DOI 10.26807/rfj.vi.400

Martens Clause: application in the context of Cyberwar

Cláusula de Martens: aplicación en el contexto de la Ciberguerra

Carolina del Rocio Changoluisa Barahona
Independent legal researcher
City: Quito
Country: Ecuador

Original article (miscellaneous)
RFJ, No. 12, 2022, pp. 170 - 202, ISSN 2588-0837

ABSTRACT: Certainly, with the codification of International humanitarian law or commonly known as the law of war or the law of armed conflict, the humanitarian problems derived from the armed conflicts were solved. However, against situations didn't consider the traditional law is given the possibility of appeal to other sources inside International law like General principles of law, the international custom, or the doctrine. The Martens Clause is shown as a mechanism of interpretation against problems or situations that couldn't be contemplated by the conventional law of IHL[1]. This article pretends to analyze the application of the Martens Clause in the context of cyberwar. It will be examined in the context of armed conflict, and it will be checked the normative development that could be applied to an armed conflict cataloged as cyberwar. It will be shown the important role that performs the Martens Clause against the empty normative of cyberwar that it will be presented as a new threat inside of the *jus in bello*.

KEYWORDS: Martens Clause, International Humanitarian Law, Information Society, Cyberwar, Cyberspace.

1 Understood as International Humanitarian Law.

RESUMEN: Con la codificación del Derecho Internacional Humanitario o mejor conocido como "las leyes y usos de la guerra", se ha logrado solucionar los problemas humanitarios generados por la barbarie de la guerra. ha sido capaz de resolver los problemas humanitarios generados por la barbarie de la guerra. Sin embargo, en situaciones no contempladas por las normas tradicionales, se deja paso a la posibilidad de acudir a otras fuentes, como los Principios del Derecho Internacional, la costumbre o la doctrina. La Cláusula Martens se presenta como un mecanismo de interpretación ante problemas o situaciones que no pueden ser cubiertas por las normas convencionales del DIH[2]. Este artículo tiene como objetivo analizar la aplicación de la Cláusula Martens en el contexto de la ciberguerra. En este sentido, se examinará su interpretación en el contexto de los conflictos armados y se identificarán las normas del DIH aplicables a la ciberguerra como conflicto armado, además, se revisará el desarrollo normativo vigente aplicable a un conflicto armado catalogado como ciberguerra. De esta forma, se demostrará el importante papel que juega la Cláusula Martens en el vacío normativo de la ciberguerra, que se presenta como una nueva amenaza latente dentro del *jus in bello*.

PALABRAS CLAVES: Cláusula Martens, Derecho Internacional Humanitario, Sociedad del conocimiento, Ciberguerra, Ciberespacio.

JEL CODE: F02, L86.

2 Entendido como Derecho Internacional Humanitario

INTRODUCTION

In the colossal world in which we live, armed conflicts have undergone great transformations. The history of humanity is marked by wars and massacres; however, States have also struggled to achieve peace through concrete actions that allow full coexistence. In the field of armed conflicts, the law has been presented to protect people who do not participate directly or those who can no longer participate in the conflict. Moreover, it is thanks to the development of International Humanitarian Law that it has also been possible to limit the methods and means used in warfare. However, the world is evolving and so is everything concerning armed conflicts, the means, and methods, and even the people involved in a conflict. Today, humanity is surrounded by a growing technology that has revolutionized and expanded the scenario of war. The terrestrial is set aside to analyze the imminent dangers that can be unleashed in cyberspace[3] . Indeed, the broad technological development has resulted in an information society[4] that poses new realities and in which, multiple changes can be observed within the branch of law. In this way, we can confirm what was stated by Bericat (1996) when referring to the existence of "a growing concern and sensitivity that surrounds scholars and theorists regarding the presence of a new society" (p.112).

3 The U.S. Department of Defense defines it as a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

4 The "Information Society" better known as "Infocommunication Society" is defined as a society that uses, both intensively and extensively, computers and telematic networks, the combination <<Computer-Network>>, the social technostructure of <<Computers in Networks>> technologically defines the information society. (Bericat, 1996).

The existing concern has been generated because there is uncertainty about how to cope with the growth of new technologies since every day more and more human activities are added to the dependence on a computer which in turn is connected and interacts structurally through a network[5] . In addition, with the emergence of information and communication technologies[6] , it is now easy to obtain information and establish communications. Consequently, the ITU[7] emphasizes that "networks now play a key role in the critical infrastructures of many countries, such as electronic commerce, voice and data communications, facilities, finance, health, transport, and defense" (Unión Internacional de Telecomunicaciones, 2008, p. 6).

In the field of law, reference has already been made to the role played by the States in the face of the progressive technological development, considering what has been pointed out by Drezner (2007) (cited by Radu, 2002, p. 8) that the power of the State increased in the digital era due to tactics employed by them, where the emphasis is placed on the work done by the great powers to safeguard their interests. This is how a prominent inequality can be evidenced, since at the interstate level some States may be better equipped for the management and development of technology. Therefore, the idea that networks transform spaces, in which territoriality prescribes and is extinguished, is present. (Drezner, 2007, p. 92).

5 For the purposes of this article, the network will be understood as the interactive infrastructure on which the Infocommunication Society is based (Bericat, 1996).

6 ICT is defined as Computer-based technologies and computer-mediated communications used to acquire, store, manipulate and transmit information to people and business units both internal and external to an organization (Benjamin and Blunt, 1992).

7 The International Telecommunication Union (ITU) is the specialized agency of the United Nations in the field of telecommunications and information and communication technologies.

Furthermore, it can be evidenced that networks have also come to modify the scenarios of war, since unlike traditional scenarios such as air, sea, land, or space; the new war scenario cataloged as cyberspace represents multiple uncertainties for the States. Cyberspace has established itself as "an environment with its means and rules, with the particularity of not having a specific physical location, which would imply a questioning of the usefulness of the traditional categories with which we approach real warfare" (Eissa et al., 2012, p. 2).

The approach to the development of an eventual war within this new environment has already been considered by international security and defense organizations, and for this reason, security is approached as the process whose purpose is to protect systems, applications, resources, and networks (Unión Internacional de Telecomunicaciones, 2008, p. 6). As services are permanently connected to a network, they are vulnerable to possible attacks or problems that may arise in cyberspace. Therefore, the concept of security has also been transformed to deal with the problems that may arise in this changing scenario, for which international law must be prepared.

States must be aware of the new changes represented by the inclusion of cyberspace as a "field or territory" of warfare. Considering that, while this may be a novel space for human interaction, on the other hand, it also takes shape as a space in which cybercrimes or cyber espionage are carried out. This site is the one that should generate more concern as the results that are triggered within this realm "can produce modifications in the physical world" (Eissa et al., 2012, p. 3).

However, "cyber warfare can have far-reaching consequences" (Kittichaisaree, 2017, p. 1). For this reason, States must safeguard certain rights of individuals, since many

of these rights may be infringed in the context of an armed conflict generated in cyberspace. What has happened is a transition regarding how societies can initiate an armed conflict and the new role played by the armed forces within this new scenario. In the defense field, cyberspace would come to be configured as a new military domain.

This gives way to cybersecurity[8] which would configure a cyber defense for the protection of the so-called *critical information infrastructures*[9] defined as organizational structures and facilities with a high degree of importance for a State. It should be noted, "that their failure or degradation would result in sustained supply shortages, significant disruption to public safety, or other dramatic consequences." (García Zaballos, 2016, p. 35). For this reason, what must be considered are the possible consequences of an attack on critical infrastructures in the event of a cyberwar.

The purpose of this paper is to analyze the application of the Martens Clause in the context of cyberwarfare. Moreover, it will start by examining the interpretation of the Martens Clause in the context of armed conflicts. It will then move on to identify the rules of international humanitarian law applicable to cyberwar as an armed conflict. This part will study cyberwar and its relationship with IHL, the framework

8 ITU defines it as the set of tools, policies, security concepts, security safeguards, guidelines, risk management methods, actions, training, best practices, insurance, and technologies that can be used to protect organizational and user assets in the cyber environment (Recommendation ITU-T X.1205, 2008).

9 The Commission of the European Communities states that: Critical infrastructures consist of those physical and information technology facilities, networks, services, and assets that, if disrupted or destroyed, would have a serious impact on the health, safety, or economic well-being of citizens or the effective functioning of governments in the Member States (European Commission, 2004).

that regulates cyberwar will be discussed: *jus ad bellum* and *jus in bello*, in addition, the development of the rules that have been established for its application will be indicated. The final part of the paper will evaluate the role played by the Martens Clause in the normative vacuum that regulates cyberwarfare. This part will analyze the role of States in the regulatory development of cyber warfare and the vulnerability of critical infrastructures to the development of cyberwarfare. In this way, the aim is to answer two questions that guide the writing of this paper:

What protection would the Martens Clause provide in the face of the lack of regulatory development in cyberwarfare as a regulatory conflict?

How does international humanitarian law intervene in the face of an armed conflict categorized as cyberwar?

1. ORIGIN OF THE MARTENS CLAUSE

1.1. Fyodor Fyodor Firovich Martens as a jurist and diplomat

F.F Martens (1845-1909) entered the Faculty of Law of the University of St. Petersburg in 1863, where he obtained the title of professor of international law. He stood out as a brilliant student and gained the support and admiration of great professors of the time from Western Europe. His way of seeing the world allowed him to develop an independent and innovative way of thinking for his time. Martens was always critical of the state of international law as a science, and his ideas called for the creation of a contemporary international law with functions that would meet the needs of States and at the same time express the moral values of mankind. (Pustogarov, 1996, p.326).

Martens was an opponent of thinking that implied that law is based on force, he pointed out that:

> In such cases, even leading experts confused law enforcement mechanisms with the law itself, because the fact that force exists to safeguard the law does not mean that force should be the basis of law. According to Martens, the inviolability of human life, honor, and dignity are recognized rights of every person, not because they are protected by criminal law, but because every person has an inalienable right to life, honor, and dignity. (Pustogarov, 1996, p. 327)

For Martens, the idea of protecting the rights and interests of the human being was paramount in international relations, in his opinion, what determined the degree of civilization of the States and the field of international relations lay in the respect for human rights. In the diplomatic sphere, Martens did not share the idea that law would be the mechanism to abolish war completely; for him, what had to be done with the help of humanitarian objectives was to limit the barbarity of war using norms that were accepted by the states (Pustogarov, 1996, p. 328).

It is within his diplomatic position as a delegate of Russia that in the Preamble to the Second Hague Convention of 1899, by a declaration, the Martens Clause begins to become part of the law of disputes (Ticehurst, 1997, p. 131). The transcript states that:

> Pending the promulgation of a more complete Code of the laws of war, the High Contracting Parties deem it expedient to record that, in cases not covered by the regulations adopted by them, the peoples and

> belligerents remain under the safeguard and the rule of the principles of the law of nations, such as result from the usages established among civilized nations, from the laws of humanity, and the requirements of public conscience. (Convención II de La Haya relativa a las leyes y usos de la guerra terrestre y reglamento anexo, 1899, preámbulo)

1.2. Interpretation of the Martens Clause

Although the Clause has been enunciated, it does not have an official interpretation that allows knowing exactly its field of application. Given this, different interpretations have been established and analyzed from the doctrine, jurisprudence, and custom, conceived strictly or broadly (Ticehurst, 1997, p. 132). The broad interpretation establishes that considering that there is a low number of international treaties relating to the law of armed conflict, "the Clause stipulates that what is not explicitly prohibited by a treaty is not permitted *ipso facto*" (Ticehurst, 1997, p. 132).

This interpretation could be considered the most functional since it provides comprehensive protection per se to the parties involved in the development of an armed conflict by delimiting a barrier to the methods and means used in war, however, the future problem of this conception is its difficult acceptance because States will not commit themselves to diminish their power of defense and attack as a response in the scenario of an armed conflict. States will always look after their interests and will try to find ways of not being bound by a norm whatever its origin.

On the other hand, according to Tocino (2018) "the Martens Clause is general, avoids possible normative gaps,

and reaches all parties to International Humanitarian Law" (p. 179). This idea can be understood in the light of the fact that "conduct in armed conflicts is not only judged based on treaties and custom but also on the principles of international law to which the Clause refers" (Ticehurst, 1997, p. 132).

This interpretation that enunciates features of generality could finally help to understand what the Clause mentions and its field of application for a close normative development, it is the opinion of Judge Shahabuddeen within the Nauru case that could contain the answer by stating that:

> The principles of international law referred to in the Clause derive from one or more of three distinct sources: the established customs among civilized nations (referred to as "established usages" in Art. 1.2 of Additional Protocol I), the laws of humanity (referred to as "principles of humanity" in Art. 1.2) and the requirements of public conscience (referred to as "dictates of public conscience" in Art. 1.2). (Ticehurst, 1997, p. 135)

The Martens Clause, in mentioning customary norms, stresses the importance of their application concerning armed conflicts. In the same way, the reference to the laws of humanity will be interpreted in the sense of prohibiting any method or means of warfare not necessary for the attainment of a military advantage. Finally, for the dictates of the public conscience, it refers to declarations, resolutions, and communications made by qualified persons and institutions that evaluate the laws of war (Ticehurst, 1997, pp. 135-136).

1.3. Evolution of the Martens Clause

The Martens Clause was drafted in both the 1949 Geneva Conventions and their Additional Protocols. It had one important change; in the case of the Geneva Conventions, it was removed from the Preamble to the body of the treaty. In the case of the I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field of 1949, it was established in Article 68; the II Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea of 1949, it was established in Article 62, the Third Geneva Convention relative to the Treatment of Prisoners of War of 1949 provided for it in Article 142 and the Fourth Geneva Convention relative to the Protection of Civilian Persons in Time of War of 1949 provided for it in Article 158.

The Clause was stipulated for a different purpose; thus, it was framed in the articles concerning the denunciation of the Convention by the High Contracting Parties (Meron, 2000, p. 80). The articles have the same content, which is as follows:

> The denunciation shall be valid only to the denouncing Power. It shall not affect the obligations which the Parties to the conflict are bound to fulfill under the principles of the law of nations, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of public conscience. (Geneva Convention relative to the Protection of Civilian Persons in Time of War, 1949, art. 158).

On the other hand, in the I Additional Protocols the Martens Clause was moved to Article 1 (2) and worded as follows:

> In cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and rule of the principles of the law of nations derived from established custom, the principles of humanity, and the dictates of public conscience (Protocol Additional to the Geneva Conventions and Relating to the Protection of Victims of International Armed Conflicts, 1949, art. 1).

According to Meron (2000) "in Protocol II, a changed version of the clause was included in the Preamble, which omits references to both custom and international law" (p. 81). It is worth considering that another of the changes that the clause has undergone are the words used for its drafting since they have caused it to lack coherence and even the meaning of the clause to be misunderstood or have different interpretations (Ticehurst, 1997).

About the principles of humanity, it is stated that the Martens Clause incorporates three elementary considerations of humanity: a) the right of the parties to choose the means and methods of warfare is not unlimited; b) the duty to distinguish between civilians and those engaged in military operations; c) prohibition of targeting the civilian population. (Meron, 2000, p. 83). In this case, the International Committee of the Red Cross (ICRC) pointed out that the clause has a dynamic factor, thus proclaiming "the applicability of the above principles irrespective of subsequent developments in types of situations or technology". (CICR, 1977, p.39) Furthermore, within the Commentaries to the Additional Protocols to the Geneva Convention it was concluded that the Martens Clause: a) applies independently of the treaties containing it; b) provides that the principles of international law apply in all armed conflicts (CICR, 1977, p. 39).

The interpretation given by the Jurisprudence has allowed for a clearer notion of the scope of the rule, which is why the International Court of Justice has made it clear that the Martens Clause is "an effective means to cope with the rapid evolution of military technology" (Meron, 2000, p. 87) This opens the way to the possibility of a wide application of the clause to eventual situations that may arise in the new scenarios of war. For this reason, the importance of the clause is stressed as a mechanism that limits certain means and methods of warfare that have been evolving and have not been contemplated by the rules of IHL. Thus, it fulfills its purpose of legally covering situations arising from hostilities and everything that is not contemplated by the conventional norms (Salmon, 2012, p. 36).

2. ARMED CONFLICT AND CYBERWARFARE

2.1. Definition of Armed Conflict

Custom is the source of IHL, at first, IHL applied exclusively to international armed conflicts, however, humanity witnessed conflicts without a purely international character, and due to this, rules have been adopted to protect the victims against the development of these hostilities. Therefore, an armed conflict may be of an international or non-international character.

As he points out. Salmon (2012) "neither the four Geneva Conventions of August 12, 1949, nor their Additional Protocols of June 8, 1977, contain a definition in the proper sense of this". (p. 29) However, the Jurisprudence has been providing elements to define and specify the concept of armed conflict. In this case, the Criminal Tribunal for the former Yugoslavia defined it as "a resort to armed force between states" (Kittichaisaree, 2017, p. 204)

Reference has also been made to the existence of other elements which are: a) of a temporary nature, since the conflict will be prolonged in time; b) of organization, referring mainly to a level of organization that the group participating in the conflict must have; c) inclusion of the notion of groups, since the conflict may be generated between States or between an armed group and the State authority; d) inclusion of the notion of groups, since the conflict may be generated between States or between an armed group and the State authority (Salmon, 2012, p. 30).

On the other hand, the ICRC has pointed out that IHL applies to cyber warfare, but it does not neglect the progressive development of IHL that must be carried out concerning new technologies. The update of the Commentary to the First Geneva Act of 1959 emphasizes the issue of progressive development, thus the ICRC states:

> The updated Commentary to the I Convention offers a more comprehensive look that takes into consideration the issues and challenges observed in contemporary armed conflicts, developments in technology, international law, and national legislations. (Cameron et al., 2015, p. 7)

The same commentary discusses the issue of "dealing with operations cyber as an armed force equitable to armed conflict" (Cameron et al., 2015, p. 15). What should be kept in mind is that IHL will be triggered "by cyber operations if they are conducted by one State against another and in support of more classical military operations." (Kittichaisaree, 2017, p. 204) Even the ICRC states that if the effects of cyber operations are like those of classic military operations, they would be equivalent to an armed conflict, with the main attention if they

have the consequence of causing the death of civilian or military persons, or in turn, destroying both military and civilian assets" (Kittichaisaree, 2017, p. 204).

2.2. Cyberspace as a new theater of warfare and cyber attacks

The impact of the technological development that the human being has given to different matters has generated that there is a frenetic change of the known everything. This has been done to give way to technological innovations, however, this growing technology has come to encompass spheres of Law that merit important attention for its full development. Cyberspace is "an artificially created domain of information and economic exchange" (Kiggins, 2002, p. 163). This domain has no central authority, it is seen as an anarchic domain, in such a sense Deibert & Rohozinski (2010) (cited by Kiggins, 2002, p. 163) point out that cyberspace is subject to rules concerning physics and codes.

The formation of cyberspace is established through the interconnection of computers resulting in a globalized network, which can be seriously affected by possible vulnerabilities of the network or attacks to control and obtain its information. The exchange of information is carried out through cyberspace, which crosses the control of the State in the geographical aspect since they are networks that cross borders without any limit. Faced with this eventuality, States have formulated norms that allow information to be exchanged securely (Kiggins, 2002, p. 174).

The definition of attack contemplated in Protocol I related to the Geneva Conventions enunciates certain characteristics that allow classifying a cyberattack as an armed conflict. For this, the cyberattack should be understood as "that

offensive or defensive cyber operation which is expected to cause loss of life, injury to persons and damage or destruction of property" (Reguera Sánchez, 2015, p. 15). If understood in this way it will be regulated by IHL. By nature, a cyber-attack aims to prevent access to a network, either by disconnecting it or by accessing computer networks to steal information and manipulate it. In addition, it is important to consider the advantages that come from the use of cyber-attacks in an armed conflict, firstly, its organization in cyberspace provides speed; as a second point, for a cyber-attack no target is remote; finally, cyber-attacks have more tools and targets of attack that are coupled with limited costs (Kittichaisaree, 2017, p. 158).

The means of warfare used to carry out a cyber-attack encompass "any device, material, instrument, instrument, mechanism, equipment or software" (Kittichaisaree, 2017, p. 158). The lack of security in cyberspace directly affects Information Technologies, for this reason, it is the role of the State to guarantee the fulfillment of individual freedoms within this environment known as cyberspace (Carlini, 2016, p. 11).

The concept of cybersecurity has been established due to the latent threats in the use of cyberspace, one of these threats is cyberwar understood as "Sanchez (2015) the conflict between technologically advanced states, which is carried out through cyberattacks in isolation, or as part of a conventional war" (cited by Polloni, 2018, p. 131). It is because of this threat that cyberspace has been categorized as a new battlefield. Regarding the law of armed conflict, States will have to respect the *ius ad bellum* and *ius in bello in the* event of a cyberwar, until international law develops regulations applicable exclusively to these conflicts (Reguera Sánchez, 2015, p. 5).

On the other hand, it should also be considered that the functioning of society currently lies in the performance of tangible and intangible elements that form a critical infrastructure, and it is this infrastructure composed of services, goods, and mechanisms dependent on a technology that make a State vulnerable (Luke, 2012, p. 409). For this reason, the protection of this infrastructure that can be attacked in the context of cyberwarfare in the face of the growing development of computer weapons is emphasized. (Polloni Contardo, 2018, p. 21).

A case in point is the attack on the computer network to disable air defense systems during NATO military operations in Kosovo in 1999 or the massive blackout in Ukraine due to a cyberattack that stopped and shut down the systems of six energy suppliers of the electricity network (Kittichaisaree, 2017, p. 156).

2.3. Regulatory framework for cyberwarfare

In the framework of the *ius ad bellum* a cyberattack can be categorized as an act of war by a) a universal manifestation through a United Nations declaration of the cyberattack as an act of war; b) the definition that a group of States gathered in an organization gives to the cyberattack, identifying its illegality; c) the unilateral declaration of a State establishing the cyberattack as an imminent act of war (Polloni Contardo, 2018, p. 136). However, in any of these scenarios, there are doubts as to how the action of the affected State should be conceived and what would be the responsibility of the responsible State.

Within the framework of *ius in bello,* International Humanitarian Law will regulate cyber warfare only if the cyberattack takes place within the context of an armed conflict.

Therefore, it is required that the cyberattack is previously classified as an armed conflict, in addition, cyberwarfare refers to the means and methods of warfare using technologies that can cause consequences outside the network system and reach to develop palpable effects in the real world (Droege, 2011). Among these consequences, it is noted that:

> The materialization of potentially catastrophic scenarios such as the collision of aircraft, the emission of toxic substances from chemical plants, or the disruption of vital infrastructure and services such as electricity or water supply networks cannot be ruled out. The main victims of such operations would most likely be civilians. (Polloni Contardo, 2018, p. 137)

Thus, the *ius in bello* will determine that "if the means and methods of cyberwarfare were to come to produce the same real-world effects as conventional weapons (destruction, disorder, damage, injury or death), they are governed by the same rules as conventional weapons" (Polloni Contardo, 2018).

2.4. Regulatory development

With the cyber realm, state practice and judicial decisions in Europe and the USA "are the most developed of all the regions of the world due to their dominant advancement in cyber technology" (Kittichaisaree, 2017, p. 52). Added to this problem is the regulatory vacuum in cyberspace and the unwillingness of states to develop it. In 2002, during the Prague Conference, NATO launched the global program for the coordination of cyber defense to strengthen alliances between states and combat cyber-attacks. In 2010, the Lisbon Summit was held to define a strategic concept on cyber defense policy. As a result, NATO approved a new cyber defense policy on June

1, 2010. In the case of the United Nations, initiatives for the regulation of cyberspace have been minimal and those that have been made only cover specific aspects, there is still no consensus among all states. However, in the face of disagreements between States, global agreements have been established, with basic principles relating to the subject (Reguera Sánchez, 2015). The main resolutions are:

- General Assembly Resolutions 55/63 (2000) and 56/121 (2001) invites the Member States to take steps to develop national laws and policies to combat the criminal misuse of information technology.

- General Assembly Resolutions 57/239 (2002) for the creation of a global culture of cybersecurity.

- General Assembly Resolution 58/199 (2004) for the protection of information infrastructures.

- On December 5, 2018, the General Assembly adopted resolution 73/27 on developments in the field of information and telecommunications in the context of international security.

- On 22 December 2018, the General Assembly adopted resolution 73/266 on promoting responsible behavior by states in cyberspace in the context of international security.

The United Nations Counter-Terrorism Office on its official website mentions documents on cybersecurity submitted to a principal or subsidiary organ of the United Nations, these are:

- Sixth Review of the United Nations Global Counter-Terrorism Strategy A/RES/72/284

- UN Security Council Resolution 2341 (2017).
- UN Security Council Resolution 2370 (2017).
- Security Council text S/2015/939 (Madrid Guiding Principles).

The Council of Europe was the first international organization to adopt a treaty for the fight against Internet crime, thus the Budapest Convention entered into force on July 1, 2004. This is a treaty that addresses both cybercrime and Internet crime, through international cooperation and the adoption and development of national regulations on cyber security. (Reguera Sánchez, 2015, p. 12). As the Estonian Minister of Foreign Affairs points out in the 2020 Cybersecurity Report Risks, Progress and the Way Forward in Latin America and the Caribbean:

> From the national and international perspective, the Budapest Convention provides a comprehensive and reliable international legal framework for combating cybercrime, and during almost two decades of its existence, it has become a global reference instrument. Therefore, the Budapest Convention has become a preferred model for many countries in terms of promoting their national legislation, building international cooperation, and exchanging electronic evidence. (BID & OEA, 2020, p. 36)

In May 2010, the European Commission presented one of the seven pillars of the Europe 2020 Strategy, which aims to set targets that will enable the European Union to grow and exploit the potential of ICTs (Reguera Sánchez, 2015, p. 12). As for recent actions they have taken, it is noted that:

- The European Commission signed with the European Cyber Security Organization (ECSO) a public-private partnership to structure and coordinate industrial resources for digital security in Europe. (BID & OEA, 2020, p. 36)

Furthermore, the European Union is aligned with the position that international law, and in particular the UN Charter, applies to cyberspace. Moreover, the EU gives high priority to establishing a strategic framework for conflict prevention and stability in cyberspace, including the special protection it gives to fundamental rights and freedoms in the face of possible limitations under the pretext of cybersecurity. Although the strengthening of European cybersecurity is essential, the aim is to provide safe and secure cyberspace for all. Similarly, the Organization of American States (OAS) has played an important role in certain actions that have helped States to become aware of cyber threats and the mechanisms to deal with them (BID & OEA, 2020, pp. 27-34).

To continue developing applicable regulations, the Tallin Manual created by Michael N. Schmitt is positioned as a tool for jurists, since it allows interpreting the existing rules to the assistants, in the same way, it is a tool for jurists who analyze the eventual conflicts that can be generated in cyberspace (Reguera Sánchez, 2015, p. 15). To understand cyber-attacks comprehensively, it is necessary to consider what has been analyzed and drafted by the Group of Experts of the Tallinn Manual. This non-binding body of norms is of great help and serves as a tool for understanding cyberspace attacks. The Tallinn Manual has established:

> Eight factors - previously proposed by Michael N. Schmitt in 1999 - are essential to determine whether

> a cyber operation can be classified as a "use of force". These factors consist of invasiveness, severity, military character, immediacy, state involvement, quantification of effects, presumed legality, and directness. According to a group of experts, a cyber operation counts as a "use of force" when it produces the same level of physical damage to objects and people. (Carlini, 2016, p. 9)

In addition, the Manual identifies the means of cyberwarfare, defines the subjects of cyber-attacks to the category of persons within IHL, determines when the cyber-attack will constitute an armed conflict, etc.

3. THE ROLE OF STATES IN THE REGULATORY DEVELOPMENT OF CYBERWARFARE

3.1. Global governance

Global governance is a concept that should focus on the role and effectiveness of the state in an era in which the globalization of information and economic exchange is characteristic. Cyberspace presents itself as a new scenario that surpasses the concept of sovereignty agreed upon by states. For this reason, what is required is that through continuous cooperation on the part of states, a fusion of transnational information exchange policies is achieved (Kiggins, 2002, p. 175).

States have formed organizations that have emerged from transnational cooperation, such as the case of NATO created to promote regional security. However, the inaction of states to coordinate global governance focused on cybersecurity is evident. It should be noted that transnational norms focused on cybersecurity issues would be considered of vital importance for the formation of support structures within

global governance. The role of leading this global governance is based on a) driving the constitutive rules that will shape the regulatory rules in a global regime (Kiggins, 2002, p. 175).

In addition, it should be noted that cooperation on cybersecurity issues should focus on a) non-proliferation of cyberweapons. This would have the effect of limiting the number of cyber threats for which the State will have to develop countermeasures; b) increased cooperation in cybersecurity could pool resources and capabilities to overcome the problem of resource allocation. This would overcome the technical obstacles arising from the lack of resources for cybersecurity development; c) develop a consensus on a standard or set of standards governing the exchange of information, arrest, and prosecution for the commission of crimes in cyberspace; d) develop a consensus on a standard or set of standards governing the exchange of information, arrest, and prosecution for the commission of crimes in cyberspace (Kiggins, 2002, p. 175).

Hence, as pointed out in the Cybersecurity 2020 report:

> As cyber threats are becoming increasingly sophisticated, it is the responsibility of states to ensure that the activities of perpetrators do not go unnoticed. Therefore, policy and legislative initiatives, along with capacity-building measures, are some of the key elements in combating threats arising from cyberspace, including the conduct of criminals. Therefore, the implementation of relevant legislation and the adoption of strategic approaches will support the effectiveness of national criminal justice efforts and international cooperation. (BID & OEA, 2020, p. 42)

3.2 Importance of critical infrastructures

Today, modern society depends on many services provided by critical infrastructures. If these services were to be affected or interrupted for a prolonged period, they could generate serious economic impacts and could even affect people's physical integrity. Problems related to critical infrastructures can arise from a variety of sources, problems related to system downtime, natural disasters, acts of terrorism, or even war (Lopez et al., 2012, pp. 1-2).

The Critical Infrastructure Protection Act of 2001 issued by the United States defined critical infrastructure as:

> Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on the national security, national economic security, national health or national public safety, of any combination of those matters. (Harašta, 2018, p. 2)

On the other hand, the European Commission 2004 in a communiqué stressed the increasing dependence of society on high-tech infrastructures and emphasized with much more importance of the growing interconnection between these infrastructures. In 2005 the European Community adopts the European Programme for Critical Infrastructure Protection (EPCIP), who's main "the objective is to improve the protection of critical infrastructures (CIP)[10] of the European Union (EU)" (Programa Europeo Para La Protección de Infraestructuras Críticas, 2006).

10 PIC stands for Critical Infrastructure Protection or CIP for Critical Infrastructure Protection.

The EPCIP established a more delimited definition of critical infrastructures, intending to expressly cover cyber and physical networks:

> Therefore, the definition was expanded outside of physical facilities (railroads, pipelines, and power plants) to procedures: complex networks of socially and culturally determined values preceding and helping to operate heavy physical facilities. These social and cultural procedures may be technologically connected, but the diffusion of these values will be mediated to a large extent by the technological means present in the information society. (Harašta, 2018, p. 3)

The EU has identified the sectors that comprise critical infrastructure, these are: a) energy; b) nuclear energy; c) information and communication technologies; d) water; e) food; f) health; g) finance; h) transportation; i) chemical industry; j) space; (García Zaballos, 2016, p. 39).

Regarding the vulnerability to which IICs are subject[11], Nickolov (2005) has determined that:

> Critical Information Infrastructure (CII) has become particularly vulnerable to fun-seeking hackers, criminals, and even state actors and terrorists. The main tools used to attack critical systems are malware (computer viruses, worms, logic bombs, Trojans) that modify and destroy the information or crash computer systems. Tools to spy on the exchange of information on computer networks, as well as tools to modify the normal operation of the computer network and block access to its services, are also widely used for destructive purposes. (p. 107)

11 CII stands for Critical Information Infrastructures.

The measures that can be taken to provide protection should be focused on preventing cyber-attacks on IICs and reducing the recovery time from cyber-attacks. These measures can be taken at the company level with a focus on a) physical protection of key elements of the IIC; b) technical security; c) social, regarding training and control of personnel; d) security policy including security issues, control, data availability, as well as data recovery and contingency plans; and e) public-private cooperation between companies and the government. (Nickolov, 2005, p. 112). While each State at the national level, what must be done to protect the IICs is:

> Improving secondary legislation related to CIP; monitoring the implementation of relevant legislation by the parties involved; auditing security plans of critical infrastructure operators; advising critical infrastructure operators, sharing information, disseminating alerts on security threats, and supporting CIP and resilience efforts; and organizing joint exercises to test procedures and strengthen relationships and habits of cooperation. (García Zaballos, 2016, p. 52)

Indeed, the effective management of cybersecurity measures is a highly complex task that requires a variety of resources and mechanisms. The prioritization of critical infrastructure protection implies commitments that states must be willing to make to protect their citizens and provide security. As stated in the 2008 Report on Critical Infrastructure Protection in Latin America and the Caribbean, CIPs require tools and regulatory frameworks to protect virtual information structures and physical infrastructures, which should be considered a high priority for the States:

Effective critical infrastructure protection must rely on public-private partnerships. Governments, critical infrastructure owners and operators, and ICT providers must partner across sectors and borders to better manage risk. The benefits of collective action in cybersecurity are clear. Information sharing is one example of the potential value of a collective response to cyber threats. When information about attackers and attack methods is shared, organizations are better prepared to thwart them. Therefore, governments should consider implementing frameworks and incentives that would encourage critical infrastructure organizations to engage in this activity. (OAS - Microsoft, 2018, p.52)

CONCLUSIONS

It is evident the little normative development contemplated for scenarios such as cyberwarfare. The world is changing, and states are safeguarding everything that is their property, while at the same time developing new technologies for new war scenarios. Although States have witnessed the effects of conventional weapons and methods of warfare, there is still no clear perception of the damage that new technologies can cause in terms of means and methods of warfare. The role of the States in giving rise to this law in the current technological era is of fundamental importance, however, everything lies in the unwavering will of the States to give way to the development of the Law. Its effectiveness lies in the "normative" force that has been given to it. Although it was initially established to determine whether civilians carrying weapons against an occupying force should be considered snipers and be punished with execution or should be considered legitimate combatants, it is its interpretation in the face of technological progress that

opens the possibility of its application until the International Community develops the law of war completely.

The interpretation of the Martens Clause could be taken by IHL as a mechanism that provides broad protection to the victims of cyberwar as an armed conflict since it would limit the means and methods of combat that could be used and would even provide protection to IICs as they are considered services that are linked to indispensable goods for survival within a State. In this way, the international community could use the interpretation of the clause in the event of events occurring in cyberspace.

The current foolishness on the part of some States to identify or include the Martens Clause as a source of international law is perceived and is a reality. However, this does not detract from the value and weight of those who advocate in favor of considering it as a tool to limit action in the face of evolving armed conflicts. The interpretation of the Martens Clause as part of the law of armed conflict allows the parties to a conflict to be protected by the rules of international humanitarian law in the face of the evident normative vacuum. Finally, cyberspace plays an important role, being configured as another scenario of confrontation, which is why States must adopt provisions that further restrict the use of means and methods of cybernetic nature in the development of regulations applicable to cyber warfare. Since there is no international regulation that specifically regulates cyber-attacks within an armed conflict, each of the States must give way to its development.

REFERENCES

Bericat, E. (1996). The information society: Technology, Culture, Society. *Revista Española de Investigaciones Sociológicas*, (76), pp. 99-121.

Cameron, L., Demeyere, B., Henckaerts, J. M., La Haye, E. & Niebergall-Lackner, H. (2015). The updated Commentary on the First Geneva Convention - a new tool for generating respect for international humanitarian law. *International Review of the Red Cross*, (97), pp. 1209-1226. DOI: https://doi.org/10.1017/S181638311600045X

Carlini, A. (2016). Cybersecurity Bulletin: a new challenge for the international community. *IEEE Bulletin,* (2), pp.950-966.

Drezner, D. (2007). *All politics is global: Explaining international regulatory regimes.* United States: Princeton University Press.

Droege, C. (2011). *No gaps in cyberspace*. Retrieved from: https://www.icrc.org/es/doc/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm

Eissa, S., Gastaldi, S., Poczynok, I. & Zacarías, M. (2012). *Cyberspace and its implications in national defense.* Approximations to the Argentine case. Retrieved from: https://core.ac.uk/download/pdf/296371994.pdf

European Program for the Protection of Critical Infrastructures. (2006). European Program for the Protection of Critical Infrastructures.

García Zaballos, A. (2016). *Best Practices for Critical Information Infrastructure Protection (CIIP)*. United States: A&S Information Specialists, LLC.

Hague Convention II. (1899). *Relative to the Laws and Customs of War on Land and Regulations annexed thereto*.

Harašta, J. (2018). Legally critical: Defining critical infrastructure in an interconnected world. *International Journal of Critical Infrastructure Protection*, (21), pp. 47-56. DOI: https://doi.org/10.1016/j.ijcip.2018.05.007

ICRC. (1977). *Commentary on the Additional Protocols to the Geneva Conventions*. United States: Kluwer Academic Publishers.

IDB, & OAS. (2020). *Cybersecurity. Risks, Advances, and the way forward in Latin America and the Caribbean*. Retrieved from: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

International Telecommunication Union (2008). ITU-T Recommendation X.1205

Kiggins, R. (2002). US Leadership in Cyberspace: Transnational Cyber Security and Global Governance. In J. Kremer & B. Müller (eds.), *Cyberspace and International Relations*, pp. 161-180. London: Springer.

Kittichaisaree, K. (2017). Cyber Warfare. K. Kittichaisare (eds.), *Public International Law of Cyberspace* pp. 335-356. United States: Springer International Publisher.

Kittichaisaree, K. (2017b). Regulation of Cyberspace and Human Rights. In C. Pompeu & G. Sartor (eds.), *Public International Law of Cyberspace. Law, Governance and Technology Series,* pp. 45-150. United States: Springer International Publisher.

Lopez, J., Setola, R. & Wolthusen, S. D. (2012). Overview of Critical Information Infrastructure Protection. In J. Lopez et al. (eds.), *Critical Information Infrastructure Protection*, pp. 1-14. Berlin: Springer-Verlag Berlin Heidelberg.

Luke, V. (2012). Computer Security and Public International Law in the 21st century: legal challenges facing the protection of computer infrastructures. *Public Law Review,* (77), pp. 405-424. DOI: https://doi.org/10.5354/RDPU.V0I77.30935

Meron, T. (2000). The Martens Clause, Principles of Humanity, and Dictates of Public Conscience. *American Journal of International Law*, 94 (1), pp. 78-89. DOI: https://doi.org/10.2307/2555232

Nickolov, E. (2005). Critical information infrastructure protection: analysis, evaluation, and expectations. *Information & Security. An International Journal*, (17), pp. 105-119.

OAS - Microsoft, O. of A. S. (2018). *Critical infrastructure protection in Latin America and the Caribbean 2018*. Retrieved from: https://www.oas.org/es/sms/cicte/cipreport.pdf

Polloni Contardo, M. (2018). International law as a regulatory framework for cyberwarfare. In M.Velásquez (ed), *La ciberguerra sus impactos y desafíos,* pp. 1219-145. Chile: Centro de Estudios Estratégicos CEEAG.

Pustogarov, V. (1996). Fyodor Fyodorovich Martens (1845-1909) - humanist of modern times. *International Review of the Red Cross*, 21 (135), pp. 324-339. DOI: https://doi.org/10.1017/s0250569x00021026

Radu, R. (2002). Power Technology and Powerful Technologies: Global Governmentality and Security in the Cyberspace. In J.-F. Kremer & B. Muller (eds.), *Cyberspace and International Relations*. London: Springer.

Reguera Sánchez, J. (2015). Legal aspects in cyberspace. Cyberwarfare and International Humanitarian Law. *Análisis GESI*, (7), pp. 1-30.

Salmon, E. (2012). *Introduction to International Humanitarian Law*. Lima: ICRC.

Ticehurst, R. (1997). The Martens Clause and the law of armed conflict. *International Review of the Red Cross*, 22 (140), pp. 131-141. DOI: https://doi.org/10.1017/s0250569x00021919

Tocino, I. M. (2018). The importance of the Martens Clause in regulating the use of drones during armed conflict. *Lessons and Essays,* (101), pp. 175-203.

Received: 15/06/2021

Approved: 21/07/2022

Carolina del Rocio Changoluisa Barahona: Independent legal researcher

Email: carito.delrocio@hotmail.com

City: Quito

Country: Ecuador

ORCID: https://orcid.org/0000-0003-3622-8376