Reflections on the Concept of Cyberwar and the Contributions of the International Community in the Peaceful Use of Cyberspace

Received: January 10th, 2022• Approved: September 11st, 2022
https://doi.org/10.22395/ojum.v21n46a4

Evelyn Téllez Carvajal
INFOTEC / UNAM, Mexico city, Mexico
evelyn.tellez@infotec.mx / iustellez@yahoo.fr
https://orcid.org/0000-0001-6136-6821

Jessica González Hernández
Tata Consultancy Services, Mexico city, Mexico
jessicagonzalez@politicas.unam.mx
https://orcid.org/0000-0002-0857-5285

ABSTRACT

The objective of this article is to analyze the concept of "cyber warfare" by contrasting it with the concept of warfare to identify the problems that international law faces to regulate, punish, and prevent cyberattacks committed by States against other States either by affecting their critical infrastructure or by stealing top secret information. We emphasize the contributions of some scholars and the Group Governmental Experts on Developments in the Field of Information and Telecommunications in Context of International Security regarding the States' obligations to promote the peaceful use of cyberspace and prevent cyber warfare and headline on some States' contributions such as France, and its Paris Call for Trust and Security in cyberspace.

Thus, making use of documentary analysis and the inductive-deductive method, the first results were that there is a lack of consensus on the concept of cyberwar, although its use has become popular. Furthermore, elements of *jus ad bellum* and *jus contra bellum* are neither clear nor forceful to explain cyberattacks perpetrated against States. In other words, international law on the use of force and the law on the prevention of war is diluted in the digital environment, which allows us to conclude that the law of armed conflict, as we currently know it, does not conform to the digital environment. Until now, there is no international law that can promote the peaceful use of cyberspace and States are facing their own setbacks in this regard.

Keywords: war; cybercrime; cyber peace; cyberwar; cyber armies; weapons.

Reflexiones sobre el concepto de ciberguerra y los aportes de la comunidad internacional en el uso pacífico del ciberespacio

RESUMEN

El objetivo de este artículo es analizar el concepto de "ciberguerra" contrastándolo con el concepto de guerra para identificar los problemas a los que se enfrenta el derecho internacional para regular, castigar y prevenir los ciberataques cometidos por los Estados contra otros Estados, ya sea afectando a sus infraestructuras críticas o robando información de alto secreto. Destacamos las aportaciones de algunos estudiosos y del Grupo de Expertos Gubernamentales sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional en lo que respecta a las obligaciones de los Estados de promover el uso pacífico del ciberespacio y prevenir la ciberguerra, y nos centramos en las aportaciones de algunos Estados como Francia y su: L*lamamiento de París* por la confianza y la seguridad en el ciberespacio.

Así, haciendo uso del análisis documental y del método inductivo-deductivo, los primeros resultados encontrados son que existe una falta de consenso sobre el concepto de ciberguerra, aunque su uso se ha popularizado. Además, los elementos del *ius ad bellum* y del *ius contra bellum* no son claros ni contundentes para explicar los ciberataques perpetrados contra los Estados. En otras palabras, el derecho internacional sobre el uso de la fuerza y el derecho sobre la prevención de la guerra se diluyen en el entorno digital, lo que nos permite concluir que el derecho de los conflictos armados, tal y como lo conocemos actualmente, no se ajusta al entorno digital. Hasta el momento, no existe ningún derecho internacional que pueda promover el uso pacífico del ciberespacio y los Estados se enfrentan a sus propios reveses en este sentido.

P*alabras clave*: guerra; cibercrimen; ciberpaz; ciberguerra; ciberejércitos; armas.

Reflexões sobre o conceito de ciberguerra e as contribuições da comunidade internacional em torno ao conceito do uso pacífico do ciberespaço

RESUMO

O objetivo desse artigo é analisar o conceito de "ciber-guerra" comparando-o om o conceito de guerra para identificar os problemas aos que se enfrenta o direito internacional para regular, castigar e prevenir os ciber-ataques cometidos pelos Estados contra outros Estados, já seja afetando as suas infraestruturas críticas ou roubando informação ultrassecreta. Destacamos algumas contribuições de estudiosos e do Grupo de Expertos Governamentais sobre os avances no campo da informação e as telecomunicações no contexto da seguridade internacional face as obrigações dos Estados de promover o uso pacífico do ciberespaço e prevenir a ciber-guerra, nos concentramos nas contribuições de alguns Estados como França e seu apelo de Paris pela confiança e a segurança no ciberespaço.

Assim, fazendo uso da análise documental e do método indutivo-dedutivo, os primeiros resultados encontrados é que existe uma falta de consenso sobre o conceito de ciberguerra, embora o seu uso está popularizado. Além disso, os elementos *del ius ad bellum* e do *ius contra bellum* não são claros nem contundentes para explicar os ciberataques perpetrados contra os Estados. Em outras palavras, o direito internacional sobre o uso da força e o direito sobre a prevenção da guerra diluem-se no entorno digital, o que nos permite concluir que o direito dos conflitos armados, como o conhecemos atualmente, não se encaixa ao entorno digital. Até o momento, não existe nenhum direito internacional que possa promover o uso pacífico do ciberespaço e os Estados se enfrentam aos seus próprios reveses neste sentido.

P*alavras-chave*: guerra; cibercrime; ciberpaz; ciberguerra; ciberexércitos; armas.

Introduction

Societies around the world have been impacted, both positively and negatively, with the incorporation of scientific and technological advances. The industrial revolutions have been a watershed in the changes of the individuals' daily life. The First Industrial Revolution in England caused, without a doubt, the abandonment of fields as people moved to cities to work in factories. With the advent of the telegraph and later the telephone, there was a new age in communications, and the Second Industrial Revolution appeared due to more agile the way to communicate.

It is unclear when did the Third Industrial Revolution begin, but artificial satellites, fiber optics, computers, touristic space trips and, of course, the Internet, are some of the technologies that have male relevant changes in the societies.

Today we are in the era of satellite television, smartphones, wireless Internet, embedded systems, and the way all these technological advances have changed how work is carried out, institutions are organized, people communicate and consume commerce is implemented, relations are carried out but above all this, we must highlight the new threats and risks that information and communication technologies (ICTs) represent for all the States due to the increase of malicious and misuse of ICT's by States and non-State actors.

Some of the activities carried out on the Internet can have diverse effects within cyberspace as well as in the analogical world. Such is the case that concerns this study, which is "war" in cyberspace or, as it has been called, cyberwar, a concept coined to explain "warlike" activities carried out within cyberspace. However, it is necessary to analyze what are those specific activities in cyberspace that can be considered as cyber warfare.

Derived from the above, as stating point we present the definition of the concept of cyberwar, highlighting the "warlike" actions in a virtual scenario and the complexity to arrive at consensus on this regard.

Secondly, we explain why it is difficult to identify that States are facing a cyberwar, especially because that officially does not exist. Today's virtual scenario allows States to deny their responsibility for the actions carried out against other States due to the nature of cyberattacks.

In the third section we present considerations that the international community and some States, in particular France, have made in order to alleviate these adverse situations in the digital environment. It is important to note the different capabilities and commitments that States have depending on their resources, their technological capabilities, and their particular interests in this regard.

Thus, the general objective of this contribution is to provide the reader with an analysis of the concept of cyber warfare, showing the lack of uniformity in its conception, as well as emphasize that the legal concepts used in armed conflicts do not necessarily adapt to the digital context. For this reason, it is necessary to become aware of the international proposals for the peaceful use of cyberspace, understanding the obligations and responsibilities of the members of the international community.

In 1998, the Russian Federation set the topic on the role of technology in the context of international security on the UN agenda, and later, in 1999, the Resolution 53/70 on developments in the field of information and telecommunications in the context of international security was adopted. Since then, there have been seven working Groups of Governmental Experts (GGES):

Table 1. Groups of Governmental Experts

Period	*Resolution*	*Members*
2004-2005	A/RES/58/32	15 members No consensus
2009-2010	A/RES/60/45	15 members
2012-2013	A/RES/66/24	15 members
2014-2015	A/RES/68/243	20 members
2016-2017	A/RES/70/237	25 members No consensus
2019-2020	A/RES/73/27	All member States
2019-2021	A/RES/73/266	25 members

Source: Own elaboration with information taken from United Nations Office for Disarmament Affairs.

Some of the GGEs' recommendations through the years have been: to reduce risk and protect critical infrastructure by norms for the State use of ICTs; to apply international law to cybersphere, and to State sovereignty. The settlement of disputes by peaceful means is one of the principles of international law that States must observe in their use of ICTs (UNODA, 2019).

In this way, making use of documentary research, some experts' opinions on cyber warfare are rescued to identify and delimit the use of the concept. We also analyze the current regulations that govern armed conflicts that apply to the cybersphere and, finally, some of the contributions of the international community are identified through high-level meetings and official documents that account for the concern and proposals from the national and international contexts to guarantee the peaceful use of cyberspace.

It is necessary to point out that in this analysis we do not refer to the attacks in cyberspace carried out by non-state entities since they are not strictly considered as armed conflict between States, but rather classified as cyber terrorism, a topic that is not part of our analysis.

1. The Concept of War and Cyberwar

The word war has a Germanic origin "werra" (disorder or fight) and it is understood as a confrontation between two or more powers, nations, sides, or things (Real Academia Española, n. d.). There is also a Latin word "bellicus" that refers to the use of military force in a confrontation. "War constitutes [...] an act of force that is carried out to force the adversary to obey our will." (Clausewitz, 2016, section 2. Definition, our translation).

Although clashes between groups must have existed since prehistoric times, the first record of a war is the stelae in the city of Thebes with hieroglyphs, it traces back to 1457 B.C. and it refers to the war between Egypt and the city of Megiddo, today Palestine. (De Souza, 2008, p. 31, our translation).

Throughout history there have been some authors who have referred to the concept of war such as St. Tomas Aquinas and his concept of just war, Maquiavelo and his short and decisive war, Kant conceiving war as a state of the nature of man or Hobbes with his war of all against all (*bellum ómnium contra omnes*). Despite the references there is not a consensus on a definition of war.

War must not be understood solely as the absence of peace, nor peace as the absence of war or disarmament. According to Cristina Rosas (2016) peace "is built and achieved with broad, multidimensional agendas that demand efforts not only in favor of disarmament, but also in favor of social development", (para. 1) (our translation). We understand that to achieve peace, war must be avoided that is why a definition is needed.

In the attempt to define the concept of war some elements have been considered such as the kind of participants, the intensity of the attacks, or the kind of weapons that are used in the confrontations. In the past it was considered that only the States were able to participate in these conflicts as subjects of international law, leaving aside the so-called "civil wars". It has also been unsuccessful to try to name the conflict by its intensity, (such as the use of bombers), or by its motivation, (such as economic warfare), or by the type of weapons that are used, (such as in bacteriological warfare), or on the quality of the subjects who participate (as combatants, armies, or unmanned devices) in it.

In the past, the international community considered that before the confrontations between two States started, a declaration of war was needed. War declarations were

founded in the so-called *casus belli*, (causes for the declaration of war). Some of these causes were the breach of a treaty, the aggression to state sovereignty through occupation, hostile acts, or threats to internal order, to name a few.

Reinel Sánchez (2004) considers that the

> [v]arious definitions of war coincide with the following points: I) War as such is an armed struggle and, therefore, violent; II) occurs between two nations or two parties of the same nation; iii) there is a diversity of wars depending on the intensity of the fighting and the origin of the combatants; iv) the concept of war has other meanings […] such as conflict… (p. 10, our translation)

Rojas Amandi (2010) sustains that,

> there are difficulties in defining the concept of war, however it is usually estimated that war is the existence of a violent situation contrary to PIL [Public International Law] that implies the breakdown of peaceful relations [and adds that] [t]he modern norms of PIL do not use the concept of war and the concept of 'armed conflicts' is employed instead because it has a broader meaning and it covers all types of conflicts in which force is used. (p. 145, our translation)

Thus, war declarations of yesteryear were a manifestation of the intention to break diplomatic relations between States and were the means to initiate hostilities but today they are not used anymore, since States committed to the 1945 Charter of the United Nations that prohibits the use of force in its article 2.4 and empowers the Security Council to endorse, through its resolutions, any threat of use of force or lawful use of force between members of the United Nations.

The international community has no unique concept of war nor a consensus about the concept of cyber warfare. In the context of cyber space in Spanish, the concepts: digital warfare or virtual armed conflict are less used, and the concept of cyber war is much more widespread. Carrillo y Vargas (2016) define it as the "use of capacities based on the network of a State, to interrupt, deny, degrade, manipulate or destroy information residing in computers and computer networks, or the computers themselves and the networks of another State" (p. 12, our translation).

Vélez Martínez (2019), from the Engineering Institute of the National Autonomous University of Mexico, points out the differences between conventional warfare and cyber warfare as:

> the environment, the strategies, and the weapons [which] are totally different but with a destructive potential similar to physical weapons. In cyber warfare the borders are non-existent and virtual attackers are invisible. The objective of this cyber warfare is to dismantle or disable the enemy's computer infrastructure with all the implications such as: blocking access, causing delays in the network, causing a denial of service, massively launching malware (spyware, viruses, worms, Trojans), creating botnets, stealing information, among many others. (para. 2, our translation)

Gema Sánchez, (2010) explains that:

> [c]yberwar can be understood as an aggression promoted by a State and aimed to damage seriously the capacities of another State in order to impose its own objectives or, simply, to steal information, cut or destroy the communication systems of the other, alter its databases, that is, what we have usually understood as war, but with the difference that the means used would not be physical violence but a computer attack. (p. 64, our translation)

In this way, taking into consideration the elements of the different definitions of the concept of cyber warfare above mentioned, we can say that:

- It is about one or several actions deployed against a State's computer or computer network with the intention to interrupt, deny, degrade, manipulate or destroy information stored in it;
- Its motivation is political;
- It is an aggression carried out by a State against another;
- The objective of the aggression is to impose one's own objective or to steal information;
- Its intention is to seriously harm the capabilities of another State;
- The activity is carried out through the network of a State;
- The violence is not physical but it is developed through a computer attack against communication systems and databases.

Despite having no clear definition, cyber war is understood as any action deployed by a State within cyberspace with political motivation and the purpose to weaken the computer systems of another State or group of States causing serious damage in the other or others' capabilities and succeeding in it.

1.1. Actions and "Weapons" in Cyber Warfare

There is no consensus in the international scenario about what can be considered as an action of cyber warfare, as Libicki (2009) states:

> What constitutes an act of war may be defined one of three ways: universally, multilaterally, and unilaterally. A universal definition is one that every state accepts. The closest analog to "every state" is when the United Nations says that something is an act of war. The next-closest analog is if enough nations have signed a treaty that says as much. As far as cyberwar goes, no such United Nations dictum exists, and no treaty says as much. One might argue that a cyberattack is like something else that is clearly an act of war, but unless there is a global consensus that such an analogy is valid, cyberattack cannot be defined as an act of war. (p. 179)

To understand the actions and weapons that are used in the digital context, we must point out that military actions are "... all those that are related to the military field, such as the strategy in a battle, the movements of troops or any other circumstance of the tactics of an army" (Navarro, 2016, para. 1, our translation). In cyber war it is difficult to differentiate between what is a cyberattack and what is a true military action in cyberspace.

Scheiner (2007) points out that the biggest problem with cyber warfare is precisely its definition, since it is usually described by using elements that, more than cyber warfare, describe actions of cyberterrorism, cybercrime, cybervandalism and cyber hooliganism, and even espionage. He also comments that the tactics used by armies, terrorists, and criminals in the virtual setting are practically the same.

Today in "warlike" actions in cyberspace, the use of weapons such as bombs and conventional weapons (understood as weapons that are not intended to cause massive damage), such as pistols, are changed to the use of tactics to denial deny services, exploits that can violate military intelligence and penetrate the systems, or the introduction of viruses, worms, Trojans that attackers carry out against computer systems.

Harris, Acton, and Herbert (2016) identify some of the characteristics of a cyber weapon as follows:

- "[...] the duration and spatial scale of the cyber weapon's impact can span many orders of magnitude. But any given cyber weapon almost certainly is not to span such range.
- [...] can be used only once because a penetration that takes advantage of a system or network vulnerability usually reveals the vulnerability [...].
- The successful use (launch) of a cyber weapon generally depends heavily on accurate, detailed, and timely information about the target (and what is connected to it). Such information may be gathered using a variety of methods, including the use of other cyber weapons. In the absence of such information, the use of any given cyber weapon may have no effect whatsoever.
- The effects of using a cyber weapon remain unknown until the payload executes (or until all the payloads are available for analysis).
- The expertise and infrastructure needed to create certain kinds of cyber weapons extend beyond the usual purview of computer scientists. Cyber weapons that are intended to be used against cyber-physical systems —systems or devices that are controlled by computers but have tangible effects in the physical world— also require expertise specific to those systems or devices and also, under some circumstances, test facilities that are a high-fidelity replicas of the targets to be attacked. (para. 11-20)

Schneier (2007) explains that a major difference between the concept of war and cyber warfare is that the attacks in the latter do not seek to destroy a combatant army

or enemy infrastructure. On the contrary, it is intended to infiltrate computers to gain control of networks, access valuable information, or spy, as this is more beneficial for the attacker than destroying a computer.

Some best-known cases that have been defined as cyber warfare include Stuxnet, an attack against Iran's nuclear plant in 2010, and the malware Flame in 2012 against Middle Eastern countries such as Israel, Iran, Saudi Arabia, and Egypt, among others.

Stuxnet was a case in which a program was infiltrated into the systems of a nuclear plant in Iran. The exploit was introduced into Iran's system through an infected pen drive. That was the access door for the virus designed to reach the Programmable Logic Controller (PLC) which operated the uranium centrifuges. The virus used the networked computers and even the printers connected to the system, until it took control of the PLC and began to damage the centrifuges while it was imperceptible to people because the virus had the ability to erase the system failures. The virus was capable of modifying the information of the attacked centrifuges. That was the reason why operators did not notice the failures of the centrifuges' programs because they obtained correct operation records. The attack was aimed to destroy the centrifuges and we can say that part of its goal was achieved. It is not known for sure who the author of this virus was, but it is said that it was developed in American and Israeli labs thetheir intent to damage Iran's nuclear program. (BBC , 2015).

The case of the malware called Flame is a mixture between the so-called Trojans and computer worms. This malware mainly targeted Iran, Israel, Palestine, and Syria. Kaspersky Internet security experts consider that it was not a virus created by common cybercriminals, but rather that a State was behind its development since its purpose was the theft of strategic information. It was software designed to basically spy. Within its functions, it can perform screen captures, record conversations, search for mobile devices and steal information such as contact lists, recover passwords that are transmitted over the network, and control the computer on which it is installed. (Reventos, 2012) This is one of the most sophisticated computer attacks and demonstrated that countries with less progress in cybersecurity are at a great disadvantage. As in the Stuxnet case, it is considered that this software was designed by state agents, but it is not certain who the authors were.

Until today, the authors of the cyberattacks directed against States have not been identified. It is unclear which States are being affected by these kinds of attacks and it is very likely that there are many other cases being carried out now. But it is necessary to clarify if these cyberattacks should be considered as part of a cyber warfare or they should only be considered as common cyberattacks perpetrated by any hacker or group of hackers.

Thus, it must be defined if the "attacks" that are being deployed in cyberspace against States could be considered as "weapons" or "strategies" like those that are used in a traditional armed conflict. The following is just a list of the most common cyberattacks, it is not limiting, since we do not delve into the specifications of each type of attack as it is not an objective of this work.

Denial of Service (DoS)

According to the Seattle-based company F5 Networks (2021) founded in 1996, specializing in technology, a denial of service, or DoS, is known as

> an attack that makes a computing resource inaccessible to previously authorized users by flooding a network or server with an immense quantity of requests and data. It can also refer to the fact that a resource, such as an email or a website, does not work as it should", that is, this type of attack denied users who have permission to access certain resources on the network, therefore, connectivity is limited and is used by hackers to bring down servers, which globally could be circumstantial for critical information.

Access Blocking

There are other types of attacks related to authentication, such as those that violate databases or confidential information, specifically towards a File Transfer Protocol (FTP) which is a program that allows, as its name indicates, to transfer files over the Internet through the TCP/IP network, that is the way computers communicate over the Internet.

> An access attack allows a person to gain unauthorized access to information that he or she has no right to see. Access attacks can be classified into four types. One of the most common types of access attacks is the password attack. Password attacks can be implemented with packet sniffer programs to obtain user accounts and passwords that are transmitted in clear text. Password attacks can also refer to repeated attempts to log on to a shared resource, such as a server or router, to identify a user account, password, or both. These repeated attempts are called "dictionary attacks" or "brute force attacks". (Instituto Roque, n.d., our translation)

Espionage

Espionage has been considered a very important strategy among States, since it has functioned as an instrument to gather information that can be used to carry out plans against those affected, even during a war.

New threats for the States in the 21st century are different from those of other eras, among them, cyber threats are highlighted. Espionage is an activity that has been highly relevant throughout history, and today it is conditioned to the current context. Cyberespionage is described by Joaquín Ruíz (2016) as the strategy to "obtaining information, of a mainly strategic type, which today is stored electronically, albeit under great security measures, on the servers of the strategic defense institutions of the vast majority of countries" (p. 1, our translation).

It should be noted that the main objective of this type of activity, as it is in traditional espionage, is to obtain a certain political, economic, commercial, and military advantage, which is classified as a strategic tool during cyber warfare.

Sabotage

Cyberespionage has certain characteristics that differentiate it from cyber sabotage. In both cases, the main objective is to obtain information so that the attacker can act to favor himself, although both are considered crimes. Different from cyberespionage, cyber sabotage seeks to cause damage directly in the software and/or hardware of a specific system. It is "the act of deleting, removing or modifying computer functions or data without authorization with the intention of hindering the normal operation of the system" (Delgado Granados, 2021, p. 10, our translation) and it is carried out with the support of malware as a tool to fulfill the established purpose.

The idea of carrying out sabotage is to be able to hinder the system's correct operation and in this way interfere with the critical functions of the infrastructure, causing damage not only in the system itself but also affecting its users. In damaging the State's critical infrastructure certain information can be compromised and thereby it could be possible to infringe on their national security. Since cyber sabotage performs an attack on such infrastructure, there will be a disruption with detrimental damage.

Mass Malware (Spyware, Viruses, Worms, Trojans)

The so-called malware, according to Veracruz University (2016) is "a type of software that aims to infiltrate a computer or computer system without the user's consent" (par. 4, our translation) and that can be divided into several types.

In the case of spyware, as defined by Kaspersky (n. d.) "as a software designed to collect data from a computer or other device and forward it to a third party without the knowledge or consent of the user. This often includes the collection of sensitive data", which is used to obtain information from users and share it with cybercriminals to profit from said information.

Computer viruses work as a kind of biological virus, that is, they infect the devices through a computer program that is introduced through the download of an attached file that can be executable (Univesidad Veracruzana, 2016).

The computer worm is different from the virus, in that it "has the ability to replicate itself, it's only objective is to increase its population and transfer to other computers through the Internet or storage devices" (Universidad Veracruzana, 2016, para. 18, our translation), in other words, it replicates itself to infect other computers without the need of a previous download.

Trojans are very similar to computer viruses in terms of their implementation, however, what they do is to "provide a back door for other malicious programs or

cybercriminals, so that they can enter the system and steal information without the knowledge or consent of the user" (Universidad Veracruzana, 2016, para. 25, our translation).

1.2 The Cyber Armies, Who Are the Combatants in the Cyber War?

In a military confrontation there are traditionally two parties, on the one hand, the State or States that initiates the hostilities and on the other the State or States that fight or try to dissuade such violent acts. In the case of cyber warfare, it is difficult to identify with certainty who is the author of the actions carried out in cyberspace against a State or group of States.

Determining who the combatants are in cyberspace is also complicated since they cannot be defined as the law of international armed conflicts does. Rojas Amandi (2010) points out that

> [t]he combatant status is acquired by the members of the combat forces of the parties in the conflict. Combat forces are understood as official armed military units ostensibly identified as such. These include groups of volunteers, health forces, and military intelligence. In contrast, mercenaries do not have the status of combatants. Nor do spies enjoy the status of combatants and although their activity is not contrary to the international law, they can be sanctioned by the States in which they carry out their activities. (pp. 148-149, our translation)

"Only combatants who have the legally recognized status of combatants are authorized to carry out violent behaviors that cause harm and, if they are detained, to be treated as prisoners of war". (Rojas, 2010, pp.148-149, our translation).

Therefore, identifying the combatants in a confrontation in cyberspace seems quite complex, as Scheiner (2007) points out, it is difficult to differentiate when we are facing an attack in "cyber warfare" or when it is an attack performed by a terrorist group, for example.

In this way and given the circumstances in which a State can be in the presence of cyber warfare, cybersecurity is an issue of the utmost importance. Thus, States need to develop their capabilities to deal with cyber threats and take advantage of technological advances and create cyber military commands or cyber armies, which Corredera (2012) defines as that military capacity that is possessed for the defense of cyberspace (p. 240). Therefore, the role of cyber armies is essential to have adequate cyber security that includes cyber defense.

An army is "[a] set of air or land forces of a nation. Large units are made up of various army corps, as well as homogeneous units and auxiliary services" (Royal Spanish Academy, n.d., our translation). Therefore, the cyber army is derived from the army, it is focused on cybersecurity and cyber defense activities within cyberspace and the environment that entails it.

The work of cyber warfare agents is relevant since, as in land, sea, or air warfare, there must be forces trained to affect particular combat tactics. In the case of cyber armies, they have tactics, techniques and procedures designed to create, avoid or counter cyberattacks.

In order to protect the infrastructure of the States from cyberattacks that can cause serious damage to the economic, political, and social structures, cyber armies are the protagonists of cyber defense within the cyberspace. However, and despite the fact that the defense of cyberspace is the main task of cyber armies, they cannot always defend their own cyber infrastructure, since not all States have the same capabilities to defend themselves or counteract a cyber threat or cyberattack. In addition, it should also be considered that there are cyber armies that, rather than having defense strategies, they are dedicated to attack, such is the case of the Iranian cyber army (Acosta *et al*., 2009, p. 137).

American and Chinese cyber armies are considered the best in scope; followed by those of Spain and North Korea, the latter with a strategy focused on the offensive to orchestrate cyberattacks against the United States and South Korea, which also has its own cyber army (Mateos, 2019).

There are few other States, in addition to those above mentioned, that have cyber armies, such as Argentina and Mexico, however, it is important to point out that there are countries that do not even consider implementing a cyber army or cyber defense strategies because they have limited technological capabilities, or due to the budgetary amount required to prepare and support this type of resources.

2. Cyberwar Regulation

The concepts "*jus ad bellum* (law on the use of force) and *jus contra bellum* (law on the prevention of war) seek to limit the use of force between States. Under the Charter of the United Nations, States shall refrain from the threat or use of force against the territorial integrity or political independence of any State (art. 2 (4)). This principle may be exempted in cases of self-defense and after a decision adopted by the Security Council of the United Nations under Chapter VII of the Charter of the United Nations. (International Committee of the Red Cross, 2010). Moreover, these principles contained in the Charter of the United Nations do not contemplate the cyber context and therefore it is necessary to question whether the law surrounding armed conflicts is useful for cyber warfare.

Currently, there is no international regulatory framework regarding cyber warfare. An adequate regulation in this matter is urgent since the national and regional actions and proposals for regulatory frameworks that governments have carried out unilaterally are not enough.

As antecedents to the regulation of cyber warfare, it can be mentioned that the Declaration of Saint Petersburg of 1868, prohibits the use of certain weapons during war and it emphasizes "That the only legitimate purpose that the States must propose during the war is the weakening of the enemy's military forces" (International Committee of the Red Cross, n. d.). The same idea is raised in the proposals for the regulation of cyberwar since cybersecurity sought to avoid the use of cyber defense.

Another antecedent is the Geneva Convention of 1949, which seeks to establish certain limitations during war so human rights could be fully granted and protected during the arm conflicts. This is relevant for International Humanitarian Law, which was previously known as the Law of War, and that today serves as the Law that governs war and that is taken, in part, into consideration to guide the cyber warfare issues.

The Wassernaar Arrangement, 1996, can also be considered as an antecedent to prevent cyber warfare, as it "has been established in order to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations". (Wassenaar Arrangement, 2019, p. 4) The aim is also to prevent the acquisition of these items by terrorists.

Even though it is not a binding instrument (Horzella, 2021) it is a guide for its 42 Participating States (Argentina, Australia, Austria, Belgium, /Bulgaria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Russian Federation, Slovakia, Spain, Sweden, Switzerland, Türkiye, Ukraine, United Kingdom, United States, Croatia, Estonia, India, Latvia, Lithuania, Malta, Mexico, Slovenia, South Africa) to implement arms export controls including cyber weapons such as surveillance technologies or malware counter-proliferation (Kimball, 2022).

Unfortunately, the Wassernaar Arrangement fails in its tendency to regulate technology first by its own nature that does not respect borders or national controls and secondly because of the lack of political consensus among the States (Hernández, 2018).

These Conventions, and Agreement, have influenced the Convention on Cybercrime by the Council of Europe, better known as the Budapest Convention. This Convention focuses not only on eradicating the dangers that may exist towards computer systems, networks, and data, but also it proposes international cooperation to deal with threats in a digital environment in general. However, the Convention is not directly applicable to cyber warfare, since the specific issue it addresses is cybercrime, but it is useful in the analysis of cyber warfare, since, as stated above, it is difficult to differentiate the acts that constitute a cyberwar from those of cybercrimes.

The document par excellence on the subject of cyber warfare is the 2013 Tallinn Manual on the International Law, applicable to cyber warfare, from the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE). This document is a compilation of research, studies, and opinions of a group of experts reflected in a proposed regulation.

However, it should be noted that it is not a binding document, but it indicates the applicability of international law to cyber conflicts, and, in particular, to cyber warfare. It proposes 95 rules to govern the cybernetic conflicts. And it emphasizes that this document was based on the applicability of different treaties and their proposals, including the previously mentioned Budapest Convention.

It is clear that the applicability of that legislation in terms of armed conflicts will not depend on the qualification of the situation under the principle of *ius ad bellum* (law on the use of force), but rather that there must be an equitable application with the law of conflict. (Schmitt, 2013). It means, that the idea proposed by the *ius ad bellum* of waging a just war through legitimate reasons of a State to be able to get involved in any war, vanishes in the digital sphere because it must be subject to the law of armed conflicts.

The Tallinn Manual, as previously mentioned, governs cyber warfare or armed conflicts within cyberspace even though it is not a binding document. However, the International Group of Experts carried out an analysis concluding in the creation of the Tallinn Manual 2.0, which is a variation of the first version presented in 2013 with new annexes.

Manual 2.0, presented in 2017, has 200 rules, which are divided into four sections. The first three refer to International Law and cyberspace, as well as the way in which it is applicable to cyber operations, with the inclusion of certain articles of the Manual 1.0. The fourth part is annexed regarding Manual 1.0.

This variable of the Manual sought to broaden the focus beyond armed conflicts within cyberspace, that is, all cyber interference that exists within it, focusing on cyber operations used in cybersecurity and cyberdefense strategies, that could trigger a cyber warfare, that also encompasses civil, state, and private participation, such as the activities carried on by private companies. Therefore, not only State actors threaten the peaceful use of cyberspace.

This is how the Group of Experts takes into account the case of the Stuxnet virus, previously mentioned in this article. To analyze the case again, and with the new foundations exhibited in the second version of the Manual, those actions must to be considered as a direct armed attack since, in the words of Jacobo de Salas Claver (2019) and based on what is stated in the Manual, "the Stuxnet attack has reached the level of use of force and, for some of them, it has even reached the level of armed attack" (p. 150, our translation).

Due to its amorphous nature, cyberspace provides a context in constant transformation. In 2021 the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defense Centre of Excellence (CCDCOE) began the works on the Tallinn Manual 3.0 together with the International Group of Experts, which aims to address new issues emerging from the international cyber context without changing the non-binding nature of Tallin Manual 2013, but (like the previous ones), be a starting point for binding regulations within international society to maintain cyber peace.

3. International Community and its Proposals to the Pacific use of Cyberspace

Notwithstanding, there is no consensus about the concept of cyber warfare, States faced numerous cyberattacks perpetrated by hackers presumably hired by other States. Examples of this kind of attacks are for instance the theft launched presumably by Chinese military hackers against the Pentagon in the United States; or the already explained Stuxnet attack against Natanz, Iran's nuclear plant, that is suggested as carried out by a coalition that included countries as US, Germany, France, UK, and Israel; or the one of the ransomware called WannaCry that attacked the social security services in England on May 12, 2017, attributed to north Korean hackers.

The ransomware WannaCry, in particular, affected simultaneously computers as well as mobile phones in 16 hospitals and health care centers all around London, Nottingham, and Cumbria causing serious affectations, not only to the health institutions but also to individuals, as those who were being transferred in an emergency without knowing that the ambulances transfers were modified by the ransomware, putting their lives at risk.

These kinds of cyberattacks are every time more effective and sophisticated and could be used as a strategy to affect national systems to force the States to answer the hostilities through cyber warfare because an attack against the States' critical infrastructure can provoke instability and uncertainty in its political, social, and economic fields and today States face these threats with their own capacities. (Álvarez, 2019).

3.1 Cyber Peace

If there is a concept of cyber warfare there must be a concept of cyber peace in the digital era. Hamadoun Touré (2011) refers to the concept of cyber peace in the modern context based on the International Union of Telecommunications:

> [C]yber peace, understood much broader than by the SMWIPM, as meant to be an overriding principle in establishing a "universal order of cyberspace". If the use of the term has more to do with politics and with political emphasis, with orienting the mind towards the right choices, then it also follows that it must remain somewhat open-ended. The definition cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.

> Yet, a basic definition is necessary. The starting point for any such attempted definition must be the general concept of peace as a wholesome state of tranquility, the absence of disorder or disturbance and violence, – the absence not only of "direct" violence or use of force but also of indirect constraints. Peace implies the prevalence of legal and general moral principles, possibilities, and procedures for the settlement of conflicts, durability, and stability. (p. 78, our translation)

Based on the concept of peace, cyber peace intends to keep order within cyberspace avoiding conflicts or violent acts that could represent a destabilization.

3.2 Paris Call for Trust and Security in Cyberspace as well as Individual Efforts

As mentioned in the introduction, some States such as France have stood out to promote security in cyberspace. On November 12th, 2018, French president Emmanuel Macron presented a cybersecurity proposal. It was a call to join efforts from governments, enterprises, civil organizations, and professional associations around the world to make cyberspace safer, avoiding disinformation and addressing new threats for critical infrastructure as well as for citizens.

Important enterprises such as Microsoft, Kaspersky, Siemens, Google, Facebook, and Huawei attended the call.

The Paris Call highlights the need for States' responsible behavior in order to get a safer cyberspace and to ensure that the monopoly of legitimate violence is still in the States. The Call lists 9 principles that are:

1. Protect individuals and infrastructure
2. Protect the Internet
3. Defend electoral processes
4. Protect intellectual property
5. Avoid malware proliferation and actions that intend to cause damage
6. Assure the digital information life cycle to strengthen secure digital processes, products, and services as well as their life cycle and their chain supply
7. Cyber hygiene, understood as efforts to support and to strengthen a prevention culture
8. Do not return to private hacking
9. Promotion of international law

The Paris Call also highlights the responsibilities of private actors in a safe cyberspace. In this way, governmental entities, as well as private actors, public, social and

private organizations, and professional associations must prevent any security threat in cyberspace as well as quit all activities that can harm it.

On December 5th, 2018, the General Assembly by its Resolution 73/27 called D*evelopments in the field of information and telecommunications in the context of international security* points out the background of the international community work in this regard:

1. 1981 Resolution 36/103 Declaration of the Inadmissibility of Intervention in the Internal Affairs of the States

2. 1988 Resolution 43/78 Review of the implementation of the recommendations and decisions adopted by the General Assembly at its 10th special session about disarmament, non-proliferation of nuclear weapons and the prevention of Nuclear War.

3. Diverse Resolutions on Developments in the field of information and telecommunications in the context of international Security.

The above-mentioned 73/27 Resolution highlights the progress that has been made for the peaceful use of information and communication technologies (ICT) in favor of the common good of humankind, and sustainable development around the world but it is also important to recognize that ICTs could be used in negative ways and with illegitimate proposes. The international community in this Resolution is "Expressing concern that a number of States are developing ICT capabilities for military purposes and that the use of ICTs in future conflicts between States is becoming more likely", (p. 2). In the same Resolution, the General Assembly urged that "States should not conduct or knowingly support ICT activity contrary to its obligations under the international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public" (p. 4).

On Resolution 74/120, Developments in the field of information and telecommunications in the context of international security, 2019, Report of the Secretary-General Egypt's reply stood out that:

> In light of the severity of emerging cyberthreats, Egypt highly values and supports the recommendation in resolution 73/27 that establishes an open-ended working group, acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States with a view to making the United Nations negotiation process on security in the use of information and communication technologies more democratic, inclusive and transparent. Moreover, Egypt looks forward to joining and supporting the efforts of the open ended working group to develop ways for the implementation of these rules, norms and confidence-building measures. (p. 15. Bold was added)

On the same Resolution 74/120, France laid out specific actions with respect to cyber defense. Its Defense Ministry explains that since 2019 France has a "defensive information warfare policy and, at the same time, the Chief of Staff of the armed forces

made a public presentation of the offensive information warfare doctrine of military operations". (p. 20) And "[i]n order to strengthen the fight against the proliferation of malicious techniques and tools, France has supported the inclusion of hacking software on the list of dual-use items of the Wassenaar Arrangement on the control of exports of classical weapons and dual-use foods and technologies. France considers that the regulatory effort should be continued in this regard, including certain cybernetic tools, depending on the severity of their effects, on the list of war materials". (p. 23)

Finally, France considers that cyberwar operations must follow 3 principles:

1. Distinction between civil goods and military targets.

2. The principle of humanity in the understanding that any hostility of cyber combatant or armed group that commits cyberattacks can be attacked either with conventional or cyber means and;

3. The principle of proportionality which must prevent direct effects of the weapons (damage to the system or interruption of service, for example, or indirect consequences for non-combatants, and any weapon that cannot be controlled is prohibited. (pp. 25- 26).

The case of Egypt and France stand out because their cybersecurity strategies are based on creating a regional legal regulation in the hope to make it international through an action program. In the A/77/92 (2022) Report of the Secretary - General, France and Egypt's proposal has been supported for states such as Australia (p. 4), Denmark (pp. 12 - 13) and the European Union (p. 34).

As the objective of this contribution is not to delve into individual proposals of the States, but rather reflect on the concept of cyber warfare and the contributions of the international community in the peaceful use of cyberspace, these examples serve to headlight the need of the international community to advance in an effective action program for cyberpeace.

Conclusions

Jus ad bellum and *jus contra bellum* are not fully adaptable to conflicts within cyberspace. Some experts consider cyberspace to be the fifth domain after land, sea, air, and space where ITC's can be used to deploy military actions. The parameters that regulate armed conflicts seem to be useless when cyberattacks take place against States' critical infrastructures. So far there is not a definition of cyberwar, and it is difficult to identify when a cyberattack is perpetrated by States or when it is caused by terrorists for example.

International Law of the Armed Conflicts emerged to order and humanize the hostilities caused by the warfare but todays cyberattacks follow a different objective as

Robles Carillo (2019, p. 3), points out. The cyberattacks are deployed to affect the States critical infrastructure, to steal information, instead of neutralizing the counterpart forces.

There is not any international cyber warfare regulation, but the international community considers some basic principles in order to protect individuals from cyberattacks. International society has worked together to strengthen cybersecurity within the Tallinn Manual and different General Assembly Resolutions as the ones mentioned above.

It was demonstrated that international law of armed conflicts intends to regulate conflicts among States but it is not enough to regulate cyberattacks. There is no mandatory instrument that regulates cyberwar but the international community is concerned about the topic and it is working to develop resolutions and promoting the work of the experts in order to guarantee the correct use of the ITC within cyberspace and avoid cyberwar. However, there are some States such as France and Egypt that propose to advance in an action-based program supported by rules, norms, and confidence-building measures.

References

Acosta, O. P., Pérez Rodríguez, J. A., Arnáiz de la Torre, D. & Taboso Ballesteros, P. (2009). S*eguridad Nacional y ciberdefensa*. Fundación Rogelio Segovia para el Desarrollo de las Telecomunicaciones.

Álvarez Valenzuela, D. (2019). La paz y la seguridad internacional en el ciberespacio. R*evista chilena de derecho y tecnología*, *8*(2), 1-3. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842019000200001

BBC News Mundo. (2015, October 11st). E*l virus que tomó control de mil máquinas y les ordenó autodestruirse*. BBC News. https://www.bbc.com/mundo/noticias/2015/10/151007_iwonder_finde_tecnologia_virus_stuxnet_

Carrillo, L. & Vargas, P. (2016). C*iberguerra: descripción de estrategias políticas internacionales y algunos planteamientos jurídicos para afrontarla* [Undergraduate Thesis, Universidad Militar Nueva Granada]. Institutional Repository. https://repository.unimilitar.edu.co/handle/10654/16043?show=full

Casar Corredera, J. R. (2012). E*l ciberespacio. Nuevo escenario de confrontación*. Ministerio de Defensa; Instituto Español de Estudios Estratégicos. https://dialnet.unirioja.es/servlet/libro?codigo=547632

Clausewitz, K. (2021). D*e la guerra*. Ediciones Obelisco.

Comité Internacional de la Cruz Roja. (1868, December 11th). D*eclaración de San Petersburgo de* 1868 *con el objeto de prohibir el uso de determinados proyectiles en tiempo de guerra*. https://www.icrc.org/es/doc/resources/documents/treaty/treaty-declaration-1864-st-petersburg.htm

De Souza, P. (2008). E*l mundo antiguo en la guerra. Una historia global*. Akal.

Delgado Granados, M. L. (2021). D*elitos informáticos*, D*elitos electrónicos*. http://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

F5 Networks. (2021). *Denial of Service*. F5 Glosary. https://www.f5.com/es_es/services/resources/glossary/denial-of-service

Harris, E. D., Acton J. M. & Herbert, L. (2016). Chapter 3: Governance of Information Technology and Cyber Weapons. In E. D. Harris (ed.), *Governance of Dual-Use Technologies: Theory and Practice* (pp. 112-157). American Academy of Arts & Sciences. https://www.amacad.org/publication/governance-dual-use-technologies-theory-and-practice

Hernández Sánchez, C. (2018). Control a las exportaciones de cibertecnologías: Un análisis del Arreglo de Wassernaar y sus implicancias para la ciberseguridad. *Revista chilena de derecho y tecnología*, *7*(1), 61-78. https://doi.org/10.5354/0719-2584.2018.48828

Horzella Cutbill, B. (2021) *Control de transferencias de armas convencionales y bienes de uso dual: Acuerdo de Wassenaar. Antecedentes de contexto y revisión de las experiencias de Argentina, México y la Unión Europea*. Biblioteca del Congreso Nacional de Chile. Asesoría técnica parlamentaria. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/32103/2/Informe_BCN_Acuerdo_de_Wassernaar.pdf

International Committee of the Red Cross. (2010). *Jus ad bellum y jus in bello*. https://www.icrc.org/es/doc/war-and-law/ihl-other-legal-regmies/jus-in-bello-jus-ad-bellum/overview-jus-ad-bellum-jus-in-bello.htm

Kaspersky. (n. d.). *¿Qué es el spyware? – Definición*. https://latam.kaspersky.com/resource-center/threats/spyware

Kimball, D. (2022). *The Wassenaar Arrangement at a Glance*. Arms Control Association. https://www.armscontrol.org/factsheets/wassenaar

Libicki, M. (2009). *Cyberdeterrence and Cyberwar*. Rand Corporation https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Mateos, I. (2019, September 13th). *Corea del Norte, la última apuesta nuclear*. CISDE Observatorio. https://web.archive.org/web/20200927174620/https://observatorio.cisde.es/actualidad/corea-del-norte-la-ultima-apuesta-nuclear/

NATO Cooperative Cyber Defence Centre of Excellence. (n.d.). *The Tallinn Manual*. https://ccdcoe.org/research/tallinn-manual/

Navarro, J. (2016). *Bélico- Definión, Concepto y qué es*. Definición ABC. https://www.definicionabc.com/historia/belico.php

Real Academia Española (n. d.). *Guerra*. Diccionario de la lengua española. Consulted January 4th, 2022. https://dle.rae.es/guerra

Reinel Sánchez, J. (2004). Una respuesta a una pregunta ¿Qué es la guerra? *Apostа*. *Revista de Ciencias Sociales*, (6), 1-28. http://www.apostadigital.com/revistav3/hemeroteca/reinel1.pdf

Reventos, L. (2012, May 28th). *Flame, el código malicioso más complejo para ciberespiar*. El País. https://elpais.com/internacional/2012/05/28/actualidad/1338218887_695257.html

Robles Carrillo, M. (2019). El régimen jurídico de las operaciones en el ciberespacio: estado del debate. *Documento Opinión*. *Instituto Español de Estudios Estratégicos*, (101), 1-18. https://www.ieee.es/Galerias/fichero/docs_opinion/2019/DIEEEO101_2019MARROB_legalciber.pdf

Rojas Amandi, V. M. (2010). *Derecho Internacional Público*. UNAM; Instituto de Investigaciones Jurídicas; Nostra Ediciones.

Rosas, M. C. (2016, September 21st). La paz es mucho más que la ausencia de guerra o el desarme. *Boletín* UNAM-DGCS-638, *September*. https://www.dgcs.unam.mx/boletin/bdboletin/2016_638.html

Ruíz, J. (2016). Ciberamenazas: ¿el terrorismo del futuro?, *Documento Opinión*. *Instituto Español de Estudios Estratégicos*, (86), 1-21. http://www.ieee.es/Galerias/fichero/docs_opinion/2016/DIEEEO86-2016_Ciberamenazas_JRuizDiaz.pdf

Sánchez Madero, G. (2010). Los Estados y la Ciberguerra. *Boletín de Información*, (317), 63-76. https://dialnet.unirioja.es/servlet/articulo?codigo=3745519

Schmitt, M. (2013). *Tallin Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. http://csef.ru/media/articles/3990/3990.pdf

Schneier, B. (2007). *Cyberwar: Myth or Reality*? Schneier on Security [Blog]. https://www.schneier.com/blog/archives/2007/11/cyberwar_myth_o.html

Salazar Claver, J. (2019). De la flecha al ratón. Consideraciones jurídicas de las operaciones ofensivas en el ciberespacio. In A. Serrano Barberán, E. M. Silvela Díaz-Criado, R. J. de Espona, S. de Tomás Morales, J. de Salas Claver & A. López-Casamayor (coords.), *Cuadernos de Estrategia* 201. *Límites jurídicos de las operaciones actuales: nuevos desafíos* (pp. 133-175). Instituto Español de Estudios Estratégicos; Ministerio de Defensa. https://www.ieee.es/Galerias/fichero/cuadernos/CE_201.pdf

The Wassenaar Arrangement. (2019). *On Export Controls for Conventional Arms and Dual-Use Goods and Technologies. Public Documents, Volume* I. *Founding Documents*. Wassenaar Arrangement Secretariat. https://www.wassenaar.org/app/uploads/2021/12/Public-Docs-Vol-I-Founding-Documents.pdf

Touré, H. (2014). *La búsqueda de la confianza en el ciberespacio*. Unión Internacional de Telecomunicaciones.

U/A. (N. D.) *Ataques con acceso*. Consulted January 9th, 2022. https://www.sapalomera.cat/moodlecf/RS/1/course/module11/11.2.2.3/11.2.2.3.html

United Nations. (2018, December 5th). *Resolución* 73/27. *Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional*. https://undocs.org/sp/A/RES/73/27

United Nations. (2019, June 24th). A/74/120 *Resolution. Developments in the field of information and telecommunications in the context of international security*. https://undocs.org/Home/Mobile?FinalSymbol=A%2F74%2F120&Language=E&DeviceType=Desktop&LangRequested=False

United Nations. (2022, June 8th). A/77/92 *Developments in the field of information and telecommunications in the context of international security, and advancing responsible State behaviour in the use of information and communications technologies*._https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/375/58/PDF/N2237558.pdf?OpenElement

United Nations Office for Disarmament Affairs (UNODA). (2019, July). *Fact Sheet, Developments in the field of information in the context of international security*. https://front.un-arm.org/wp-content/uploads/2019/07/Information-Security-Fact-Sheet-July-2019.pdf

Universidad Veracruzana. (2016). *Conocimientos generales: ¿Qué es el malware y cómo se clasifica*? https://www.uv.mx/infosegura/general/conocimientos_virus-2/

Vélez Martínez, C. (2019). *Ciberguerra*. Instituto de Ingeniería UNAM. http://www.ii.unam.mx/es-mx/AlmacenDigital/CapsulasTI/Paginas/ciberguerra.aspx