adopting electronic governance, connect all Iraqi ministries to each other, many decision makers in Iraq, they do not realize the importance of cyberspace, and it has become a fourth dimension alongside the three dimensions, land, sea and air, which represent the sovereignty of the state.

For the purpose of demonstrating the reality of the penetration of the cyberspace in Iraq, the Digital Center in Iraq has indicated that most websites of official government ministries and institutions are not secure and can be easily hacked, intercept data being traded across these sites (23).

Evidence of the weak and possibly a lack of relationship between the Ministry of Communications and other ministries, all these data made the cyberspace of Iraq vulnerable to penetration, the Global Cybersecurity Index (GCI) released by the United Nations International Telecommunication Union, to assess the state of states in the field of cybersecurity, except clear evidence of apparent failure in this area, which indicated that Iraq advanced to the center (107) internationally in 2018, after being at the center (158) in 2017, on the Arab level, Iraq ranked 13th for the year 2018, after he was at the center (19) in 2017 (24).

The Digital Center team in Iraq was surprised, Iraq obtained this rank, although it is ahead of the year before, because he was fighting a fateful battle against a terrorist organization that used cyberspace in its war against Iraq, so Iraq was supposed to have all the tools, that improve cybersecurity plans and programs, environment was strengthened to confront the terrorist enemy who was good at working in this field.

Analysts believe that Iraq failed again to deal with the main indicators and pillars of cyber security that relate to legal measures related to cybersecurity, technical aspects, organizational issues, as well as capacity building, training and cooperation, they pointed out a fundamental point is the absence of an institution specializing in cyber security in Iraq, or the existing are sections in different departments that lack coordination or professional cooperation in this aspect, each side works alone (25).

Thus, Iraq is still reeling in late positions that are not commensurate with its financial and scientific capabilities, which requires a rapid renaissance in this field to avoid the risks posed by cyberspace.

These challenges to cybersecurity, the National Security Adviser in Iraq has initiated a cybersecurity strategy, has been published on the Internet, the Internet, a good step, however, it has many drawbacks that can be pointed out to some:

1. For every strategy when it is developed targeting a specific period, however, the Iraqi cybersecurity strategy was not limited to a period of time, as if it is valid for all times, and this matter is incorrect.
2. The clear dominance of the theoretical content in the strategy at the expense of the applied content, this indicates the fact that the authors of this strategy are not aware of the experiences of Arab or international

countries, developed cyber security strategies that are in fact numerous and available on the Internet.

3. The strategy lacked any definition of the infrastructure that was the subject of repeated targeting, for the purpose of confirming it and providing the necessary protection.
4. The strategy did not refer to the entity that is responsible for the mechanism of its implementation, satisfied with the implicit reference to the government, at the same time, did not specify the responsibilities and tasks of government agencies.
5. The strategy lacked reference to the most important strategic programs, as the strategy was not specified in time as previously stated, supposed to be available.

As is the case, for example, in the Egyptian National Strategy for Cybersecurity for the period 2017-2021 that indicated the most important strategic programs in this period are (26):

- A program to develop the appropriate legislative framework for it from cyberspace, fighting cybercrime, protecting privacy and protecting digital identity.
- Program for developing an integrated national system to protect cyberspace and secure communications and information technology infrastructure, by preparing and activating what is known as Computer Emergency Response (or Readiness) Teams (CERTs), or Computer Security Incidents Response Teams (CSIRTs) in vital sectors at the national level.
- A program to protect the digital identity, the citizen's digital program, and activate the necessary infrastructure, to support confidence in e-transactions in general and in e-government services in particular, such as the Public Key Infrastructure (PKI), the electronic signature depends and its regulation, supervised by the Information Technology Industry Development Agency.
- Program for preparing human cadres and the necessary expertise to activate the cybersecurity system in various sectors, cooperation and partnership between government agencies and the private sector in universities and civil society institutions.
- Program for supporting scientific research and developing the cyber security industry, by supporting cooperation programs and projects between research agencies and national companies, especially in the field of advanced malware analysis in the field of digital evidence analysis and in the field of industrial control systems.
- Community awareness program on the opportunities offered by electronic services for individuals, institutions and government agencies, the importance of cyber security to protect services from the risks and challenges.

Second: The solutions necessary to achieve cybersecurity in Iraq.

Cybersecurity is closely related to or linked to the national security of the state, any breach of it may destroy the state's infrastructure and expose it to many risks, therefore, we note that many countries have taken more attention to me through which cyber security is achieved despite the difficulties in achieving, not easy process, as needs the necessary political will, to design and implement a strategy to develop digital infrastructure and services that are verifiable from it, from its management, and also, cybersecurity strategy must be part of multidisciplinary approaches with ready solutions at the cultural, legal, administrative and technical levels (27).

1. Establishing a supreme body or a higher council for cyberspace, directly linked to the Council of Ministers, take charge of cyberspace directly in Iraq, protect it from any breach and provide the necessary support, connect it directly to the Iraqi Cyber Incident Response Team (CERT), benefiting from the experiences that he enjoys, which includes a number of things including monitoring and analyzing the activity outside the context, analyzing cyber risks and vulnerabilities and disseminating information related to cyber hazards, analyze and compile information related to accidents and weaknesses distributed by other agencies, including IT suppliers and technology experts; to provide an evaluation to be presented to interested stakeholders, establish reliable communication mechanisms and facilitate communication between stakeholders to share information and address issues related to cybersecurity. Provide early warning information, including information related to reducing vulnerabilities and potential problems, disseminating general cybersecurity best practices and guidelines for incident response and prevention (28).
2. Introduce and enact new laws to enhance the Iraqi cyber legal status, such as the Telecommunications and Information Security Law, the Privacy Act as well as reviewing and improving the existing Iraqi cyber laws, for addressing the dynamic nature of threats to cyber security in Iraq (29).
3. Participate in cooperative and information-sharing activities at the international level, by encouraging the government to collaborate with organizations, technology suppliers and other experts on this issue, benefit from them in the pre-response to accidents, then a global base for behavior, the government enhances the capabilities of cyber security incidents teams to join international and regional conferences and forums in order to build capacities, in order to improve the latest technology in incident response at the regional level (30).
4. The necessity for the academic side to be present strongly in achieving cybersecurity, though, among other things, working to promote, develop and market intellectual property, technology and innovations, specialized and development research, likewise, to expand and strengthen the research community in the field of cybersecurity, work to create a bachelor's degree in cyber security that is in accordance with special criteria (31).
5. As computers and smartphones have spread widely, along with a wide spread of the Internet, the establishment of seminars, workshops and scientific conferences in order to address all segments of society without exception requires a definition, to create societal awareness of the most important cyber risks and how they can be faced, issue semi-annual reports in this regard, to spread cyber awareness which will undoubtedly reduce the risks of cyberspace. Emphasis must also be placed on security education, which includes raising awareness of cybersecurity, which involves spreading a cybersecurity culture between the general public and the institutions concerned, establishing links with government professionals in cybersecurity, share information on cybersecurity initiatives, developing and strengthening cooperation in the field of

cybersecurity issues between the concerned institutions and individuals, exchanging communications and messages with a focus on developing internal communications (within the government agency responsible for this program) and external communications (other government agencies), industry, educational institutions, computer users and the general public (32).

RESULTS

The researchers found, through the course of the research, a set of results, the most prominent of which are:

1. Cybersecurity has become a basic requirement that all developed and developing countries strive to achieve due to the dangers that result from conflict in cyberspace, therefore, many countries resorted to formulating strategies to ensure that they protect their cyber security.
2. There is a clear correlation between the cyber security and the national security of the state, at the same time, cyberspace represents the fourth area of the state, along with the three terrestrial, air and maritime domains, so any breach of cybersecurity is a violation of the sovereignty of the state.
3. The threats posed by the conflict in cyberspace are internal mobilization against existing political systems, use as a means of conflict within the state among its components on sectarian, economic or religious grounds, create a soft war, influence feelings and thoughts, and launch a psychological and media war, the electronic conflict has taken on a competitive nature over the acquisition of technological advances and theft of economic and scientific secrets, until that conflict extends to trying to control the Internet, by seeking to control domain names and addresses, controlling information, and working to penetrate the national security of countries without using planes or explosives or even violating sovereign borders such as hacker attacks, site destruction, and espionage, it has an impact on destroying the economy and infrastructure with the same strength that a devastating conventional bombing may cause.
4. The result has been an increase in the number of computer users and smartphones, lack of clarity in a cybersecurity strategy, lack of reference on cybersecurity, if the cyberspace in Iraq becomes exposed to the outside and vulnerable to penetration, the breaches that the Iraqi ministries have been subjected to, in addition to Iraq having late positions in the Global Cybersecurity Index, ranked (107) internationally in 2018, considered evidence.
5. The lack of relationship between the Ministry of Communications, which is supposed to be concerned with cyberspace and other ministries. All these facts strongly indicate the necessity of adopting realistic solutions to achieve cybersecurity.

REFERENCES

1. Dhia Muddalloul Faraj Al-Taie, Cyberspace and its effect on reformulating the drawing of the Middle East map, Master Thesis (unpublished), College of Education, Diyala University 2017, pp. 9-10.
2. Sabah Abdel-Sabour Abdel-Hay, The Use of Electronic Force in International Interactions of Al-Qaeda as an Example of the First Part, The Egyptian Institute for Political and Strategic Studies 2016, p. 13.
3. Abd Al-Rahman Bajad Sharie Al-Otaibi, The Role of Cyber Security in Promoting Human Security, Master Thesis (unpublished), College of Strategic Sciences, Naif Arab University for Security Sciences, Riyadh, 2017, p. 16.
4. Dhia Muddalloul Faraj Al-Taie, Previous Source, p. 10.
5. Dhia Muddalloul Faraj Al-Taie, Previous Source, p. 11.
6. Hamed Bin Quneifith Wanas Al-Shammari, A Strategic Vision for Cyberspace Protection for the Kingdom of Saudi Arabia, Master Thesis (unpublished), College of Strategic Sciences, Naif Arab University for Security Sciences, Riyadh, 2015, p. 8.
7. Alem Al-Deen Banja, the risks of cyberattacks and their economic effects: A case study: Gulf Cooperation Council countries, Journal of Development Studies, Arab Planning Institute, Kuwait, No. (63), 2019, pp. 9-10.
8. Hamed Bin Quneifith, Wanas Al-Shammari, Previous Source, p. 35.
9. Herbert Lynn, Cyber Conflict and International Law, An Anthology of the International Review of the Red Cross, Volume (94), No. (886), 2012 pp. 518-519.
10. Ahmad Abees Nima Al-Fatlawi, Cyber Attacks: Its Concept and International Responsibility Arising from it in the Light of Contemporary International Organization, Al-Mohaqiq Al-Hali Magazine and Legal and Political Sciences, Fourth Issue, 2016, p. 617.
11. Todd, Graham H., Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition, Air Force Law Review, 64, No. 96, 2009, p. 65.
12. Abd Al-Rahman Bajad Sharie Al-Otaibi, The Role of Cyber Mother in Promoting Human Security, Master Thesis (Unpublished), College of Strategic Sciences, Naif Arab University for Security Sciences, Riyadh, 2017, pp. 28-30.
13. Abd Al-Rahman Bajad Sharie Al-Otaibi, Previous Source, S32-34.
14. Aisha Al-Tab, Counter-Digital Revolution: A Sociological Approach to Cyberspace Crime, Additions Magazine, Center for Arab Unity Studies, Beirut, First Issue, 2008, p. 154.
15. Mona Al-Ashqar Jabbour, Cyber Security: Challenges and Requirements for Confrontation, The First Annual Meeting of Specialists in Cyberspace Security and Safety, Beirut, 27-28 August 2012, p. 3.
16. Abd Al-Rahman Bajad Sharie Al-Otaibi, previous source, p. 22.
17. Walid Ghassan Saeed Jaloud, The Role of Electronic Warfare in the Arab-Israeli Conflict, Master Thesis (Unpublished), College of Graduate Studies, An-Najah National University, Palestine 2013, p. 52.
18. Adel Abdul-Sadiq, Cyberspace and New Threats to National Security, Arab Center for Cyberspace Research, http: //www.accronline.com/article_detail.aspx? Id = 8745 # _edn2
19. Adel Abdel-Sadiq, Cyberspace Weapons Under International Humanitarian Law, Awraq Magazine, Future Studies Unit, Bibliotheca Alexandrina, No. (23), 2016, pp. 12-13.
20. Mona Al-Ashqar Jabour, previous source, pp. 2-3.

Adel Abdul-Sadiq, Cyberspace and weapons of mass proliferation between deterrence and arms race, the Cyber Space Wars conference is available at: https://seconf.wordpress.com/
21. Republic of Iraq, Ministry of Planning, Central Statistical Organization, Communications and Post statistics for the year 2017, p. 4.
22. The Iraqi Digital Center: Most ministries' websites are unsafe and their data are vulnerable to penetration and misrepresentation, available at the link: https://dmc-iq.com/2019/08/31
23. Global Cybersecurity Index 2018, p58. Digital Media Center: Iraq occupies a humble position in cyber security available at the link: http://non14.net/110629
24. Arab Republic of Egypt, Presidency of the Council of Ministers, Supreme Council for Cyber Security, National Cyber Security Strategy 2017-2021, p. 12-14.
25. International Telecommunication Union, Cybersecurity Manual for Developing Countries, 2006, p. 7.
26. Aws Majeed Ghaleb Al-Awadi, Cyber Information Security, Series of Publications, Al-Bayan Center for Studies and Planning, 2016, pp. 30-31.
27. National Security Adviser, Secretariat of the Supreme Technical Committee for Communications and Information Security, Iraqi Cybersecurity Strategy, p. 8.
28. Aws Majeed Ghaleb Al-Awadi, previous source, p. 33.
29. National Security Adviser, previous source, p. 9.
30. Aws Majeed Ghaleb Al-Awadi, previous source, pp. 37-38.