Cyber Wars and Their Impact on International Security

Reman Ahmed Abdel-Aal[1*] Rasha-Atwa[2]

1. Faculty of Commerce, Suez Canal University, 4.5 Km the Ring Road, Ismailia, Egypt.
2. Faculty of Commerce, Suez Canal University, 4.5 Km the Ring Road, Ismailia, Egypt.

* E-mail of the corresponding author: doctor_reman@hotmail.com

Abstract

The relationship between cyberspace and international security has emerged with the growing adoption of electronic governments by many countries, in addition to the expansion of the users of communication and technology means in the world. National databases are in a state of external exposure, which exposes them to the risk of being exposed to cyber-attacks. National interests are also related to the infrastructure that is vulnerable to the risk of cyber-attack. This research aims to study the impact of cyber wars on international security. The research has found that cyber wars are more dangerous than military wars because they have the ability to destroy systems and completely prevent them from working, as well as the recurring cyber-attacks that will lead to increased interest in security information.

Keywords: cyber wars, cyber security, cyber space, international security.
DOI: 10.7176/IAGS/99-05
Publication date: June 30th 2023

Introduction

The means of electronic communication have brought a scientific leap in the history of human development. The use of these means is no longer limited to the economic, industrial and social fields only, but the means of electronic communication have entered the space of human conflicts to bring a great information revolution in the military, security and political sectors. Therefore, technological advances and digital infrastructure have linked entire societies with complex and intertwined systems. The demand for the internet calls for a constantly increasing integration of communication and information technology and has been integrated into products that were working without it before. Military services and logistics, transportation systems and electricity supplies all depend on the use of information and communication technology and the stability of cyberspace; therefore, the information age has changed the form of wars from traditional, which depended on military armies and combat weapons, to cyber wars. These wars are characterized by speed and accuracy in the implementation of military operations through the use of information and communication technology, as well as the increasing reliance on smart networks and other surveillance and monitoring systems via the Internet.

Research problem

Although every country seeks to protect its cyber security, the challenges resulting from technological development as a result of the massive information revolution and the expansion of its use in various fields have led to major shifts in the quality of international threats and conflicts.

Research Questions

The main question:

To what extent is cyber war a threat to international security?

Several sub-questions arise from it:

1) What is cyber warfare?
2) What are the types of cyber warfare?
3) What are the challenges of cyber warfare?
4) To what extent do international efforts affect the confrontation of cyber wars?

Research Aims

- Determining the patterns and origins of cyber wars.
- Knowing the challenges of cyber wars on international security.
- Highlighting the most important modern threats.
- A study of the extent to which countries' laws and efforts are effective in confronting cyber wars.

Research Importance

Scientific significance

The issue of cyber wars is one of the topics on the scene, as it is considered an important topic at that stage, especially with the spread of technology and means of communication. Cyber wars take place through cyberspace, which leads to a threat to the stability and security of countries.

Practical Importance

The fact that this research reveals the new forms of security threats and how cyber wars can be contained.

The Method Used:

The deductive method is used in addition to a number of approaches:

- Introduction to content analysis by interpreting the contents of the most important official documents and international and regional agreements in order to confront the problem of cyber wars.
- Relying on the neo-realist theory:

  This theory was established by Kenneth Waltz. The basic intellectual premise of neo-realism is represented in the chaotic structure of the international system, considering that this structure is the determinant and directive of the behavior and choices of states to stay.

  This theory is based on two assumptions:

First assumption: States are the main actors in international politics.

Second assumption: The primary motive of states is survival[i] and the neo-realists recognize the possibility of cooperation between states, achieving security goals, and ensuring relative gains through cooperative policies instead of competitive policies.

Search split

The research is divided into three axes:
The first axis: cyber wars.
The second axis: international security.
The third axis: Cyber wars and their repercussions on international security.

The first axis
cyber wars

There have been rapid developments in the field of information technology, which led to far-reaching changes in all areas of life, especially in the military and security fields. The emergence of cyber wars was linked to two important events:

First: The development of computers in the mid-fifties of the last century in order to process and preserve information, in addition to the concerted efforts of a number of public and private companies that culminated in the development of the central processing unit (CPU) in order to facilitate the tasks of the computer until it became important in the work of many institutions in addition to the daily lives of individuals.

Second: The emergence of the Internet: It has made a development in human life through rapid communication and information transmission. This axis will be addressed through:

First: Defining cyber wars
Second: Concepts related to cyber wars
Third: The factors that led to the possibility of the emergence of cyber wars
Fourth: The characteristics and forms of cyber wars

First: Defining Cyber Wars

1- Linguistic definition:

War: the opposite of the word peace.

Cyber: as the infinitive of the word cyber (Cyber in linguistic dictionaries is a word of Greek origin that goes back to the term (Kybernetes), which was mentioned at the beginning of science fiction literature and means command or remote control [ii].

The American Military Dictionary defines the word cyber as any act used by electronic networks for the purpose of controlling and disrupting other electronic programs.

The American Military Dictionary defines the word “cyber” as any act used by electronic networks for the purpose of controlling and disrupting other electronic programs[iii] .

Andres defined cyber as the virtual environment in which information is digitized through computer networks and determines the military strategy of the countries to be invaded through network-connected systems and associated physical systems[iv].

2- Terminological definition of cyber wars:

Cyber wars have become one of the tools of modern wars, as war no longer depends on military armies and combat weapons only. There is no specific definition of the concept of cyber war, but these definitions are multiple, and among these definitions are the following:

Cyber wars are operations of disruption and destruction of the database in the computer network or between computers and the Internet itself. They may be directed against infrastructure, communications, global economic forces, or even against countries completely.[v]

The International Committee of the Red Cross has defined cyberwar as the actions taken by the parties to a conflict, in order to achieve an advantage over their opponents in cyberspace, through various technical tools[vi].

According to a recent Security Council resolution: a cyber war is the use of computers or digital means by one country against another, by destroying the digital infrastructure or the production and distribution of devices that can be used to sabotage the local activity[vii]. The cyber war is virtual and of a tangible nature. It is a war without blood and tools of conflict focused on electronic confrontations and technical programs.[viii] The term "cyber wars" is used to describe everything related to sabotage campaigns and disruption of the Internet, in order to reach the actual state of war using electronic means.

Therefore, any conflict that occurs in cyberspace and has an international character is called cyber war. The concept of cyber war does not include military capabilities and systems only, but rather targets the vital infrastructure of society, including smart networks, surveillance networks and data acquisition (SCADA). The tactics of cyber warfare typically involve collecting data or chaining to computerized systems in order to cause damage to critical systems. Therefore, cyber warfare is the most dangerous level of conflict in cyberspace, and aims to influence the political will of the target party and its ability to make the decision-making process.

3- Procedural definition of cyber wars:

Through the previous definitions, we find that:

Cyber wars are a conflict that arises in cyberspace, and is a means or method in itself, as it can contribute to directing military operations. They also can be a combative means by using it to infiltrate electronic systems designed to protect or regulate the workflow of vital facilities.

- You use the digital influence, which is motivated by political motives, to force the opponent to implement the will of the attacking party.
- An attack motivated by a state in order to harm the capabilities of another state, by threatening its communication systems or destroying or damaging its databases

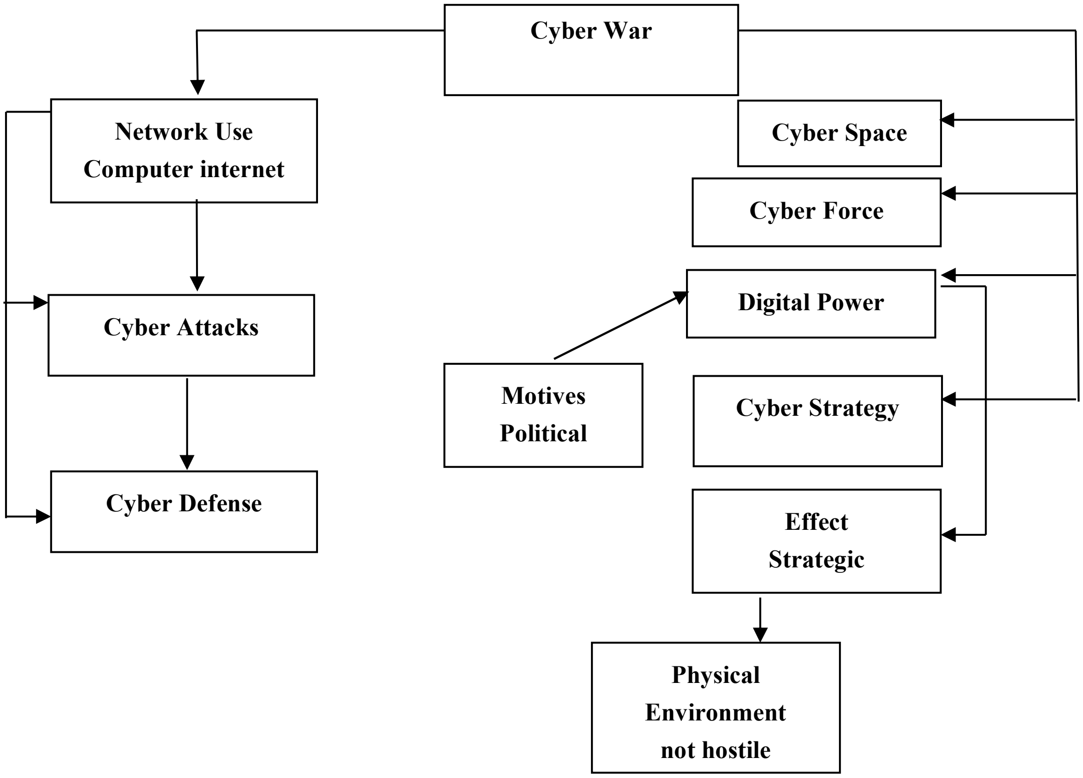

Figure No. (1) illustrates the definition of cyber wars.

Source: Zainab Shaltout, "Cyber War in the Digital Age: Post-Clauseauce Wars", Algerian Journal of Security and Development, No. 2, 2020, p. 21.

Second: Concepts Related to Cyber Wars:

1- Cyberspace:

Cyber wars occur in the cyberspace. It is defined as the medium in which computer networks operate, including computers, software, computing information, its transmission and storage, in addition to its human users, organizations and institutions[ix].

The International Telecommunication Union defines it as: the physical and immaterial domain that consists of elements that are computers, software, networks, transmission and control data, and the users of all these elements[x]. Cyberspace, like traditional space, consists of 4 basic components: place, distance, size and path. However, cyberspace is characterized by the absence of geographical boundaries and the absence of the element of time[xi]. Cyberspace is a society in which citizens interact through networks[xii]. Military operations in cyberspace are divided into 4 levels: intelligence gathering, psychological warfare, offensive operations, and defensive operations.

2- Cyber Security

Cyber security has imposed itself as a new dimension of international security. In light of the connection of all international interactions with the digital and technological aspect, the concept of cyber security has become an imperative necessity, which called on countries to find effective mechanisms and means to confront cyber threats. There is no specific definition of cyber security, but there are many definitions of which:

It is a set of procedures and frameworks aimed at protecting software and computers from various cyber-attacks that may threaten the national security of countries. It is a defensive means aimed at detecting and thwarting attempts by hackers.

Cybersecurity is the activity that secures the protection of human and financial resources that are related to information and communication technologies, in addition to ensuring the reduction of losses and damages[xiii].

Therefore, cybersecurity is defined as a set of measures taken to limit or defend computer attacks. It also includes the tools and means used in facing risks. Thus, cybersecurity is the sum of technical and organizational means that are used to prevent unauthorized use and misuse and to recover electronic information and the information and communication systems that they contain, with the aim of ensuring the availability and continuity of the work of information systems and enhancing data protection [xiv].

Through these definitions, we find that the concept of cyber security is a security concept concerned with the protection of information and everything related to this information in terms of operations, devices, services and technologies.

Third: The factors that led to the possibility of the emergence of cyber wars

- The role of the state has declined in light of globalization, in addition to its withdrawal from some strategic sectors for the benefit of the private sector. Moreover, the roles of multinational companies, especially those working in the field of technology, have escalated as an influential actor in the cyberspace, and have become technical capabilities that surpass governments.
- Increasing the world's connection to cyberspace, which led to the widening risk of electronic attacks on the global information infrastructure.
- The cost of cyber wars is low compared to conventional wars, as a cyber-attack may be launched at the cost of a tank through new electronic weapons.
- The increasing dependence of countries on electronic systems in all their vital facilities, especially the electricity and water networks, the stock exchange, banks, and others, along with military systems and information collection such as satellites and drones, has contributed to the war, making them vulnerable to this threat due to its overlapping civil and military features.
- Cyber wars have turned into one of the tools for influencing the information used in the different levels and stages of the conflict.
- The scope of the risks of hostile activities practiced by both state and non-state actors in cyber wars has expanded.
- The escalation of risks and threats in the cyberspace has led to the emergence of competition between partnerships working in the field of cyber security, with the aim of strengthening global spending markets to secure the cyber infrastructure of countries[xv].Therefore, cyber wars have features that are:
  - Increasing network influence inside and outside countries, as individuals, groups and countries use modern technology related to cyberspace.
  - Absence of electronic transparency: With the inability to know the identities of those responsible for piracy attacks, the dilemma of the absence of transparency and laws restricting conflicts in the electronic field, in addition to the fact that the source of electronic attacks may cause great losses.

- The difficulty of electronic deterrence: Cyberspace is a virtual arena and thus it is difficult for countries to set limits on their sovereignty over it, and with the weakness of international laws to control this space, deterrence is absent in light of the possibility of masquerading on the Internet and the unknown source of electronic attacks [xvi].

Fourth: The characteristics and forms of cyber wars

1- Characteristics of cyber warfare

- The attacker has one advantage: these wars are characterized by flexibility and speed, and the attacker has a great advantage over the defender.
- Asymmetric wars: There is no need for certain countries to manufacture very expensive weapons, such as aircraft carriers or advanced fighters, to pose a threat to a country.
- Its risks go beyond targeting military sites: they target civilian and sensitive infrastructure in the targeted countries.
- The tools of cyber warfare depend on the computer, and their goal is to cause harm. Therefore, cyber warfare consists of two parts:

The first part: The defensive part and electronic protection, and its mission is to protect the material and moral components of cyberspace, its tools, work procedures, and the personnel in charge of it.

The second part: It is the offensive part, since after the cyberspace turned into a field for international interactions, many patterns appeared for its uses of a civil or military nature, making this space a field for various conflicts between states or non-states in order to achieve the greatest degree of influence and influence on them.

2- The forms of cyber warfare:

A. Viral Information War

It occurs through an electronic attack on communication networks by a variety of information viruses, including: the system virus, the software virus, the multilateral virus, worms, the robot, the translator virus, the Flame virus. The Flame information virus is described as an information weapon aimed at embezzling documents in the form pdf. The effect of using viruses is doubled, as it involves directing an army that includes a large group of computers connected to a single network loaded with viruses. They are controlled remotely in order to confront the target system with a number of commands and spread viruses in it with the aim of paralyzing it[xvii]. There are five cyber-attacks that are the most popular:

* Phishing attacks: They are represented in phishing a large number of victims by sending thousands of e-mail messages, and they are used to steal user data.

* Ransomware attacks: Designed to block file access, threatening to release victim data unless the ransom is paid.

*Denial of Service Attacks: Disable websites by flooding a system or network with more requests for access than it can handle.

* Phishing: It is mostly used by cybercrime crews who want to bypass antivirus software.

* A data breach attack is exploited by hackers through a vulnerability in the site to steal customer data such as email addresses and phone numbers.

B. Remote controlled weapon system:

Controlled by cyberspace, unmanned aircraft are a prominent example of remote-controlled weapon systems. These aircraft have enhanced the capabilities of real-time air control, which led to an increase in the forms of precautionary measures that can be taken before launching an attack. X-47, the new model of unmanned aircraft was launched in 2013. This aircraft, in addition to other similar types, represents a development in weapons technology [xviii].

Second axis

International Security

Studies have appeared international security as a scientific field in the forties and fifties of the twentieth century, in parallel with the pressures of realist theory in the study of international relations, especially in the writings of Edward and Hans Morjantha. This parallel had its impact in determining the basic premises and central issues of international security studies to reflect a conformity with the realistic vision in relations International[xix]. This axis will be addressed through:

First: the definition of international security

Second: Cooperation between states to achieve international security

First: the definition of international security

1- Linguistic definition of the concept of security:

Security in the Arabic language means tranquility and lack of fear.

2- Idiomatic Definition:

The concept of security is considered one of the most controversial political terms because it is related to the survival and continuity of individuals and states. The concept of security differs in its definition according to the theory through which the concept is considered. Security according to the realistic theory is state security in the sense that it refers to regional integration, political stability of the state and social cohesion. Thus, the security of the individual and the group must be contained [xx].

Another definition of security is the ability to be freed from a major threat
to individual and collective higher values.

Barry Buzan argues that in the case of security, the debate is about the pursuit of freedom from threat [xxi].
Security includes confronting any threat that would curb human freedom[xxii] .

3- Defining international security:

International security is considered the broadest unit of analysis in security studies, because it is related to the security of each member state in the international system. International security is the security relations between states[xxiii].

International security includes military and diplomatic measures taken by states and international organizations to ensure mutual safety and security throughout the world. It includes the multiplicity and overlapping of international interests. The structure and map of security threats have changed from the traditional type to a new one, especially with regard to technological and technical development to achieve international security. There must be collective action mechanisms, including:

A- Force Balance System:

The basic idea of this system is that conflict is the distinguishing feature of international relations, where states vary in relative strength, and also differ in their national interests. Each state seeks to maximize its gains at the expense of the other, especially if a state gains superiority in its capabilities and strength. The situation in which the distribution of power between a number of countries is relatively uneven, so that no country has the ability to impose its hegemony over other countries. The balance of power is achieved in two cases:

- Preserving international peace by gathering in counter-axes against the forces of threat, with the aim of achieving deterrence.
- Finding equal axes of power for countries with different goals[xxiv] .

B- Collective security system:

That system appeared as a reaction to the system based on a balance of power/ This system does not mean the end of the existing contradictions in the interests of states, but the denial of armed violence as a tool for resolving it and focusing on peaceful means. In order to achieve collective security, the following is required:

- Considering peace indivisible, and it follows from this principle that states accept the sacrifice of freedom of action and waive the right to make national decisions and adhere to the pattern of work imposed by the collective security system. This principle requires the availability of the following:
  Respecting international obligations related to the maintenance of international peace and security.
  - Respecting international obligations related to the maintenance of international peace and security.
  - Settling disputes by peaceful means.
  - Non-interference in the internal affairs of states.

Second: Cooperation between states to achieve international security

With the presence of threats to states in the global information society, the issue becomes linked to international security. Therefore, the first attempt was to establish an international treaty to monitor cyberspace and related matters in 2001. The United Nations played a role through its resolutions that support security and safety in cyberspace. It also played a role in drawing the attention of Member States to the importance of cyber challenges. The United Nations has made several efforts by specialized working groups with the support of the International Telecommunication Union to adopt a set of rules and standards that guarantee the peaceful use of the cyber domain[xxv], in addition to launching many initiatives undertaken by international organizations to support cyber security, such as the North Atlantic Treaty Organization that established a cyber defense unit. The International Telecommunication Union launched the Cyber Security Initiative, and the International Committee of the Red Cross has monitored all technological developments that could be using it as a means of warfare and evaluating the challenges and risks resulting from technical development. The ICRC invited a number of experts to meet to develop a realistic assessment of the potential cost of cyber operations,[xxvi] in addition to the efforts of countries in this regard, as the United States of America adopted the International Strategy for Cyber Judiciary, which is the first political document of this kind that outlines the comprehensive vision for the future of international cooperation related to cyberspace.

1 - The international response to address cyber-attacks:

The international response to addressing cyber-attacks has been recorded in the “Tallinn Handbook” [xxvii], which searches for the possibility of applying international law to cyberspace. This guide has dealt with a number of concepts such as cyber siege, cyberspace, attacks accompanied by the use of force. These concepts are subject to international humanitarian law, and Tallinn Law was prepared by a group of international law experts at the invitation of the center of the Cooperative Franchise for Defense of the Cyberspace of the North Atlantic Treaty Organization. It was intended to study the extent to which the rules of international humanitarian law can be applied to cyber wars.

This guide answers how to manage cyber war through the rules of cyber engagement, the description of the cyber fighter, in addition to the possibility of observing international humanitarian law known as the principle of distinction and the legality of targeting the cyber fighter by physical military means, such as military drones [xxviii]. The Tallinn Manual acknowledged that cyber-attacks alone may constitute armed conflicts depending on the circumstances, especially the devastating effects of those attacks. The guide clarified the restrictions and limits imposed by the application of some rules of international humanitarian law to cyber-attacks, such as: * The rule of obligation to take precautions.

* Prohibition of indiscriminate attacks whereas indiscriminate attacks that would harm civilians are prohibited[xxix]. The Tallinn Manual is the most comprehensive procedure that seeks to interpret the rules of international law in the context of cyber warfare, and also the text of the Tallinn Manual on the precautionary principle, as it looks at the complexity of electronic operations and the high potential for damage to civil systems[xxx] .

2- The legality of using cyber force:

Cyber wars were not known until recently, which constituted one of the most important current challenges faced by specialists in international law, especially with regard to determining their nature or elements.[xxxi] Therefore, the emergence of cyber wars as one of the repercussions of conflicting technological developments in the world represented a challenge to the Charter of the United Nations, especially since it is prohibited in Article (2), Paragraph (4). The use of force or threats to use it in international relations requires the intervention of the international community in order to maintain international peace and security from threats[xxxii]. The UN Charter, the Geneva Conventions of 1949, the Hague Conventions of 1899 or 1907, and the North Atlantic Treaty do not address "cyber conflict", as the UN Charter and the North Atlantic Treaty use terms such as territorial integrity, use of armed force and armed attack. These terms do not align with perceptions cyberspace, ostensibly placing it outside the scope of international law[xxxiii].

The international custom is that the force intended to be prohibited is military force. In this case, the question arises whether the use or threat of using cyber force falls under the scope of military force or is it outside the scope of the ban.

Therefore, a distinction must be made between two types of cyber-attacks. If the attacks are of a military nature and result in the same results as the physical use of military force, then this type of cyber-attack applies to the aforementioned prohibition. If cyber-attacks constitute, depending on the circumstances, an armed conflict, in this case the term cyber war applies to them, because it is considered an electronic process, whether offensive or defensive, that is expected to cause injury or death to people. Therefore, cyber-attacks can be a reason to start a war[xxxiv]. However, if the electronic attacks are of a non-military nature, their results are of a social or economic nature, such as electronic psychological warfare, which is the use of modern media and Internet services to publish certain ideas and directives in order to influence the masses and decision-makers by sending electronic means through Mobile phone or e-mail, which contains threatening means or includes certain demands. Such a type is not seen as a use of military force in its traditional form, although it can be viewed as one of the sources that threaten security in general. Dealing with it requires penalties Less than stipulated in the prohibition of the use of armed force [xxxv].

The third axis
Cyber wars and their repercussions on international security

The increasing global reliance on information and communication technology has led to an increased vulnerability to attacks through cyberspace, as cyberspace has become vulnerable to violations by network intruders, whether they are countries or non-states who own these information technologies. In 2007, the role of

cyberspace as a new field in Hostilities in the conflict between Estonia and Russia, and thus cyber security has become among the foreign policy priorities of many countries. Many countries have adopted strategies that would support the military side in cyberspace. The axis will be addressed as follows:
First: Legal conditioning of cyber wars according to their intensity and extent
Second: the models of cyber warfare
Third: Cyber security at the international level
Fourth: The means taken by countries to confront cyber wars

First: Legal conditioning of cyber wars according to their intensity and extent

The first pattern: low-intensity cyber cold war:

In this pattern, cyberspace is used as a low-intensity conflict arena, as it is an ongoing conflict between conflicting actors. The soft power of cyber wars is usually resorted to in such conflicts. [xxxvi] This type of war has multiple means, including espionage, psychological warfare, multiple penetrations, waging a war of ideas, and information theft.

An example of this is the accusation that Russia was subjected to electronic hacking in the American elections to support the Republican candidate Trump in the face of a competitor. In addition, Iran launched cyberattacks on oil facilities in the Persian Gulf region, in protest of allegations of discrimination against Shiite minorities, as well as the Doku virus attacks in 2012 and Shamoon virus attacks against Saudi Arabia in January 2017[xxxvii].

The second pattern: is medium-intensity cyber warfare

In this pattern, the conflict is transformed through cyberspace as a parallel arena or linked to a conventional war on Earth, and historically, medium-intensity cyber warfare was used in the 1999 NATO attacks on Yugoslavia, where cyber-attacks aimed to disrupt the communication networks of opponents.[xxxviii] This pattern emerged during the war between Hezbollah and Israel in 2006, as well as the cyberattack carried out by Israel on 12/6/2007 on one of the Syrian facilities suspected to be a nuclear facility in the city of Deir ez-Zor. This led to the disruption of these defenses in order to enable The Israeli warplanes bombed this site without the attack being detected[xxxix]. as well as between Georgia and Russia in 2008[xl] .

The third pattern: high-intensity cyber warfare

This pattern expresses the emergence of wars in the cyberspace. This type of warfare involves the control of the technological dimension over the management of military operations, where electronic weapons are used only against enemy facilities. Therefore, electronic power is acquired. Electronic weapons have witnessed greater development in their ability to influence opponents, such as high-powered microwave weapons and electronic attacks through viruses. The world has not witnessed this type of war as a result of destructive effects through penetrating high-tech military operations or targeting civilian life and infrastructure. However, there are examples of those wars represented in the form of threat means and are accompanied by limited effects as a result of these attacks. It is expected that the third type of cyber wars will be present in the future with the development of technological capabilities, as this pattern has imposed itself recently as an effective multi-tasking weapon in military battles. countries have sought to own it because of its importance in striking the enemy at a low cost.

Second: the models of cyber warfare

The international community began to care about cyber wars since 1990. The international interest in information warfare increased after the events of September 11, 2001, as well as after the cyber-attacks on April 27, 2007, which were carried out against Estonia. Cyber wars have become afflicting many countries and many organizations. The following table No. (1) shows the most prominent cyber-attacks:

Year	The accident	Influence	Determining the Source in the General System
2007	Cyber-attacks on Estonia	Massive server blocking attacks on Estonian websites in the context of tension with Russia	The Estonian government has accused Russian state actors
2007	Cyber-attacks on the Syrian nuclear reactor project in Deir Ezzor	A cyber-attack on Syrian air defenses with the aim of disabling and jamming them before the planes enter	Israel[xli].
2008	A cyber-attack on Georgia coordinated directly with a land, sea and air attack	Computers have been hacked and infected with malicious software for the "Computer Control and Monitoring" server by issuing commands to these robots	Russia[xlii].
2009	Cyber-attacks on ISPs in Kyrgyzstan	Disrupting the flow of information on the Internet	The source is not specified
2010	Cyber-attacks on Iran	Material damage to Iranian centrifuges, computers were damaged, and more than 1,000 centrifuges were destroyed, in addition to sending false information to the control rooms.	The United States of America and Israel, according to leaks by American officials.
2012	Distributed blocking of service attacks on US banks.	Influence on more than 46 of the most prominent financial institutions in the United States.	Iranian state actors were indicted in March 2016.
2012, 2016	Aramco Saudi Arabia	35,000 Saudi Aramco computers were scanned or destroyed, and a similar attack occurred in late 2016.	In 2012 US officials linked the attack to Iran in the media
2014	The White House and the State Department of the United States of America	Massive hack of unclassified computer systems	The US government has not officially identified the source
2014	Cyber-attacks on the White House and State Department networks	Hacking into the White House's networks	Russian hack
2015	The communications system in Ukraine has been subjected to a cyber attack	The attackers used equipment installed inside the Okratecom networks, compensated in the area of the Crimean network of special Russian control, and this led to the closure of three power plants in Ukraine	The source is not specified
2016	Hillary Clinton campaign cyber-attack	Hacking the election campaign of Hillary Clinton and the Democratic Party and trying to influence the presidential election	The source is not specified
2018	Cyber-attacks to infiltrate hundreds of American universities and companies	Hundreds of universities and companies have been hacked for the purpose of stealing research, academic data and intellectual property	The US Department of Justice has filed criminal charges and imposed sanctions on an Iranian company and 119 Iranians active in the Iranian MENA Institute.
October 17, 2019	Washington launched a cyber-attack against Tehran	Iranian databases and support centers were targeted with the aim of paralyzing Iran's capacity	United States of America

February 21, 2020	Australia under cyber attack	Penetration of the main parties and parliament	It was by hackers residing in Iran and working for a party that cooperates with the Revolutionary Guards.
February 21, 2020	Cyber-attacks in Georgia	It aims to sow division, destabilize security and undermine democratic institutions	Georgia accused Russia, according to Sky News
May 3, 2020	A cyber-attack on a group of American hospitals	Penetration into a group of American hospitals, research laboratories, medical service providers, and pharmaceutical companies	Hacking attempt by hackers and it is believed that China is behind it.
July 17, 2020	Cyber-attacks on institutions involved in the anti-Covid 19 vaccine	set mounted" APT29 Cyber-attacks on organizations involved in developing the COVID-19 vaccine in Canada, the United States of America and the United Kingdom	The British National Cyber Security Center confirmed that this was for the benefit of the Russian intelligence service, according to “BBC".
September 18, 2020	Cyber-attacks to steal data from Spanish intelligence	Data theft from Spanish laboratories seeking to develop a vaccine against Covid 19	Chinese pirates
December 2020	A cyber-attack on the websites of a number of important ministries in the United States of America	Hacking the websites of a number of important ministries, including the Ministry of Defense, Foreign Affairs, Trade, Energy, and Internal Security	An accusation that the Russian intelligence orchestrated it [xliii].
December 2020	Company attack Solar winds whose products are used by US federal and state agencies and major US corporations	The breach affected nearly 18,000 customers and more than 100 American companies	The United States accuses Russia of masterminding the cyber attack
February 2021	The famous Canadian aircraft manufacturer Bombardier suffered a data breach	Hacking confidential data of suppliers, customers and about 130 employees in Costa Rica	The source is not specified
March 2021	Exposing companies and government agencies in the United States of America that use Microsoft's email service to hack	At least 60,000 organizations have been hacked globally, and many of the victims are small or medium-sized businesses stuck in a vast network used by the attackers.	China has been accused of this

March 27, 2021	A cyber-attack targeting the Australian Parliament and Channel Nine TV	As a result, the Australian Parliament's employees were prevented from accessing their e-mails. As for Channel Nine, the broadcasting of programs was completely disrupted, and the channel's management was unable to broadcast the recorded weekend programs.	The source is not specified
March 2021	One of the largest electronic insurance companies in the United States of America CN Financial for ransom attack	This led to the disruption of customer and employee services in the organization for 3 days, and the company was forced to close to prevent further bargaining	The source is not specified
July 3, 2021	Several US networks have been exposed to a cyber attack	American companies, the information group SolarWinds and the oil pipeline network "Colonial Pipeline" have been attacked by ransomware	Attributed by the US Federal Police to hackers in Russia
July 2021	Morocco's use against France of the "Pegasus" spyware program, which is produced and licensed by the Israeli company "NSO".	Attempt to hack 37 smartphones belonging to journalists, officials and activists in the field of defending human rights	Moroccan intelligence services, according to "Media part"
July 2021	The American company Cassia, which provides many companies with information technology services, is exposed to a cyber attack	Demanding more than a thousand companies using its system to pay a ransom, as the Swedish company "Kop Sweden" announced that the attack paralyzed its activities, which represent about 20% of the sector.	The source is not specified

Source Prepared by the two researchers

Third: Cyber security at the international level

The international community has witnessed trends of transformation in the issue of dealing with cyber threats with the possibility of cyberspace shifting towards militarization. This appeared in several directions, and the most important of which is the development in the field of cyber security policies, and the adoption of cyber defense policies by the agencies concerned with defense and security, in addition to the escalation of the volume of investment in the field of development of cyber warfare tools within modern armies. Therefore, many countries have worked to introduce cyberspace into their national security strategy.

The interest in cyber security has spread at the international level, especially within the developed country. This was in the adoption of multiple security policies. Many countries have sought to increase the interest in cyber security, wanting to secure information systems that threaten economic growth and international security.

The International efforts in the field of cybersecurity are receiving increasing interest from the public and private sectors. A number of developed countries have sought to adopt an international strategy in the field of securing cyberspace[xliv].

1- Cyber Security Indicators

This indicator is issued by the International Telecommunication Union officially affiliated to the United Nations. This indicator monitors the improvement in the levels of awareness of the importance of cybersecurity and the measures taken to protect it. This indicator can be measured through several systems through five main pillars:

- Legal measures: They are based on the existence of institutions and legal frameworks that deal with cybersecurity and cybercrime.
- Technical measures: They are based on the presence of technical institutions and dealing with cybersecurity.
- Regulatory Measures: Measures based on the existence of institutions and strategies that coordinate policies to develop cyber security at the national level.
- Capacity building: These are measures based on the presence of research and development, education, training programs, accredited professionals, and public sector agencies that promote capacity building.
- Cooperation: These are measures based on the existence of partnerships, cooperative frameworks and information exchange networks[xlv].

The Global Cybersecurity Index has emerged as an initiative that attempts to measure countries' commitment to cybersecurity, in order to help promote a global cybersecurity culture and its integration into the core of information and communication technology[xlvi].

Indicators have been created aiming to implement internationally recognized cybersecurity standards in critical infrastructure and the public sector. Procedural and organizational measures are considered essential for developing the strategy of regulation and cooperation, as these measures are used to implement each type of national initiative with regard to cybersecurity, in addition to building Capacity that is related to the development of individuals' capabilities to adopt legal, technical and organizational measures on cybersecurity, in addition to the fact that the workforce's knowledge of technology is essential, because building human and institutional capacities is useful for improving knowledge and technical know-how across sectors, and cooperation is a prerequisite, and the exchange of information in the two sectors .The public and the private are useful, as well as at the international and national levels.

Table No. (2) shows the criteria of the cybersecurity index in some countries, according to the International Telecommunication Union report for the year 2020.

Countries	Legal Measures	Technical Measures	Regulatory Measures	Capacity Building Measures	Cooperative Measures
The United States	20,00	20,00	20,00	20,00	20,00
Estonia	20,00	20,00	20,00	19,48	20,00
Germany	20,00	19,54	18,98	19,48	19,41
Britain	20.00	19,54	20,00	20,00	20,00
Denmark	19:30	18,94	18,98	19,48	15,89
France	20,00	19,21	18,98	20,00	19,41
Spain	20,00	19,54	18,98	20,00	20,00
Poland	19,35	20,00	14,74	19,77	20,00
Japan	20,00	19,08	18,74	20,00	20,00
India	20,00	19,08	18,41	20,00	20,00
Sweden	20,00	18,86	18,46	19,57	17,70
Italy	19,68	17,56	20,00	19,48	19,41
Turkey	20,00	19,54	17,96	20,00	20,00
Israel	19,68	16,99	15,02	19,24	20,00
Cyprus	20,00	18,73	18,41	13,73	17,94
Singapore	20,00	19,54	18,98	20,00	20,00
Portugal	20,00	20,00	18,98	18,34	20,00
Greece	19,43	15,83	18,98	19,74	20,00
Russia	20,00	19,08	18,98	20,00	20,00
Lithuania	20,00	19,54	18,98	20,00	19,41
Luxembourg	20,00	19,54	18,98	19,48	19,41

Holland	20,00	19,84	18,98	18,82	19,41
Malaysia	20,00	19,08	18,98	20,00	20,00

Source International Telecommunication union, Global cyber security index, 2020, pp. 45- 128:

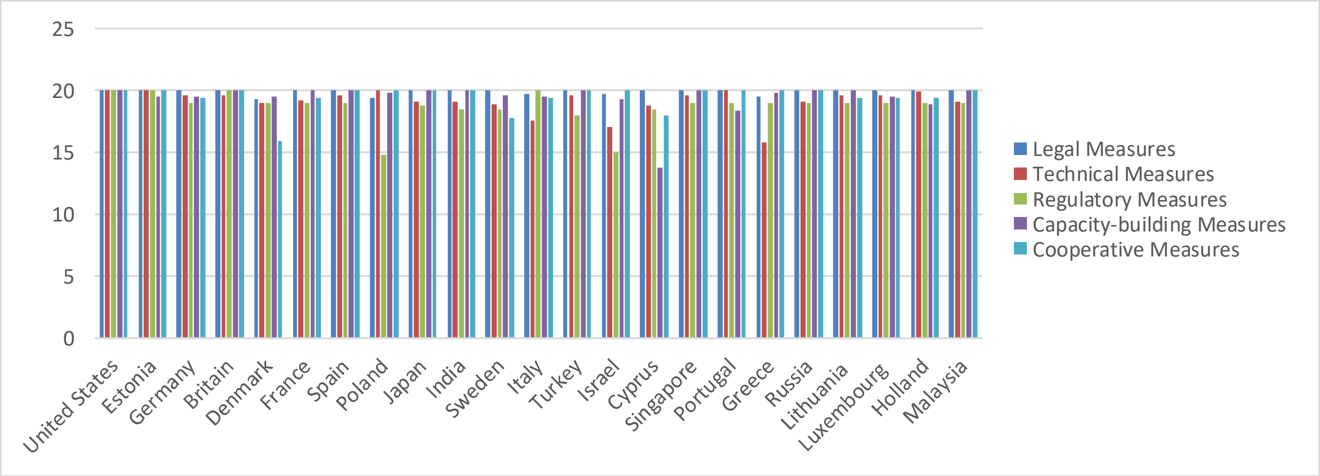

Figure No. (2) shows the criteria of the cybersecurity index in some countries

It is clear from this table and figure that the United States of America achieved all the cybersecurity indicators by 100%, but in 2017, the cybersecurity indicators were as follows: legal measures and capacity measures were achieved by 100%, and technical and organizational measures were achieved by 96% and 92% and cooperative measures by 73% [xlvii], and Germany has achieved 100% of legal and technical measures.

Table No. (3) shows the ten countries most capable of confronting cyber threats

Countries	Legal Measures	Technical Measures	Regulatory Measures	Capacity Building	Cooperation	Key Success Factors	Ranking
United States of America	20,00	20,00	20,00	20,00	20,00	100	1
Britain	20,00	19,54	20,00	20,00	20,00	99,56	2
Saudi Arabia	20,00	19,54	20,00	20,00	20,00	99,54	2
Estonia	20,00	20,00	20,00	19,48	20,00	99,48	3
Korea	20,00	19,54	18,98	20,00	20,00	98,52	4
Singapore	20,00	19,54	18,98	20,00	20,00	98,52	4
Spain	20,00	19,54	18,98	20,00	20,00	98,52	4
Russia	20,00	19,08	18,98	20,00	20,00	98,06	5
UAE	20,00	19,08	18,98	20,00	20,00	98,06	5
Malaysia	20,00	19,08	18,98	20,00	20,00	98,06	5
Lithuania	20,00	19,54	18,98	20,00	19,41	97,93	6
Japan	20,00	19,08	18,74	20,00	20,00	97,82	7
Canada	20,00	18,27	20,00	20,00	19,41	97,67	8
France	20,00	19,21	18,98	20,00	19,41	97,60	9
India	20,00	19,08	18,41	20,00	20,00	97,49	10

Source: International Telecommunication union, Global cyber security index, 2020, pp25

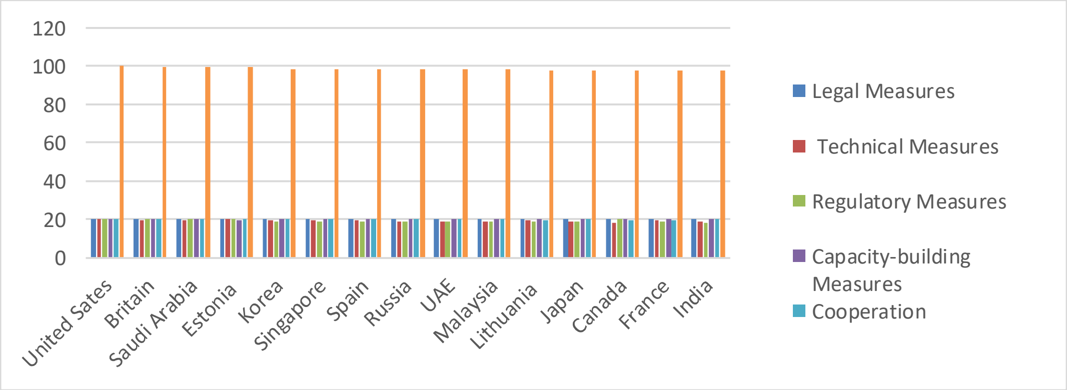

Figure No. (3) **shows the ten countries most capable of confronting cyber threats.**

It is clear from this figure that the United States of America, Malaysia and France achieve the capacity-building index by 100%, as well as the United States of America that achieves the legal measures index by 100%.

The level of cybersecurity for Arab countries was also measured in 2020, based on the same indicators.

Table No. (4) shows the top five positions in the Arab countries most facing cybersecurity

Countries	legal measures	technical measures	regulatory measures	capacity building	cooperation	Key success factors	Ranking
Saudi Arabia	20,00	19,54	20,00	20,00	20,00	99,54	1
UAE	20,00	19,08	18,98	20,00	20,00	98,06	2
Oman	20,00	16,64	20,00	20,00	19,40	96,04	3
Egypt	20,00	17,45	20,00	19,12	18,91	95,48	4
Diameter	20,00	16,94	18,46	20,00	19,41	94,50	5

Source: International Telecommunication union, Global cyber security index, 2020, pp29

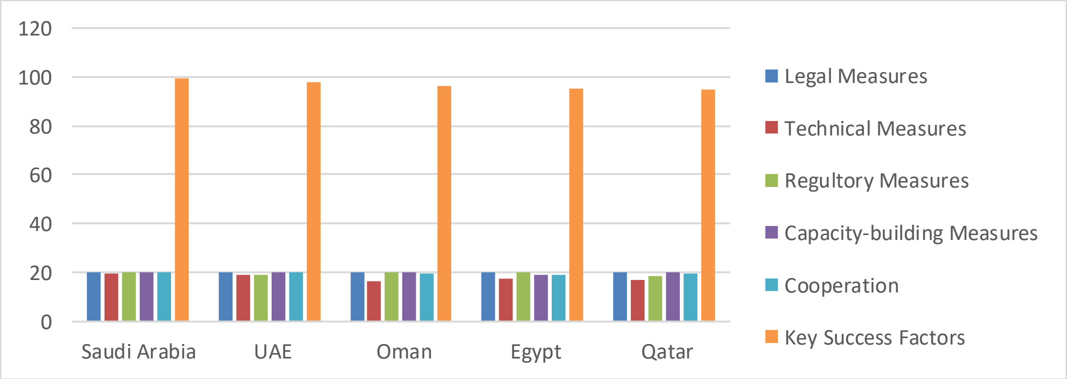

Figure (3) shows the top five positions in the Arab countries most facing cybersecurity

Through this figure, it is clear that in the 2020 report, Saudi Arabia is the highest, followed by the UAE, then Oman, and then Egypt, although in the 2017 report measuring cybersecurity indicators, Oman scored the highest percentage in legal measures, organizational measures, capacity building and cooperation, and Egypt scored the highest in technical measures. The main success factors are Oman, followed by Egypt, followed by Qatar, according to a report issued in 2017.

Fourth: The means taken by countries to confront cyber wars

The factor of cyber power is disrupting the balance of forces in the world. The major countries have created great electronic armies to remedy this gap, and the most prominent of which are the following:

- **Units per year in the USA:** In cyber wars, the United States of America relies on six elements: The American Cyberspace Command Unit, which is specialized in planning, coordinating and managing electronic warfare operations with the rest of the branches it follows.
- **British 77th Brigade:** Britain joined the 77th Brigade cyber wars in early 2015, and this brigade mainly focuses on pro-terrorist accounts on Twitter and wages psychological warfare. It consists of 2,000 soldiers.
- **Russian signal intelligence:** It is represented by groups of hackers working for the Russian Signal Intelligence.
- **Unit 61398 Chinese:** China is famous for having one of the best cyber-warfare armies in the world.
- **Office 121 in North Korea:** This office was established in 1998. North Korea has a special unit for cyber warfare, and its main targets are the United States of America, South Korea and Japan.
- **Israeli Unit 8200**: Where Israel is famous for using this unit for psychological warfare on the Internet.
- **Iran's Electronic Army**: Where Iran has emerged as a power in cyber wars[xlviii].

As a result of the tensions and high-level political challenges and international crises caused by cyber wars, and devastating effects on infrastructure, the economy, and international and regional security, many constitutions, seminars, conferences and studies called for caution in dealing with cyberspace and its attacks.

An example of this is the Egyptian constitution. Article (31) of the Egyptian constitution in January 2014 has been dedicated to the National Cyber Security Strategy (2017–2021) and stipulated that cyberspace security is an essential part of the economy and national security system. The state is obligated to take the necessary measures to preserve it as specified by law. One of the most important things called for by the strategy is the preparation of human cadres and expertise necessary to activate the cybersecurity system in various educational sectors, as well as supporting scientific research and development and industry development.

In addition to the efforts of countries to confront cyber wars. Countries have begun to form specialized bodies in cyber security and their mission is as follows:

- Developing national coding policies and standards.
- Preparing a national strategy for cyber security.
- Raising awareness of cyber security.
- Developing frameworks for responding to accidents and breaches.

In addition to countries resorting to the work of forming specialized bodies in cybersecurity and their interest in it and making it a part of national security. This is because internet networks do not recognize traditional borders, as cyberspace has made national borders fictitious, because the interactions between networks have made borders intangible and generally operate outside the control of states. This represents a new form of weapons that expose civilians to many dangers.

Research Results:

- Cyber wars are more dangerous than military wars because they are able to destroy systems and devices, preventing them from working completely and destroying them.
- The recurrence of cyber-attacks will increase the interest in information security, in addition to the increasing interest of countries in developing strategic, safe and military information base security systems.
- The issue of cyber security has become an international issue.
- The agreement of international efforts on regulating the use of cyber wars, and the interest of each country in cyber security, as centers were established within each country in order to prepare specialists and experts in cyber defense technology to repel any possible cyber war on civil and military facilities.
- The rules of international humanitarian law did not refer to cyber operations in particular, but the absence of specific references in that law does not mean that these operations are not subject to the rules of international humanitarian law, but rather are subject, through its general rules that regulate all methods and means of warfare.

Recommendations

- Modernizing defensive and offensive capabilities, as countries must seek to modernize defense activity to face the dangers of cyber war.
- Investing in and securing information infrastructure.
- International participation in the protection of the information infrastructure.
- Inclusion of informational viral warfare in cyberspace within the concept of aggression.
- Countries have appropriate cyberwarfare systems in order to help prevent countries from becoming havens for terrorist acts that attack information technology systems.

[i] Mearsheimer, John J.," Rockless states and realism", international relation, Vol. 23, No.2, 2009, p. 241 - 242 .

[ii] - Munir Baalbaki, Al-Mawred: An English-Arabic Dictionary, Beirut: Dar Al-Moallem for Millions, 2004, p. 243.

[iii] Richard Kissel, Glassory of key information security terms, National institute of standards and technology,Us Department of commerce,may 2013,p 57

[iv] Andress, J., winter Deld, S.,"What is cyber warfare", in: R.Rogres(ed.), cyber warfare: Techiniques, taxtics tools for security paretitioners, New York, Esevierinc, 2011, p2.

[v] Salama Tariq Al-Shaalan, "Adapting the Use of Electronic Warfare in Armed Conflicts According to International Humanitarian Law," Kufa Journal of Legal and Political Sciences, No. 26, 2016, p. 125.

[vi] - Herbert Leith, "Cyber Conflict and International Humanitarian Law", Journal of the International Committee of the Red Cross in: www.icrc.org

[vii] - Mosaed Kamal, Virtual War and Simulation of Reality Scenarios, Lebanese Army Magazine, Arab Thought House, 2007, p. 65.

[viii] Paulo ∞ Jana Shakarian, Andrew ReueF, Introduction to cyber war fare, Amultidis ciplinary approach, Elsevier, 2013, P3.

[ix] - Adel Abdel-Sadiq, "Cyberspace and Public Opinion: Society Change, Tools and Influence," The Arab Center for Cyberspace Research, Strategic Issues, No. 2459, 2013, p. 35.

[x] - Hamdoun Iturieh, The Search for Cyber Peace, International Telecommunication Union, 2011, pp. 6-7.

[xi] - Hassan Muzaffar Al-Razzo, Information Space, Beirut: Center for Arab Unity Studies, 2008, pp. 213-214.

[xii] - Lawrence Lessig, The Code Organizing Cyberspace, translated by: Mohamed Saad Tantawy, Cairo: Hendawi Foundation for Education and Culture, second layer, 2006, p. 31.

[xiii] - Salah Mahdi Hadi and Zaid Muhammad Ali, "Cyber security as a new anchor in the Iraqi strategy," Al-Nahrain University, Political Issues Journal, No. 62, 2020, p. 277.

[xiv] Canongia, C., ∞ Mandarino, R., Cyber security, the new challenge of the information society, in crisis management concepts, methodologies, tools and applications, 2004, p.67.

[xv] - For more on the factors that led to the possibility of developing cyber wars, see: Mohamed Abbas Mohsen, Cyber Attacks and the Legislative Vacuum Zone: A Study in the Charter of the United Nations and International Law, Algeria /: Alef for Publication and Distribution Documents, 2021.

[xvi] - Sherif Hashem, "Towards a National Cyber Security Strategy: Presidency of the Council of Ministers: The Supreme Council for Cyber Security, in www.cutt.ly/ Bppyn3F .

[xvii] - Adel Abdel-Sadiq Muhammad, The Impact of Cyber Terrorism on the Principle of Using Force in International Relations, Master Thesis, Cairo University, Faculty of Economics and Political Science, 2009, p. 152.

[xviii] Hagar shriveled, "The legal status of cyber war in light of the rules of international law "Journal of Communication in the Humanities and Social Sciences, No. (3), September 2019, p. 158.

[xix] - Sally Khalifa Ishaq, "Modern Trends in International Security Studies", in: www.alademia-arabia.com .

[xx] - Mustafa Alawi, "Notes on the Concept of Security", Al-Nahda Magazine, No. 5, 2002, pp. 123-124.

[xxi] Barry Buzan, people state and Fear: An Aganda for international security stadies in the post cold war, Bonlder : Lynne Rienner Publishers, 1991, p.18 .

[xxii] - Naima Khudair, "Security as a Rubber Concept in International Relations - The Problem of Definition and Employment", in: www.univ-jijel . dz .

[xxiii] - Mustafa Alawi, aforementioned reference, p. 124.

[xxiv] - Lakhmis Shaib, "A Reading in the Concept and Theories of International Security, Algerian Encyclopedia of Political and Strategic Studies", 2018, in: www.politics.dz.com .

[xxv] - Mona Al-Ashqar Jabbour, The Syriac Hajes Al-Asr, Beirut: The Arab Center for Legal and Judicial Research, 2017, p. 104.

[xxvi] - www.icrc.org

[xxvii] The Tallinn Handbook is a non-binding academic study applicable to cyber conflict and electronic warfare, written at the invitation of the NATO Cooperative Cyber Defense Center of Excellence in April 2013.

[xxviii] - Said Darwish, "What is electronic warfare in light of the rules of international law", Annals of the University of Algiers, No. 29, 2018, p. 131.

[xxix] - Saber Belqas, "Cyber attacks and confronting them in the light of contemporary international law," Journal of Human Rights and Public Freedoms, No. 4, 2017, pp. 201-202.

[xxx] - Amir Faraj Youssef, Combating Electronic Terrorism: Digital Terrorism in the Light of the GCC Agreement, House of Arab Books and Studies, 2016, p. 253.

[xxxi] Eneyew, yohannes, The impact of cyber war fare under international humanitarian law: Acritical legal analysis, PHD, school of law, wolo university, 2014, p6.

[xxxii] - Ihab Khalifa, "When does the United Nations Charter prohibit the use of cyber force", International Politics Journal, 2017, at: www.siyacsa.org.eg .

[xxxiii] - Moussa Bin Ta'zi Moussa, "Cyber War and International Humanitarian Law," Journal of Judicial Jurisprudence, No. 2, April 2020, p. 206.

[xxxiv] Philip levitz, The law of syber - Attac, Vol. 100, issu4, 2012, p 833.

[xxxv] - Nesma Younes Muhammad Al-Rafadi, "Cyber wars and their impact on the international organization," Journal of Science and Human Studies, No. 49, February 2018, pp. 9-10.

[xxxvi] - Raghda Al-Bahi, "Cyber deterrence, concept, problems and requirements", Algerian Encyclopedia of Political and Strategic Studies, No. 4741, 2019, p. 58.

[xxxvii] Saudi Arabia warns on cyber defense as shamoon resur face, Technology news, Routers, 2017, in : www.reuters.com.

[xxxviii] Florian Bieber, cyber war or side show the international and the ballan wars, at : www.search.proghest.com

[xxxix] Heather Harrison Dinniss, The status and use of computer network attacks in international law, PHD, thesis, school of economics and political science, 2008, p.33.

[xl] Robert Mc Million, was stuxnet built to A hackiram's nuclear program, in : www.pc world.com

[xli] Applegate, cyber conflict idisruption and Exploitation in ther digital ago, in: lemieux, Frederic, current and emerging trends in cyber operation: policy, strategy and practice, pp. 19-20

[xlii] Paulo shalariun, The 2008 Russian cyber.campaign against Geolgia Military review, pp. 63-64.

[xliii] - Ali Al-Din Hilal, "The New Syriac Wars", Al-Ain Al-Akhbariya, 2021, at: www.al-ain,com

[xliv] - Gharib Hakim, "Cyber-terrorism and International Security: New Global Threats and Methods of Confrontation", Algerian Journal of Political Studies, No. 2, 2018, pp. 114-115.

[xlv] - Bassem Ali Khreisan, Cyber Security in Iraq: A Reading of the Global Cybersecurity Index 2020, Iraq: Al Bayan Center for Studies and Planning, 2021, p. 9.

[xlvi] International telercommunication (TTu), Global cyber-security index ∞ cyber wellness profiles, Report Geneve, AB, research Telecommunication development sector, 2015, P 129

[xlvii] International Telecommunication union, Global Cyber Security Index, 2017, pp. 15-17

[xlviii] - Ahmed Shendi, "Cyber wars and digital globalization", in: www.elbalad,news.