Journal of el hikma for philosophical studies
Issn : 2353-0499 Eissn :2602-5264

Volume:11 / N°: 01(2023), p 1092-1106

Cyber warfare in the new media age

الحروب السيبرانية في عصر الوسائط الجديدة

Mekbel Nassima[1],

مقبل نسيمة

[1] professor lecturer A in faculty of information and communication sciences
University of Algiers 3
nassmekbel@yahoo.fr

Received: 16/12/2022 *Accepted: 09/02/2023* *Published:05/03/2023*

Abstract :

Due to the nature of cyberspace and new media , as a global arena that transcends state borders, the issue of cybersecurity extends from within the state to the group of the international system, and with risks threatening all actors in the global information society, the issue becomes linked to global security. And "cyber war" as means and methods of combat that consist of operations in cyberspace that amount to or take place in the context of armed conflict.

This is what we will try to address through this research paper, while showing methods of international control and protection from the dangers of these devastating wars of cyberspace and real space. This is done by using the descriptive survey method and the scientific observation tool to try to describe the phenomenon of cyber wars and to show its dangers and ways to prevent it.

Keywords : cyberspace , new media , cybersecurity , cyber war .

.

***Corresponding author**: Mekbel Nassima*

الملخص :

نظرًا لطبيعة الفضاء السيبراني ووسائل الإعلام الجديدة ، كساحة عالمية تتجاوز حدود الدولة ، فإن قضية الأمن السيبراني تمتد من داخل الدولة إلى مجموعة النظام الدولي ، ومع المخاطر التي تهدد جميع الجهات الفاعلة في مجتمع المعلومات العالمي ، فإن القضية تصبح مرتبطة بالأمن العالمي. و "الحرب الإلكترونية" كوسائل وأساليب قتال تتكون من عمليات في الفضاء الإلكتروني ترقى إلى مستوى النزاع المسلح أو تحدث في سياقه.

هذا ما سنحاول معالجته من خلال هذه الورقة البحثية ، مع توضيح طرق الرقابة الدولية والحماية من مخاطر هذه الحروب المدمرة للفضاء السيبراني والفضاء الواقعي معا. ويتم ذلك باستخدام منهج المسح الوصفي وأداة الملاحظة العلمية لمحاولة وصف ظاهرة الحروب السيبرانية وبيان مخاطرها وطرق ردعها.

الكلمات المفتاحية : الفضاء السيبراني ، الوسائط الجديدة ، الأمن السيبراني ، الحروب السيبرانية .

1. INTRODUCTION

Since the beginning of the eighties of the last century, the world has been experiencing an unprecedented technological revolution, which is the information and communication technology revolution.

The most important consequence of this revolution in the field of media, information and communication is the spread of the Internet, whose scope is not limited to benefiting from the techniques of merging sound, image and data with one carrier, but rather it has pushed economies and societies based on raw materials and energy to economies and societies based on information and knowledge. Horizontal organization, highly efficient human resources.

On this basis, the network is no longer just a tool of communication and communication between two specific parties, but rather, by virtue of its openness and flexibility of navigation within it, it has become a “middle” in whose “space” portals, websites, blogs and cyber wars operate.

And with the transformation of cyberspace into an arena for international interactions, many employment patterns emerged for it, whether in terms of uses of a civil or military nature, which made this space a field for various conflicts, whether for state or non-state actors to possess the greatest amount of influence and cyber influence. .

In this context, the phenomenon of "cyber wars" crystallized, which was characterized by different characteristics from its traditional counterparts, in terms of the nature of hostile activities, actors, and influences on the structure of global security.

That war expressed two types of power (soft and hard) in the process of employing interactions in cyberspace, which reflects the growing capabilities and escalating threats to the security of the global information infrastructure.

Therefore, we will try, through this research paper, to answer the following fundamental question:

What is the strategy to confront cyber wars?

In order to answer this fundamental question, we divide it into a set of sub-questions as follows:

-What is the concept of cyber warfare?
-What are the forms and types of cyber warfare?
-What are the risks of cyber wars?
-How can counter cyber wars?

The importance of this study is highlighted as follows:

-The concept of cyber warfare is considered among the new concepts of the communication phenomenon, and it is considered an additional entry point for monitoring developments in the field of conflicts, and the accompanying manifestations of violence and electronic crime.
-The study is considered a contribution to the discussion of a very important topic that has not been sufficiently given its right to discussion and analysis in scientific studies.
-The study is considered a reference in building the foundations of a service cyberspace that is free from all violations and cybercrime

The methodology used in this study is represented in the use of methodological methods imposed by the importance of the study and its general objective, as imposed by the treatment, discussion and analysis of the subject of cyber wars, which necessitates the need to choose the appropriate research method and tools that raise the problem, namely:

The survey method "which is considered one of the most prominent methodological methods in the field of media studies, which represents an organized scientific effort to obtain data and information about the phenomenon or a group of phenomena under study" (Samir Muhammad Hussein, 1995, p. 132)

This methodology is also used in studying the problem and decomposing it into its hierarchical elements, in order to reach useful implications.

Based on this, the researcher resorted to the use of analysis and interpretation, to come up with logical conclusions in order to answer the questions of the study.

Through this study, we wanted to know the relationship between the new media as a communication medium and the phenomenon of cyber wars and its manifestations in the social, political, cultural and economic reality and the strategy to confront it.

As for the tools used, the researcher presented the research contributions related to what cyber warfare is, in terms of concept, characteristics, features, and types based on the study's questions, and using the observation tool, then scrutiny and analysis to extract results.

Accordingly, we can address the main axes that make up the subject under consideration as follows :

1 . The history of the emergence and development of cyber warfare :

We can say that the first use of the term “cyber” was in the first quarter of the second half of the last century, which was mentioned by the writers Kleins and Klein in their articles to indicate between humans and electronics together. After that the extent of use of this term was rather small

In 1983, Hollywood released the movie “War Games”, which tells the story of an amateur boy and a computer genius, who can penetrate the main apparatus of the US army, causing a global crisis that almost ends in World War III.

This movie was a spark that prompted many to wonder about the possibility of actually achieving what came in the movie, and is it impossible or not! They did not realize that the matter might be a simple presentation of what will happen later due to the cyber war that will invade the whole world . (Al-Ramahi , 2022 , p 19)

After the wide, large, and rapid spread of computers and the Internet from America and developed countries to the rest of the world, fears began to increase among everyone that this could be achieved.

Then an American committee specialized in protecting infrastructure issued a report in 1997 AD, in which it called for thinking differently from the stereotype that everyone thinks about security in general and cyber

security in particular, and its repercussions on the global situation and its effects in light of the tremendous development of digital technology.

In light of all this development and the fears that surround the world about cyber warfare and its dangers, the United States formed a “red team” specialized in detecting vulnerabilities in the American digital network, and it was considered as the cyber army of America, as it discovered all the loopholes that constituted a weakness for the United States.

Cyberwar attacks increased until the beginning of the current century, when the term cyberwarfare began to appear more and more widely in 2003 when a group of Syrian hackers affiliated with the Syrian regime launched electronic attacks on global websites and spread false news on them regarding the White House, and after that the various attacks followed, which It was under the cover of cyber warfare. (Al-Ramahi , 2022 , p 23)

The great and most developed countries were the most vulnerable to these attacks, represented by the United States of America, Russia and other great countries. The United States, which was subjected in 2014 to about 100,000 electronic attacks and multiple intrusions.

It is noteworthy that the pirates did not find out about them at the beginning of the attacks for long periods after the occurrence of the attack, as it was somewhat difficult at the beginning.

2 . The concept of cyber warfare:

The content of cyberwar is related to the military applications of cyberspace, as it means - in one of its definitions - that a state or non-state actors launch an electronic attack within a mutual framework, or by one party.

Although the name "electronic warfare" is widely known in the media, it is an old term that was mainly limited to monitoring cases of jamming of communication systems, radar, and alarm devices, while the current reality in cyberspace reveals the entry of communication and information networks into the structure and scope of military uses.(Abdel Sadiq ,2011 , p 15)

With the expansion of electronic hostilities to the information infrastructure of countries to achieve overlapping purposes (political, economic, criminal, etc.), the concept of electronic warfare carried new dimensions, and some preferred the term “cyber war” as an expression of

that new trend, although the word “war” remained The same is a matter of controversy, especially since there are many names given to these hostile electronic activities, including, for example, cyber attacks, cyber terrorism, and others.

According to the traditional concept of war, it involves the use of regular armies, is preceded by a clear declaration of a state of war, and a defined battlefield.

While cyberspace attacks appear to have an undefined scope and vague goals, as they move through information and communication networks that transcend international borders, in addition to their reliance on new electronic weapons that fit the nature of the technological context of the information age, as they are directed against vital facilities, or planted by intelligence agents.

From this, it seemed that hostilities in cyberspace - if they are not described as war - are called terrorism.

This matter does not carry a moral evaluation of it as much as it is an expression of the nature of technical cyber attacks, and the methods of their occurrence. These attacks depend on intimidation, fear-mongering, the anonymity of the source, or even the actual size of the losses, or the manner in which they were carried out.(Williamson , 2002 , p 16)

Also, these hostilities fall within the framework of "asymmetric warfare", since the party that has offensive power and takes the initiative to use it is the strongest, regardless of the size of its conventional military capabilities, which affects theories of strategic deterrence, other than the inability to distinguish between targeting Civilian or military installations in electronic warfare attacks make it difficult to impose international protection.

The term cyber warfare also refers to the use of a set of practices and procedures that seek to inflict defects and malfunctions on the enemy’s electronic systems and means, in addition to achieving self-protection from hostile electronic reconnaissance and resistance, and achieving stability for friendly electronic systems. This is for the purposes of disrupting the

movement of the enemy, and preventing them from exploiting the friendly electromagnetic field

The cyber warfare takes place on the Internet as a battleground for it, and the attacks that are launched in it are due to political motives. Electronic strikes are directed against the enemy's official Internet sites and everything related to its networks and basic services.

Cyberwarfare is part of hybrid warfare and can have an impact on actual warfare on the ground. Disabling or hacking the data of the ministries of defense may change something from the war, but the dissemination of false information may have a greater impact, according to experts.

3 . Types of cyber warfare:

Cyberwar is divided into two main types, according to the objective of the electronic warfare campaign, namely: (Richard , 2011 , p 46)

Radiation War: It is abbreviated as (WR), and this war is considered an essential pillar in cyber warfare, as the use of electromagnetic radiation is an important part in reducing the quality levels of hostile information and data, and they are destroyed by relying on radiological research.

Data Warfare :which is abbreviated as DW, and this type is limited to exploiting data without causing destruction to it, and it ends as soon as data exchange between the two parties to the communication stops.

It is noteworthy that the radiation war is more accurate and efficient than the data war, although both wars contain data, but what distinguishes it is its ability to impose control, control and analysis on information and data, which makes the basic decision in the hands of the friend and not the enemy, and the radiological war is often waged by viruses , or jamming.

According to the concept put forward about cyber wars, several types of these wars can be put forward in terms of the severity of the conflict or not, the most prominent of which are:(Abdel Sadiq , 2017 , p 145)

The first type is a low-intensity cold cyber war:

where cyberspace is used as an arena for low-intensity conflict. This pattern expresses a continuous struggle between the conflicting actors, and it may be of an extended nature, and permanent hostile or non-peaceful activity, in addition to being deeply rooted and intertwined, and has multiple cultural, economic, or social aspects. The soft power of cyber

warfare is usually resorted to in such conflicts, although it does not necessarily evolve into the use of armed force in its traditional form, or the launching of a large-scale electronic war.

This cold cyber war has several means, including waging psychological warfare, multiple penetrations, espionage, information theft, waging a war of ideas, and competition between global technology companies and international intelligence services. This pattern was evident in cases of war in political conflicts with an extended social-religious dimension, such as the Arab-Israeli conflict, the Indian-Pakistani conflict, or the conflict between North and South Korea, and others.

In such conflicts, international piracy groups are active to express political or human rights positions, such as the "WikiLeaks" group and "Anonymous", as well as in cases of international crises, such as the tension between Estonia and Russia in 2007, as well as mutual penetrations between China and the United States. The United States and Russia, or between Tehran and Washington.

The second type is the medium-intensity cyber "war" mode:

where the conflict through cyberspace turns into an arena parallel to a conventional war on the ground. This would be an expression of the intensity of the conflict between the parties, and it might pave the way for military action. Here, cyberspace wars take place by hacking websites, sabotaging them, waging psychological warfare against opponents, and others.

This type of cyber war derives its intensity from the strength of its parties, and its association with conventional military action, especially in light of some estimates indicating that the cost of these wars may constitute four times the spending of their traditional counterparts, enabling a full online war campaign to be funded at the cost of a tank.

Historically, medium-intensity cyberwarfare was used in the 1999 NATO attacks on Yugoslavia, in which cyberattacks aimed to disrupt adversaries' communications networks. Also, it emerged during the war between Hezbollah and Israel in 2006, as well as between Russia and

Georgia in 2008, and the confrontations between Hamas and the Zionist entity in 2008 and 2012.

The third pattern - "hot" high-intensity cyber warfare:

Where this pattern expresses the emergence of wars in cyberspace alone, and not parallel to traditional military actions. The world has not witnessed this type of war, although the possibility of its occurrence is in the future with the development of technological capabilities, and the wide dependence between states and non-state actors on cyberspace. (Abdel Sadiq , 2017 , p 149)

4 . Forms of cyber warfare:

Wars over the long years were catastrophes that threatened the security of millions around the world, but with the great development, the matter is no longer limited to conventional wars that we experienced and used actual weapons, but has evolved to reach cyber warfare that can destroy many without a single shot being fired, We can enumerate the forms of cyber warfare in a group of points, namely : (Akart , 2015 , p 60)

• cyber attacks

It is the use of electronic force by a group of hackers in order to strike the opponent or enemy and destroy it electronically and seize its electronic systems and penetrate, manipulate and control it.

• electronic protection

It is all the attempts made by the cyber armies in order to protect the electronics of the state, and it is often of a defensive nature aimed at protecting against attacks that electronic systems may be exposed to from any sudden attack.

• **Support for cyber warfare**

It is a set of measures that are taken with the aim of providing support to protect the electronic systems in the country in anticipation of any sudden attack or threat that may harm them at the future level.

Among the methods of cyber warfare, we mention the following:

Electronic countermeasures: abbreviated as ECM, and this form is represented by taking measures that impede the enemy's electronic actions in all their forms, and striking and destroying the enemy's electronic systems, means, and equipment.

Electronic reconnaissance work: Also known as electronic support operations, it reveals the enemy's "tactics" that it intends to carry out, and its role is very important. Because it looks at the capabilities and objectives of the enemy, and these actions can be followed in the states of peace and war.

Electronic countermeasures to hostile electronic warfare measures: abbreviated as ECCM, which is the use of a number of electronic measures to resist hostile electronic reconnaissance and counter it, by implementing the highest degrees of electronic security in electronic systems and means, and among the most important measures in this method are protection of systems, and monitoring friendly electromagnetic radiation.

5. Causes and goals of cyber wars:

National interests of countries have crystallized in cyberspace, following the increasing reliance on linking their infrastructure to that space in a single networking work environment, known as the "National Information Infrastructure" (NII), such as (energy sectors, communications, transportation, government and financial services, and e-commerce). , and others). Thus, any potential threat or attack on one or all of these interests of the state may constitute a cause for a strategic imbalance, which reveals a new pattern of threats to the national security of states.

The growth of such electronic threats to the interests of states, and hence the possibility of the emergence of cyber wars, has contributed to several basic motivating contexts, the most prominent of which are: (Allou , 2018 , p 11)

1- The world's increasing connection to cyberspace, which has increased the risk of the global infrastructure of information being exposed to electronic attacks, as well as its use by non-state actors, especially terrorist groups, to achieve their goals that undermine the national security of states.

2- The decline in the role of the state in light of globalization and its withdrawal from some strategic sectors in favor of the private sector. At the same time, the roles of transnational companies, especially those working in the field of technology, have escalated as an influential player in cyberspace, especially with their technical capabilities that surpass governments.

3- The emergence of a new type of damage due to cyberattacks that can be caused by one country to another, without the need for physical entry into its territory. The increasing reliance of countries on electronic systems in all their vital facilities made the latter vulnerable to double attack, because of their overlapping civil and military features, especially since the modern technological revolution resulted in another revolution in the military fields, and the development of war techniques.

4- The low cost of cyber warfare, compared to its traditional counterparts. An electronic attack may be launched at the cost of a tank, through new electronic weapons and human skills, in addition to the fact that this attack may take place at any time, whether it is peace, war, or Crisis, and its implementation requires only a limited time.

5- The transformation of cyber warfare into one of the tools for influencing the information used in the different levels and stages of the conflict, whether at the strategic, tactical or operational level, with the aim of negatively affecting this information and its work systems.

6- Employing cyberspace in maximizing the power of states, by creating an advantage, superiority, or influence in different environments, and thus the so-called "cyber strategy" of states appeared, which refers to the ability to develop, and employ capabilities to operate in cyberspace, by merging and coordinating with Other operational areas to achieve or support the achievement of objectives, through elements of national power.

7- The escalation of risks and threats in cyberspace has led to the emergence of competition between companies working in the field of cybersecurity with the aim of enhancing global spending markets to secure the cyber infrastructure of countries, in addition to the emergence of other actors from organized crime networks, hackers, and others.

8- The wide range of risks of hostile activities practiced by state and non-state actors in cyberwarfare. States may launch electronic attacks through their security and defense agencies, and may resort to recruiting hackers or loyalists to launch attacks against opponents, without any official association. (Allou , 2018 , p 14)

the objectives of electronic warfare differ according to the nature of the objectives of cyber conflicts, as follows: (Andress , 2017 , p 69)

1- A cyber conflict of a political nature, as it is motivated by political motives, and may take a military form in which offensive and defensive capabilities are used through cyberspace with the aim of corrupting information systems, networks and infrastructure. This type of conflict includes the use of electronic weapons by actors within the information society, or through cooperation with other powers to achieve political goals.

2- A cyber conflict of a soft nature, that is, the conflict over obtaining information, influencing feelings and ideas, and waging psychological and media warfare. This is done by leaking information and using it through media platforms, which affects the nature of international relations, such as the role played by WikiLeaks in international diplomacy.

3- A cyber struggle over technological progress, as this type of cyber conflict takes on a competitive nature over the possession of the technological progress race, and the theft of economic and scientific secrets. It may extend to an attempt to control the Internet, domain names, website addresses, information control, and work to penetrate the national security of countries, without using aircraft or explosives, or even violating the borders of countries, such as computer hacker attacks, destroying websites and espionage, with what it may have. Destructive effects on the economy and infrastructure with the same power as conventional explosives.

4- Cyber conflict over information and intelligence. With the difficulty of separating intelligence activities, information gathering, and cyber warfare, or distinguishing between political and criminal use, cyberspace appears to be a more suitable environment for informational conflicts. It contributes to supporting the ability of the security agencies of countries, or even different groups, to form a global network of clients without direct involvement, in

addition to the low cost, ease of communication, and the difficulty of traditional control over electronic interactions, and such an attractive element for the use of electronic weapons, and their employment to achieve goals. political and military.

Cyber warfare is also characterized by its long-term goals, as its danger does not stop at a certain extent, and its damage has no specific scope, and its objectives are as follows: (Brian , 2015 , p 158)

• They are considered cross-border attacks. There is no time or place to stop them.

• It can reach anywhere in the world at an incredible speed.

• Its destruction is very lethal, as it may explode nuclear power stations, and it may disrupt the electricity of entire cities.

• In addition, it may reach further, which may disrupt large control systems, change missile trajectories and disrupt them, and banks may be hacked and robbed, and bank transfers are manipulated through them.

• Cyber attacks disrupt air, sea and land flights and alter their route.

6 .Defense and protection strategy from cyber wars

Cyber defense is defined as the practice of countering cyber attacks and warfare targeting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It is also known as information technology security, or electronic information security.

The term applies to a variety of contexts, from business to mobile computing, and can generally be divided into several common categories as follows: (Pathan , 2020 , p 127)

Network security:

It is the practice of securing a computer network from intrusive and opportunistic elements, whether targeted attackers or malicious software.

Application security:

Focuses on keeping software and hardware free from threats, as a compromised application can provide access to data designed to protect, and implementing a successful security concept begins in the initial design phase before the software or hardware is deployed.

Information security:

Protects the integrity and privacy of data, whether in storage or in transit

Operational security:

It includes the processes and decisions that deal with data assets and ensure their protection.

The permissions users have when accessing a network, and the actions that determine how and where data can be stored or shared all fall under this umbrella.

Disaster recovery and business continuity:

Determines how the organization responds to an electronic security incident, or any other event that causes data loss, and this involves the organization's work mechanism in restoring its data and operations, to return to the same operational capacity that it had before the incident, and business continuity is the plan that the organization relies on while trying Work without specific resources.

Education of the end user:

that is, dealing with the unpredictable factor of cybersecurity; which is people; Anyone can accidentally introduce a virus into a secure system.

Guiding users to delete suspicious email attachments, not to connect unknown USB drives, and many other important lessons is vital to the security of any organization.

In view of the various types and forms of cyber threats that users of the Internet are exposed to, everyone is seeking and primarily concerned with protecting their data and important information, their various accounts on the Internet, from tamperers, and any user can maintain the level of cyber security for all his information through several steps, represented in: (Al-Amiri , 2021 , p 48)

• Stay away from any suspicious sites or links, which the user may suspect, by checking the URL address. If it contains the HTTP protocol, this means that the site is safe, but if it does not contain it, then care must be taken in dealing with it, entering it, or entering any Personal or sensitive information.

• Beware of opening fraudulent e-mail, which often reaches the unimportant or is identified as suspicious, as it is one of the most common methods of fraud, hacking and the introduction of malicious software to devices.
• The need to follow the up-to-date updates of your devices and even the programs in them. In addition to the fact that they clean the devices from any viruses or suspicious files, they also update and make corrections to the programs in your device, especially in terms of security.
• Take care of backups, whether on the cloud or on your storage devices, in order to protect your files in a safe place separate from your device in case you want to clean your device from harmful files.
• The need to take into account the constant review of everything new in the world of cybersecurity, to know the latest developments and updates on it, to increase the security and protection of your devices.

The following are the most important methods of combating electronic espionage in cyber warfare: (Buchan , 2020 , p 100)
• Persistently not activating the geo-tracking technology within your smart devices and the platforms and application of the digital world, that is, turning on the recognition of your geographical location once when you request it, and not always and without permission.
• Do not communicate with unknown parties through social networking sites: Your communication with unknown people brings you close to security and intelligence suspicions, and espionage operations begin and study your personality and political affiliations.
• Do not activate the cookies system in computerized uses, and persevere in choosing applications that deal with ads less so that your interaction times with the digital world do not turn into ad display times and turn you into a mere economic consumption machine.
• Do not press the follow or like button for any page that has content that may be classified as dangerous or contrary to general standards. If you insist on following these pages, study all your interactions with them before you implement them.
• Use secret passwords consisting of Latin letters of several sizes and in no alphabetical order in addition to numbers, and completely move away from the known dates of your social circle and easy keywords, and link all sites

to your phone number to ensure your confidentiality and inform you about any attempt to hack your smart devices.

• Download reliable applications to protect your data, geographical location, and all your conversations and interests via social networking sites, such as the modern Nawi application, which provides complete protection for all your electronic content stored on your smart devices.

7 . International Law of Cyber Warfare:

Are there restrictions or rules governing cyberwarfare? Are computers, civilian networks, and electronic infrastructure protected against cyberattacks? A group of international legal and military experts answer "yes" to this question in a recently published Tallinn Handbook* to which the ICRC contributed as an observer. Mr. Laurent Geisel, Legal Adviser to the International Committee of the Red Cross, explains the importance of the "Tallinn Manual" as a step towards emphasizing the link between international humanitarian law during armed conflicts in all its forms and the desired goal of reducing human suffering.

The term "cyber warfare" seems to be used by many groups of people to refer to different things. The term is used here to refer to means and methods of warfare consisting of operations in cyberspace that amount to or take place in the context of an armed conflict, within the meaning of international humanitarian law. The ICRC is concerned about cyber warfare due to the vulnerability of electronic networks and the potential human cost of cyber attacks.(Harrison , 2021 , p 97)

When a country's computers or networks are attacked, hacked, or disrupted, civilians are at risk of being deprived of basic needs such as drinking water, medical care, and electricity.

If GPS systems fail to function, civilian casualties can occur, for example by disrupting the takeoffs of rescue helicopters. Dams, nuclear plants and aircraft control systems can be vulnerable to cyber attacks due to their reliance on computers.

Networks are so interconnected that it is difficult to limit the effects of a cyber attack against one part of the system without harming other parts or disrupting the entire system.

The welfare, health and even lives of hundreds of thousands of people could be affected. The ICRC reminds all parties to the conflict to take care continuously in order to spare the blood of civilians, which is one of the most important roles it plays. Wars have rules and limits that apply to resorting to cyber warfare as much as they apply to the use of guns, artillery and missiles.(Nadine , 2021 , p 114)

Those in charge of the ICRC welcomed the experts' study of the consequences of cyberwarfare and the law applicable to it. Resorting to operations in cyberspace during armed conflicts has the potential to have dire humanitarian consequences. The ICRC considers it necessary to identify ways to reduce the human cost of electronic operations, in particular reaffirming the link between international humanitarian law and this new technology when used during armed conflicts.

What exactly the experts say in the "Tallinn" guide. The means and methods of war evolve with the passage of time, and it is clear that they are no longer what they were when the Geneva Conventions were formulated in 1949, but international humanitarian law is still applicable to all activities undertaken by the parties during an armed conflict and should be respected.

However, the fact that there may be a need to develop the law to ensure that it provides adequate protection to the civilian population cannot be ruled out as cyber technology evolves or as its humanitarian impact becomes better evident. States should decide this for themselves.

While the Tallinn Handbook is a non-binding document prepared by a group of experts, they hope that it will usefully contribute to further discussion among states on these challenging topics, and that states and non-state armed groups will ensure that resort to cyber operations during armed conflicts will be conducted in accordance with their obligations. international.(Harrison , 2021 , p 101)

There is currently much debate about how international law, including international humanitarian law, should be interpreted and applied to the

activities of states and non-state actors in cyberspace. The ICRC will continue to bring its expertise in the field of international humanitarian law to address these challenges.

This does not mean that IHL applies to all cyber operations or to all what are termed “cyber attacks” in common parlance: IHL does not regulate cyber operations outside the context of an armed conflict.

Businesses and governments are as interested in cyberespionage, cybercrime, and other cybercriminal activities as they are in cyberattacks, which are governed by international humanitarian law.

The technical means used to protect electronic infrastructure from espionage or attack may be similar, but the law governing these operations is the same. Hence, a key issue is to define the circumstances under which cyber operations can be considered as occurring in the context of an armed conflict or as themselves giving rise to an armed conflict to which IHL applies.

The Tallinn Handbook provides interesting insights in this regard. It upholds, for example, the traditional dualism of international and non-international armed conflicts, and recognizes that cyber operations alone may constitute armed conflicts depending on the circumstances – particularly the devastating effects of such operations. In this regard, the guide provides a definition of a "cyber attack" under international humanitarian law as "a cyber operation, whether offensive or defensive, that is expected to cause injury or death to persons, or damage or destroy objects."

The crux of the matter, however, is in the details, i.e. what should be understood as "harm" in the electronic world. After extensive discussions, most of the experts agreed that in addition to physical damage, the cessation of work by a notable may also constitute damage. The ICRC's point of view is that if a property breaks down, it is not important how this happens, whether by kinetic means or an electronic process.

This issue is very important in practice since any electronic operation intended to disrupt a civilian network would otherwise not be covered by

the prohibition imposed by international humanitarian law on the direct targeting of civilians and civilian objects.

The ICRC contributed as an observer to the discussions of the experts who drafted the Tallinn Manual to ensure that existing international humanitarian law is reflected in the Manual as fully as possible, and to strengthen the protection afforded by this branch of law to victims of armed conflict. The ninety-five rules included in the guide reflect texts that have gained consensus among experts. The International Committee generally agrees with the wording of the rules, but there may be some exceptions. For example, the rule that reminds of the prohibition of the warring parties' retribution from a number of persons and objects that enjoy special protection does not include cultural property, contrary to the findings of the International Committee's study on international law. Human customary of the results.

Conclusion :

Cyber warfare is considered one of the most important and dangerous types of wars in the current era, especially with the development of technological means of communication, and its intrusion into all fields of life of peoples and individuals. It has become an integral part of the manifestations of the regional and international ideological conflict.

Thus, we can say that cyber war is the war of the future, and its disastrous consequences may be disastrous for humanity. The electronic competition that threatens individuals while they are safe in their homes, stems from cyberspace, which has become part of their lived reality.

This is what requires all countries of the world to take protection measures more than necessary. On the other hand, not to be complacent about any threats or dangers that we may be exposed to in this cyberspace, whose harm is not limited to individuals, but rather that it may destroy global systems politically, economically and militarily, and cause nuclear wars that we are indispensable for and the troubles that they may cause. Will cyber war have an inevitable end like others?

List of references :

Books :

-Marai Ali Al-Ramahi(2022) , Cyberwar and the New National Security Requirements, Arab Democratic Center for Strategic, Political and Economic Studies, Cairo.

- Jennie M. Williamson(2002) , Information Operations: Computer Network Attack in the 21st Century, Strategy Research Project (Pennsylvania: U.S. Army War College. Carlisle Barracks.

- Richard A. Clarke (2011) , Cyber War: The Next Threat to National Security and What to Do About It , Ecco , usa .

- Adel Abdel Sadiq(2017) , Patterns of Cyber Warfare and Its Repercussions on Global Security, Al-Ahram Foundation, Egypt.

- Bobby Akart (2015) , Cyber Warfare (Prepping For Tomorrow Book 3) , Kindle Edition, usa .

- Jason Andress (2017) , Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners , Routledge , uk .

- Brian M. Mazanec (2015) , The Evolution of Cyber War: International Norms for Emerging-Technology Weapons , Potomac books , usa .

- Al-Sakib Khan Pathan (2020) , Cybersecurity Fundamentals : A Real-World Perspective , CRC Press , usa .

- Muhammad Saeed Al-Amiri (2021) , Cybersecurity and Digital Investigations, Dar Al-Bayan, Abu Dhabi .

- Russell Buchan (2020) , Cyber Espionage and International Law , kindle edition , usa .

- Heather Harrison Dinniss (2021) , Cyber Warfare and the Laws of War , pbs , usa .

- Nadine Mudaber (2021) , Cyberwarfare and International Humanitarian Law, Al Masirah Publishing House, Amman .

Articles :

- Adel Abdel Sadiq (2011) , Future Wars... The Electronic Attack on Iran's Nuclear Program, International Policy Journal, Al-Ahram Foundation .

- Ahmed Allou(2018) , Cyberwars and Digital Violence: A New Global Reality, Journal of Studies and Research, Lebanon, Issue 402 .