Cyber Security and its impact on national security

Major General Dr.
Khaled Abdul Ghaffar Al-Bayati
Advisor of Alaietimad Center for
Security and Strategic Studies

Abstract

Despite the advantages offered by technological progress through digital services, it can pose a major threat that causes extensive damage to national security, economic development and critical infrastructure, and these threats have recently begun to escalate and become transnational, making confronting them a great and complex challenge for all Countries, given the recent experience and the presence of many threats and risks that we can face in this world, it was necessary to build the right foundations for an integrated security framework that provides adequate protection for the communications and information technology sector and enhances its role in achieving sustainable development goals.

Keywords: Cyber Security, National Security, Terrorist

Aim of the study: This study aims to accomplish a reliable idea towards a safe digital future, enjoys resilience and reliability to protect the assets and national interests to promote peaceful transaction within cyber security:

1. Learn about the concept of cyber security within the pillars of comprehensive national security
2. Identify the challenges facing national security in the field of cyber security
3. Recognize the best ways and means to deal with this type of security.

Hypothesis : The greater the technological development, the greater the risk of breaches in the field of cyberspace, which affects national security.

Importance :The importance of research lies in providing security for the critical infrastructure of information and other critical elements in the information system in light of the current situation is a huge national challenge. National security requires a coherent cyber security governance framework to provide a comprehensive approach to the current and future security landscape. Both state and non-state actors involved in cybercrime are adequately equipped with sophisticated cyber tools to cause damage of unprecedented proportion.

Structure of the Study

Chapter One: the concept of cyber security is one of the pillars of national security.

Chapter Two: cyber risks and threats to the national space.

Chapter Three is cyber threats and the extent to which they can affect national security.

Chapter Four: Iraq's experience in writing the national strategy for Iraqi cyber security

Introduction

In the last two decades, cyberspace has become an interconnected network of critical and non-critical information infrastructures, which brings together interconnected information and communication resources through the use of information and communication technologies. This space includes all forms of digital interventions, social interactions and communication, social disciplines, transactional activities, content, communications, and resources that are disseminated through interconnected networks. It is an essential part of society and the economy and plays a major role in their development, in addition to its role in strengthening the security and defense sectors and the application of e-government aside from information technology, as well as the Internet, has become the link of all these components with each other and provides development opportunities for all of them.

Chapter One
The Concept of Cyber Security as a Pillars of National Security

The Concept of Cyber Security:

The term cyber security was mentioned in many academic, governmental, media and even popular literature, but with varying and different points of view, and that the lack of a widely accepted definition that accommodates the multiplicity of security dimensions may lead to hindering technological and scientific progress due to the strengthening of the technical view of the term cyber security while separating the rest of the disciplines that It must come together to address the increasing cybersecurity challenges that have come to include political, social and economic challenges as well as local and regional regulatory and legal frameworks and countries that adopt cyberspace.

Number of definitions can cover this concept, with a focus on security, which is of interest to the research:

1. International Telecommunication Union: Cybersecurity is a set of tools, policies, security concepts, security guarantees, risk management approaches, procedures, training, best practices and techniques that can be used to protect the cyber environment and the conditions of users and owners.

2. Canadian Public Safety CNNSI: Cybersecurity is a set of technologies, processes, practices, response and mitigation measures designed to protect networks, computers, programs and data from attack, damage or unauthorized access to ensure confidentiality, integrity and availability.

3. The National Initiative for Cyber security Studies in the US Department of Homeland Security (DHS): Cyber security is the activity, process, or ability by which the information and communication systems and information contained therein are

protected, or defended against damage, unauthorized use, modification, or exploitation.

From the aforementioned, we conclude that cyber security is a set of technical, organizational and administrative means that are used to prevent unauthorized use and misuse and restore electronic information, communication systems and the information they contain, with the aim of ensuring the availability and continuity of the work of information systems, enhancing the protection, confidentiality and privacy of personal data and taking all necessary measures necessary to protect citizens and consumers from risks in cyberspace. So, cyber security is a strategic weapon in the hands of governments and individuals, especially since cyber warfare has become an integral part of modern tactics for wars and attacks between states.

National Security

The concept of national security is expanding and taking on many and varied dimensions, as it is no longer confined to one field or one dimension, but rather it has several basic dimensions, sometimes called elements of the comprehensive state power, and these dimensions may differ from one country to another.

Trager and Kernenberg define national security as “that part of government policy aimed at creating conditions conducive to the protection of vital values.” Henry Kissinger defines it as “any actions through which society seeks to preserve its right to exist. As for Robert McNamara, he believes that “security is development, and without development there can be no security, and countries that do not develop in reality simply cannot remain secure. Military security: It is a sense of armed danger, defensive capabilities, and a future reading of the intentions of states.

Political security: It is the political stability of the state, and the protection of legitimacy.

Economic security: which is the protection of wealth, financial resources and development.

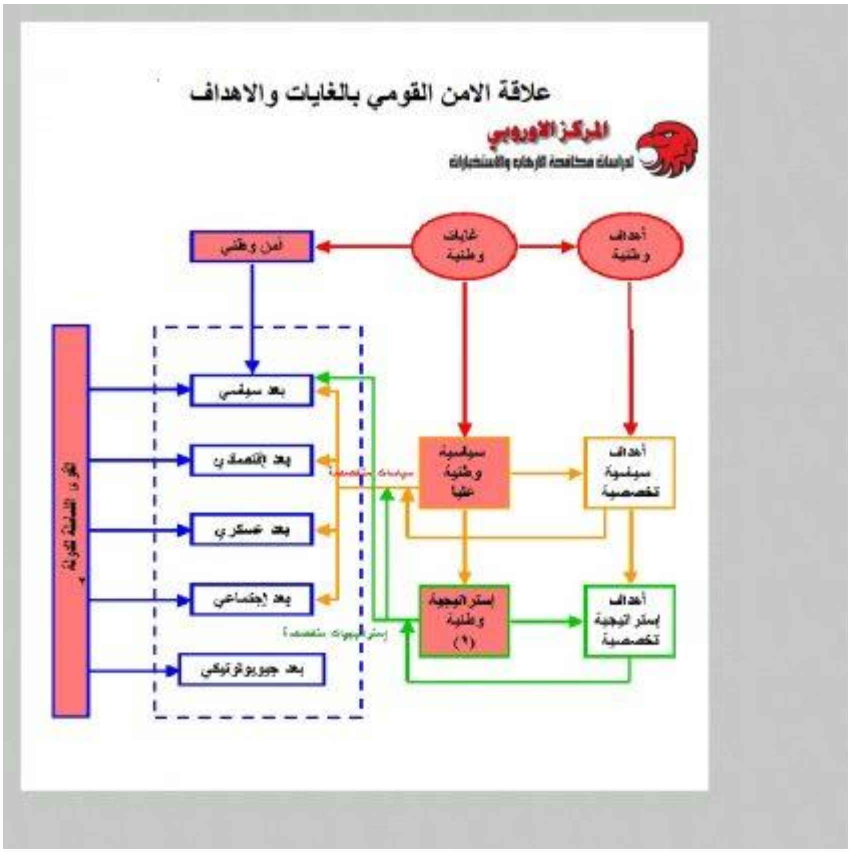
Social Security: It is the peaceful coexistence between all the components of the state through acceptance of the other side and respect for the customs and traditions of the other components, regardless of race, religion, sect, identity, and a sense of safety.

Sustainable development: It is one of the outputs of the cohesion of national security and is intended for it. It is the process for any country that means strength in its national security and its repulsion for any breach in the political, economic or social field, the first of which is the security and military field.

National security: It is the ability of the state to protect its lands, resources and interests from external threats - military and internal threats. As a result of globalization, shifts have occurred in the concept of security, most notably force, which is no longer associated with the military factor, but rather with politics, technology, education, economic growth, and the adoption of information.

Pillars of National Security

1. Realizing external and internal threats.
2. A strategy for developing the state's forces.
3. Securing the ability to confront external and internal threats.
4. Reading the hostile intentions of the target countries.



Chapter Two

Cyber risks and threats to the national space

Cyberspace: Threats and Opportunities

There is no doubt that digital infrastructure is the backbone of thriving and developed economies, strong armies, governments, transparent institutions, and free societies. poses it. Cyberspace has become deeply rooted in our lives (this field can be likened to a virtual computer or an electronic means used to facilitate communication via the Internet), so it is a global field consisting of interconnected networks of information technology infrastructures, data, communication networks, computer systems, processors, etc. Today we are talking about the number of Internet users in the world at about 4.95 billion people, according to 2022 statistics, and this number is approximately equivalent to 62% of the total world population, and this number is constantly increasing, as there are about 257 million new

Internet users during approximately one year. According to media reports, the growth rate of Internet users is currently estimated at about 5.7%, which is equivalent to more than 700,000 new users every day.

Rapid technological developments and innovative ideas are constantly changing and reshaping this virtual world, and therefore it is a dynamic development, and the degree of change in it is large and dramatic. For example, about 3 decades ago, wireless communication in public places was unimaginable. We live today how The introduction of the wireless network has raised the level of cyberspace to a different height in terms of efficiency, convenience, streamlining and ease in connection and communication.

However, it also presents a new set of threats and challenges, as the recent invention of quantum computing (a theoretical computing model in which data and computing processes are processed through "quantum" laws) is 100 million times faster than existing computers, while this It provides much higher computing power, and hackers can also use the same device to hack into securities in a faster manner, thus changing the landscape of cyber security to a great extent. This dynamic of cyberspace now requires evaluating areas of national cyber strategies for many countries.

The most common challenges in formulating cyber strategies are determined by several reasons, including but not limited to: the lack of a clear vision for electronic affairs at the national level, as most developing countries do not have coherent national policies with regard to their cyberspace, as well as the heavy reliance on hardware and software Imported, as many countries depend on importing computer technologies and technologies from advanced countries in this field, such as China and America, and use them in their vital sectors such as defense, security, economic and governmental financial institutions, and therefore this dependence poses a serious threat to the national security of states.

One of the most important other reasons in this context is the allocation of an insufficient budget for cyber operations as a result of the reluctance of some governments not to grant sufficient funds to organizations, bodies and institutions related to cyber issues, due to a lack of understanding or perhaps a lack of sufficient awareness of the seriousness and importance of this field at the vital national level, And the role of cybersecurity in the process of protecting systems, networks and programs against digital attacks in light of the emergence of a digital landscape that promotes continuous cooperation to monitor new risks.

In addition, the lack of an appropriate national structure to deal with cyber conflicts, as some countries do not have any specialized and integrated national institute or center that can manage and supervise cyber issues, respond to cyber security and enhance information security in all its forms, not to mention the absence of a continuous culture of cyber security within the bodies The flabby government bureaucracy in some Third World countries, as most of those developing countries do not have a regulatory policy to monitor threats to their vital infrastructure, such as banks, telecommunications networks, financial transactions and various vital sectors, as it seems that some developing country governments are reluctant to initiate any radical change In the current policy and the government apparatus, and this trend is reinforced by the difficulty in adopting rapidly changing technologies in a timely manner, and the lack of research and development initiatives for local digital products, with the absence of research, studies and development centers in many of our third-world countries without benefiting from the available expertise.

Based on these data, it can be said that it is very difficult for there to be modern, developed and prosperous countries without finding solutions that overcome the problems mentioned in the above points, and without having a reliable and strong system to ensure the security of its domain and cyberspace, as the latter represents at the same time a great, promising and pioneering opportunity. Without overlooking its dark and dangerous side, which should be managed properly, thoughtfully and effectively. How not, most of the infrastructure today for the various countries of the developed world is based on cyberspace based on information technology technology and communication technology in all fields, industrial, military, security, energy, water, health, transportation system, banking sector, financial and governmental institutions, until it has become an integral part of national security, and entered into Changing the form, techniques and methods of wars due to the changing nature of its threats and damage to the vital and strategic institutions and centers of states.

Some countries and other parties may view cyberspace from a different perspective, some of them see it as a job and investment opportunity or a means of self-expression, while others see it as a threat to their national security, while there are many examples of technology used for malicious purposes. Experience also tells us that Affordable access to communication technologies and global information flows can be a force for economic and technological progress and informational and technological superiority.

Cyberspace is a double-edged sword because of its positive aspects on the one hand and challenges and threats on the other hand, especially that cyber attacks and crimes have become complex, complex, accelerating and dangerous, and it is difficult for many institutions to overcome and defend their cyber security without the presence of national action strategies and the acquisition of advanced technologies and applications. And sound practices within a comprehensive strategy for cybersecurity that takes into account all possibilities to prevent the dangers and threats of this expanding global space, which has undoubtedly become the new field of war between the parties of the great world powers.

Chapter Three

Cyber Threats and the Extent to Which They Can Affect National Security

In light of the successive technological developments, the diversity in the tools of force, and the evolution of the nature of wars in its various generations; The importance of achieving “cyber deterrence” is growing, which has become a measure of the extent to which countries are able to protect themselves from any attempts to penetrate, and thus secure the data and information they possess, and protect their national security, especially in light of the employment of some countries, or non-state actors, whether multiple companies. Nationalities, international organizations, or even terrorist groups - to cyberspace as a field for achieving their goals in various conflicts, and in that framework the concept of force and the concept of “cyber wars” developed, and the capabilities threatening security and impeding the achievement of development increased, as the cyber threat multiplied in contrast with the development Technological means, and the occurrence of a huge boom in them, have become a double-edged sword.

It is the responsibility of the media to make efforts to challenge and confront threats to intellectual security, and to raise awareness of the field of cyberspace, which is being used in several forms, and non-peaceful forms, as a tool to achieve a comparative advantage in international conflicts, and new generations of wars, which negatively affects information security. Global power, which resulted in transformations in the concept of force, and the replacement of traditional power with hard power, with its military tools, leading to the concept of electronic power, which is not subject to clear international laws, because it is completely different from the traditional power covered by international law.

Cybersecurity and Its Relationship to National Security:

The concept of national security has shifted from the traditional pattern, related to the extent of the ability of military power, enjoyed by states, to protect them from security threats, and it is no longer appropriate to limit national security to hard power. The sources of state power have changed, including technology, communications, and information, along with The diplomatic and economic power of the state, and these new sources of power are less expensive and highly influential in the international system.

It should be noted that, on the other hand, military power, as an element of power, still has an important weight, but it is no longer considered, as in the past, the only source. on cyberspace, in international interactions, both conflictual and cooperative; The shift in the nature of power has intensified, the threats related to cybersecurity have intensified, and the exploitation of cyberspace to achieve advantages and an effective and influential role through electronic tools.

From the foregoing, it is clear that the information and technological revolution has resulted in replacing the elements of traditional power with new tools, and the distinguished military capabilities, as well as the money and wealth that states possess, have become insufficient elements to protect their security, or to enhance their effective role regionally and internationally. It is necessary for the state to possess the tools of cyber power, but rather to employ them as supportive tools for soft and hard power.

Technological development and the processes of its employment by states and non-state actors to achieve goals that threaten the national security of states stimulate the need to absorb cyberspace as an element of national security, as cyberattacks lead to negative repercussions on comprehensive development (economic, social, political, etc.). and others), where cybercrime is widespread, such as electronic extortion, piracy, and bargaining for a fee, and actors may exploit social media to threaten national security; By raising anxiety in society and threatening social peace, which requires continuous work to build an effective strategy, with its continuous updating to deal with cyber threats, manage these situations efficiently, and international coordination to confront these cyber attacks, as the impact of cyberspace on the security field is not limited to the state Only internally, it extends and reaches the international environment, drawing a new content for international peace and security, and setting new frameworks for the reality of international relations. The GCI Cybersecurity Index has become one of the most important mechanisms for measuring the security of every country around the world.

If national security is concerned with protecting and preventing threats to the basic values of society and eliminating the fear of these values being attacked, then cyberspace has imposed a rethinking of the concept of security, which relates to that degree that enables the state to become safe from the threat of military or terrorist attack, as well. Protection measures against the exposure of vital installations and their infrastructure to hostilities through the misuse of information and communication technology.

Hence, we come to a comparison between the concept of national security and cyber security, as the first refers to its security as a broad concept related to the degree that enables the state to become safe from the threat of military and terrorist attack, while cyber security refers to protective measures against exposure to hostilities and misuse For information and communication technology, and as has been indicated, national security means protection and prevention of threats to the basic values of society and the removal of fear that these values will be attacked. Security includes a wide range of areas within and outside the field of information technology.

Therefore, the national interests that are linked to the vital infrastructure of the state have become vulnerable to attack, which cyberspace has made linked to each other in a single work environment, which is known as the (national) infrastructure, and in light of this, every attack on one or all of the interests leads to a strategic imbalance, including It illustrates at the same time a new form of conflict.

These factors necessitated the development of the concept of national security in the direction of new non-traditional threats and the expansion of the field of security to extend from the military side to many other fields, and since the electronic government devices in the world are in an open space, and there are no geographical borders, so its devices become vulnerable to many dangers under different motives, and it is possible that Electronic government systems are attacked from within or from outside by hackers or intelligence services in hostile countries by carrying out electronic attacks with the aim of penetrating the information security system of the government and therefore changing national security to include cyber security that countries seek to protect.

As electronic crimes are no longer limited to individuals and institutions, but rather go beyond that to threaten the security of the state and the safety of its facilities and economy, which requires harnessing all technological capabilities, qualifying human resources and improving the ability to deal with cybersecurity issues, to reduce electronic risks threatening the state's economy and national security.

National security is the efforts made by the security agencies to maintain the cohesion of the security of human society and its social, political and economic construction, customs and traditions. This is done through adopting the necessary measures that ensure the security and stability of the country and the continuous progress and prosperity. Against any direct or indirect aggression, internally and externally, politically or morally, economically or militarily, and security from this logic is a means of development and there is no development without security. The level of production and interaction with the issues of the homeland as a result of the loss of security.

Today, in light of these accelerating changes, we are facing a profound challenge related to ensuring the safety of communication systems and information exchange, not only between countries and specialized institutions, but also on a personal level, which was reflected in political life and led to the emergence of serious risks and threats to national security.

Spread and Escalation:

The global structure of information is severely threatened, as a result of the growing connection to cyberspace. This has also been exploited by many terrorist groups, which seek to harm the national security of countries. Some countries, such as Russia, Iran, and Israel, also wish to launch cyber operations against other countries to achieve goals. And special interests, and therefore it has become necessary to pay more attention to protecting cyber security. The intensity and volume of electronic attacks has increased significantly, and by their nature they are characterized by difficulty in the process of accurately identifying their perpetrators, and the absence of a counter-response to this effect, and as a result of the multiplicity of actors in the electronic conflict, and the different interests sought to be achieved behind it, its forms vary, and among the most prominent methods and methods used Countries resort to it in the electronic attack:

1.Theft and transfer of information: hacking into databases to steal them, collecting intelligence information about other parties, and obtaining information owned by the opponent.

2. Destruction of information: accessing the opponent's information via the Internet or internal networks, and modifying the data so that it is misleading to the opponent, or erasing it permanently, destroying it, or destroying the facilities.

3. Disruption of service: hacking into the opponent’s devices and networks, and disrupting the service provided to him, by releasing many data and tasks on the server or computer, beyond its capacity, which may lead to slowing down its movement, or stopping it completely or partially.

4. Influencing and controlling minds: implementing schemes to control peoples, by dispersing human consciousness, through cyberspace, interactive network technology, and controlling and directing global public opinion.

Electronic power rectifiers: Countries are working on building strategies to face the new challenges posed by the dangers of cyberspace, and to resist hacking operations, which is called the “electronic deterrence strategy”, provided that attention is also paid to awareness, since the responsibility for this task lies with everyone, and technology today is a key indicator To achieve military and economic superiority, and an important criterion for national strength, and the Internet plays an effective role in achieving the goals of the state, especially in terms of reducing entry difficulties and influence for emerging countries.

There are many pillars and tools for achieving cybersecurity, represented in the availability of an advanced technological infrastructure, and a human element capable of managing it efficiently, with the provision and possession of electronic weapons, to achieve “electronic deterrence”, and the most important of these elements can be extracted as follows:

1. Establishing an early warning system: protecting the infrastructure that is expected to be attacked electronically, thus helping to provide the possibility of detecting any attacks before or immediately after their occurrence, in order to prevent their effects and expected repercussions.

2. Availability of technological infrastructure: the provision of “information technology” components, whether hardware, computer facilities, networks, or software components.

3. Training the human element: Training on how to control cyberspace devices, while developing the capabilities of human cadres to invent or develop them as well.

4. Developing a strategic plan to support the state's efforts: employing the state, managing its resources accurately, and mobilizing them; To achieve goals in cyberspace, while preventing them from being wasted, and to define methods of implementation, plans, and tactics suitable for various circumstances, in order to maintain the flexibility of the implementation movement later.

5. Possession of electronic weapons: developing programs through which information can be attacked, destroyed, or stolen, such as (chips - viruses - worms - Trojan horses).

6. Protecting computer networks: being able to protect networks and information from hacking attempts, by securing the network, devices, and electronic chips, and encrypting key data, with the availability of protection systems such as electronic shields.

7. Providing an institutional and legislative structure: the existence of an institutional structure that manages the use of cyber power, and works to achieve the objectives of the state’s strategy, by providing armies and electronic battalions that protect cyber security, and allocating budgets to upgrade the

areas of attack and defense, and a legislative structure that sets definitions for cybercrime and punishment perpetrators.

8. Diversification in reliable energy sources: To avoid the risks of targeting electricity networks in the country, for example, you should not rely specifically on supplying vital institutions, especially hospitals and factories, on only one source, as the more alternatives are available, the risks decrease.

Cyber Diplomacy:

With the advent of cyberspace in international interactions, the concept of diplomacy has evolved significantly, and the concept of “cyber diplomacy” has emerged, to which Western countries have turned in particular, and it is done through the exploitation of the means of the Internet and social communication; To disseminate diplomatic information about themselves, and to interact with the peoples of the world, to improve their image in the mind of world public opinion, and to create an influence that increases their ability to influence it and direct it to achieve its interests.

The first country to adopt this concept was the “United States of America”; With the aim of disseminating and promoting its ideas and policies around the world, Washington established the Digital Communication Team in 2006, and the Opinion Space in 2011, which enables the expression of opinions on topics related to politics, the economy, and the position of civil society, which has been employed by community organizations. Civilian in achieving the desired results of this diplomacy.

For example, since there are no official diplomatic relations between Washington and Tehran, Washington launched, in 2011, a website, as the “Virtual Embassy of the United States of America in Iran,” with the aim of disseminating information to Iranians, through this website, about entry visas. , and student exchange programs, but the Iranian government blocked it as soon as the United States launched it.

Terrorist groups and their use of cyberspace (Iraq as a case study):

Although the technological development that Iraq went through, by opening up to the field of information and communication technology, after the US invasion in 2003, achieved many advantages, it turned "Baghdad" into an open arena that is easy to penetrate, and spy on sensitive information in its security institutions, and this is due to The lack of a secure infrastructure for all security, personal, and banking information systems, and this left room for some terrorist organizations that invaded Iraq and spread there, immediately after the fall of the previous regime.

It practiced new and innovative forms of terrorism, using modern and advanced means of communication, and it did not stop at attempts to hack websites and attack the information infrastructure. Rather, it worked on creating thousands of pages and websites that aim to work on attracting young minds and spreading extremist ideas that are based on They have to organize and promote them with their slogans. These extremist groups realized, early on, the importance of the Internet and social networking sites, so they used the tools of the digital world in their interest to recruit young people easier and faster via the Internet, using many unmonitored networks, especially the "app" Telegram, and the "Deep Web," and the terrorist organization (ISIS) was able to obtain support and financing via the Internet, by obtaining "electronic currencies," and it also uses cyberspace for support in carrying out specific attacks.

Iraq is still suffering to this day from instability, and cyberspace imposes several challenges on it, which it does not have the ability to deal positively with, and adapt in order to keep pace with current developments in light of the current transition to virtual space, and dealing with cyber attacks carried out by "hackers" and armed groups, Especially what Iraq is facing in terms of numerous penetration attempts, and attacks via cyberspace, accusing pro-Iranian militias, which have affected media institutions, such as “UTV” and “Fallujah” channels, in addition to the cyberattack on the Baghdad Airport website, most of which are denial-of-service attacks targeting The network infrastructure is of the “DDos” type. Today, thanks to the national capacities, a cyber security strategy has been issued that addresses breaches and electronic attacks to reduce them.

ISIS Cyber Threats

ISIS is no longer a naive “Islamic jihadist” organization as much as it is a “secret terrorist organization.” What the organization also needs is expertise, and as long as this organization is based on globalization and multinationalism within it, it can achieve its goals on cyber and social media. Organization is possible. To turn into a secret organization, to carry out assassinations more than suicide operations, similar to the right-wing and left-wing secret organizations, and to be very active in Europe, and to carry out “cyber” and hacker attacks against it. Rather, its ability may reach the extent of destabilizing the security and stability of countries through these operations And trafficking in arms, drugs and prohibited items.

What governments need is to find digital units and recreate the anti-terrorism strategy, which goes beyond stereotypical forms on the ground and rises to the size of the threats of ISIS and extremist groups. National security threats in the era of globalization are no longer what is happening on the ground, as much as attacks and activities on the Internet, and this prompted the CIA , and the Pentagon, as well as in the European Commission, to develop digital units to deter electronic attacks, to protect national security.

Corona Pandemic and Cyber Attacks:

The Middle East region, in particular, witnessed a remarkable increase in the number and severity of cyberattacks and security threats, in light of the year 2020, and the negative repercussions produced by the “Corona” (Covid-19) pandemic, which stimulated countries to digital transformation, to diversify the sources of the economy, in light of the tension. between several parties in the region, and the digitization processes that most countries in the Middle East turned to increased the possibilities of being more affected by the cyber attack, as there were more opportunities for the spread of malware, hacking operations to steal personal data, and crimes of privacy violations, especially since many citizens did not have Adequate experience in insurance procedures, and the lack or scarcity of awareness programs to protect cybersecurity for individuals, which enhances the necessity of coordinating the efforts of the countries of the joint region, to exchange experiences, and build cadres in the field of electronic security, while working to support and develop the strategies of countries, in terms of devices, Or software, on the one hand, and the other, and securing government e-services with accuracy and high efficiency.

Some countries, such as Iran and Russia, have also been accused of launching numerous cyberattacks targeting the World Health Organization and some American and British research centers. Terrorist organizations have also taken advantage of the conditions imposed by the pandemic, and the preoccupation of the countries of the world with combating the “Corona” virus, so they have further promoted their extremist views. Reducing trust in governments through the Internet, with the aim of attracting and recruiting young people, and threatening the stability of countries, in light of spending most of the time at home, surfing the Internet, and social networking sites more, especially in rural areas affected by a greater degree of closure.

Media Role in Supporting Cyber Security:

The media is an essential pillar of the state's national security, and it plays a pivotal role in supporting culture and the national identity of the people. The means of communication and the media are also one of the soft power tools that the state enjoys and employs in protecting its national security. The Egyptian state has great experience in this regard. Within the framework of Egypt’s efforts to defend its cyber security, the Supreme Council for Media Regulation put forward a strategy “Towards Responsible Development Media” in March 2021, which includes several axes, the most important of which are:

1. Work to achieve the goals of the vision of sustainable development 2030.
2. Providing constructive media aimed at achieving the goals of the state, and urging the citizen to share in the burdens of development, with transparency in describing and explaining the challenges facing the state.
3. Preparing programs and policies aimed at raising awareness, to support the state's efforts to confront challenges and various wars, including cyberspace.
4. Confronting rumors and false news, and educating citizens, according to several media policies.

It is worth noting the importance of upholding values in society, preventing terrorism and technical crimes from spreading, issuing new laws on cybercrime, such as Egyptian Law No. 175 of 2018 (the law on combating information technology crimes), and working to establish judicial bodies specialized in this aspect, on the basis of The media should also have an effective role in supporting these efforts continuously, by raising awareness and spreading digital awareness, so that an informed and educated public opinion is formed, and to protect the privacy of individuals and their data without falling as victims of cybercrime and exploitation.

Based on the above, it can be said that the media has a pivotal role and a major responsibility.

To educate citizens about the importance of cybersecurity and the dangers of electronic hacking, and to educate and educate the people, through many tools and means that qualify them to protect their technological devices, starting with securing the personal phone against hacking attempts, and following security measures while browsing websites, which can exploit their personal data one way or the other.

Chapter Four

Iraq's Experience in Writing the National Strategy for Iraqi Cybersecurity

Towards a secure, secure, vibrant, resilient, and reliable digital future that provides opportunities for its citizens, protects national assets and interests, and promotes peaceful interactions in cyberspace for the sake of national prosperity.

As the Iraqi government seeks to achieve comprehensiveness in understanding the basic concepts of current, emergency and future challenges. Followed by interaction with these concepts by preparing plans and responding in accordance with international recommendations on its five axes with regard to cybersecurity in its various legal, technical, organizational, capacity building, and national, regional and international cooperation.

The idea of protecting the telecommunications sector and the controversy of its impact on ethnic national security emerged in 2011, when the first higher technical committee for communications security was established, which resulted in writing the first national policies for the information and communications security sector.

In 2013, a draft strategy for building the concept of cybersecurity in Iraq was started through sessions, discussions and lectures that were held at the Al-Nahrain Center for

Strategic Studies, which is one of the formations of the Iraqi National Security Advisory Council, during which the reality and study of the work environment and the challenges faced by the security and military services and other sectorial bodies were evaluated with Infrastructure identification and evaluation. He participated in these discussions in the presence of experts from the friendly side to provide advice and the experiences of their countries.

The work of these policies was not completed due to the entry of ISIS and the preoccupation with confronting it, as the focus became on establishing the psychological warfare team and the monitoring and crime-fighting team to support efforts to confront ISIS.

In 2015, the second version was written to update the information and communications security policy, introduce technical standards, and coordinate between the e-government services team and the e-government team.

In 2017, approvals were obtained for the formation of a team (response to cyber incidents), and at the same time, a team was assigned to write the national strategy for cybersecurity, where the relevant authorities were gathered, re-worked, evaluated the reality, and provided service after the war on ISIS.

In 2019, the third version of the Information Security and Data Sharing Policy was written with the development of technical standards to protect electronic systems in general.

In 2020, this policy was approved by the Council of Ministers, and in 2022, the National Strategy for Cybersecurity was approved. The national strategy for cybersecurity has been built in five phases, as shown in the model below.

The outputs of this strategy are:

1. Establishing local teams in each institution responsible for information security through technical standards and linking them to servers with central control.

2. Work on developing national capacities in government institutions regarding personal and occupational protection
3. Cooperate and coordinate with international organizations specialized in promoting protection and detection programs
4. Drafting laws to be presented to Parliament, including the Information Crimes Law and the Digital Evidence Draft Law.

Conclusion

It is clear that the escalating development that information technology has undergone has become a threat and damages national security and the sovereignty of states, and therefore digitization has become a double-edged sword, as it achieves the desired technological development, but it enhances the possibility of directing malicious attacks through cyberspace, and on the other hand Countries today adopt methods of indirect confrontation through cyberspace in most of the conflicts of the current era, and all of this confirms the utmost necessity to support the electronic security of the state with the highest levels of efficiency. Cybersecurity can be achieved by building a security strategy that adopts national standards and procedures approved by international organizations and agencies specialized in securing cyberspace, which in turn is reflected in national security, while providing material and scientific capabilities and involving research and studies centers with the enactment of legislation and laws necessary to regulate the use of cyberspace. Taking into account the compatibility between the requirements of achieving national security and guaranteeing personal freedoms, non-violation of privacy, and freedom of access to information...

1-Information and communication technology brought about a transformation in all aspects of life, and affected negatively and positively the behaviors of societies, which resulted in a change in social foundations such as belonging to the national identity, and privacy as a result of the use of social media.

2- Cybersecurity is an essential element in the dynamics of national, regional and international security and its impact on traditional national security dimensions, through information and communication technology on which the basic infrastructure of countries depends.

3- The emergence of cyber power on the international arena, which became available to a large number of non-state actors, which weakened the state's ability to protect and maintain its national security.

4- The concept of national security has expanded its comprehensive meaning to encompass all areas of life after it was confined to the realist school on the state and military power, to be confronted with the growth of interaction with cyberspace, which brought about a change in international relations adopting the concept of force, conflict and war, as power spread and was distributed among the actors, The conflict turned from physical to virtual, and the state went towards the militarization of cyberspace, which resulted in the emergence of new threats that are increasing in intensity and severity to constitute a serious threat to national security.

5- Failure to rely on developing a strategy for cybersecurity in countries will increase the risks and threats facing national security coming through the use of cyberspace.

6- The interaction of national security with information and communication technology through cyberspace is a new tributary to support and enhance stability and prosperity.

Recommendations

1- The development of the concept of national security requires a change in the level of perception of risks and threats through the introduction of the optimal investment of data and information available in the public and private sectors and the involvement of research and studies centers in the countries of the region in making security policy in the Arab countries.

2- The interaction of material and non-material components with the human element within cyberspace, granting state and non-state actors the ability to threaten national security and societal peace, which requires anticipation and preparation to confront the threat of the escalating cyber power by developing a program to support and enhance cybersecurity within the general security policy of states .

3- The clear impact of information and communication technology on the lives of individuals and groups and their behavior requires protecting the cultural identities, customs and traditions of peoples, with the aim of immunizing successive generations from the negative effects resulting from the improper use of the contents of the Internet, and this work is carried out through a comprehensive national program in which all actors participate. governmental, social and religious in countries.

4-Securing cyberspace requires local, regional and international cooperation, and continuous interaction with the competent international organizations of the United Nations.

5- Countries should accelerate the adoption of a strategy for cybersecurity in their countries, in the preparation of which participation (stakeholders from the government sector, the private sector and civil society organizations) will participate.