PONTIFICAL CATHOLIC UNIVERSITY OF ECUADOR

FACULTY OF JURISPRUDENCE

A RESEARCH PAPER SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR A BACHELOR OF LAWS

APPLICATION OF THE MARTENS CLAUSE TO CYBER-WARFARE

Carolina del Rocio Changoluisa Barahona

Dissertation Advisor: Juan José Alencastro Moya, LL.M

Quito, 2.12, 2022

“Efforts will lie but will never be in vain.”

– Yuzuru Hanyu

To my parents, Rocio and Edgar

To my grandparents, Virginia and Carlos

To my brothers, Belén and Edgar

Acknowledgments

There are many to whom I owe gratitude in preparing this dissertation. First and foremost, my mom and dad, who have been my source of strength and wisdom, and for that, l am deeply grateful. My mom always supported my craziest ideas in my student life. To my father, who always motivated me to study other languages and encouraged me to give the best of myself in each task, and my grandfather Carlos who always believed in me. Even though he is not with me, I know he always takes care of me.

To my advisor, Dr. Juan José Alencastro Moya, who was an inspired professor, counsel, and motivator. Because without that, I won’t have discovered my passion for International Law and Humanitarian Law. His outstanding intellect inspired me to do my best for this work and for that l am very thankful. Also, I am particularly appreciative of his continued supervision and support in this work, a responsibility he was not obligated to retain.

To Professor Ivette Haboud, who helped me in the previous work for this research, her guidelines helped me redact this work. I am very grateful for her teachings, her understanding, and her passion in each one of the classes.

RESUMEN: La tecnología ha revolucionado y ampliado el escenario de la guerra. Se deja de lado aquello que acontece en la tierra para pasar a analizar los inminentes peligros que se pueden desencadenar en el ciberespacio. En efecto, la transformación de las operaciones militares convencionales a operaciones cibernéticas representen un gran peligro para los Estados. Sin embargo, los Estados no han fomentado, ni adoptado mecanismos que regulen el uso de las ciber operaciones en un eventual conflicto armado. Ante la falta de normativa expresa para regular la ciberguerra, la Cláusula de Martens se presenta como un mecanismo de interpretación ante problemas o situaciones que no pueden llegar a estar contempladas por las normas convencionales del Derecho Internacional Humanitario. La investigación pretende determinar el alcance de protección de la Cláusula de Martens hacia las infraestructuras críticas de la información en el contexto de una ciberguerra, considerando el poco desarrollo normativo vigente. Al respecto, se analizará de modo sistemático la Cláusula de Martens bajo las reglas de interpretación de los tratados internacionales establecidas en el Convenio de Viena de Derecho de los Tratados de 1969 y su interpretación dada por la jurisprudencia y los Estados. De esta manera, se demostrará el alcance normativo que tiene la Cláusula de Martens teniendo en cuenta el contexto histórico desde su promulgación en la Conferencia de la Haya de 1899.

KEY WORDS: *Cláusula de Martens, Derecho Internacional Humanitario, Cyberguerra, Cyberespacio.*

ABSTRACT: Technology has revolutionized and extended the scenery of war. It sets aside the things that happen on land to analyze the imminent hazards that may develop in cyberspace. The transformation of kinetic operations into cyber operations represents a significant danger to States. However, States have not fostered or adopted mechanisms that rule the use of cyber operations in an armed conflict. In the absence of norms to rule the cyberwarfare, the Martens Clause represents an interpretation mechanism against situations not covered or protected by International Humanitarian Law. This research pretends to determine the scope of protection of the Martens Clause to Critical Information Infrastructures in cyber warfare, considering the little normative development. Therefore, the Martens Clause will be analyzed under the rules for interpreting international treaties established in the Vienna Convention of 1969 and its interpretations given by jurisprudence and States. It will demonstrate the normative scope of the Martens Clause considering its historical context since its promulgation on the Hague Conference II in 1899.

KEW WORDS: *Martens Clause, International Humanitarian Law, Cyberwarfare, Cyberspace.*

Table of Contents

Introduction....5

I. Regulation of the armed conflicts....7

1.1. Cyberspace as a new scenery of war....7

1.1.1. Characteristics of Cyberspace....7

1.1.1.1. Military Cyber Domain and military cyber operations....11

II. Cyberwarfare: the protection of the Martens Clause....16

2.1. Cyberoperations: regulation under IHL....16

2.1.1. Cyber operations in and as international armed conflicts....23

2.1.2. Cyber operations as international armed conflicts and non-international armed conflicts 27

2.2. Martens Clause: scope of protection to Critical Information Infrastructure (CII)....29

2.2.1. History and evolution of the Martens Clause....30

2.2.2. Interpretations: restrictive, ample, moderate, and jurisprudential....33

2.2.3. Interpretation under the Vienna Convention....37

2.2.3.1. Literal Interpretation....38

2.2.3.2. Context....48

2.2.3.3. The object and purpose of the treaty....49

2.2.3.4. Rules of interpretation under article 31.1: subsequent agreement, subsequent practice, and relevant rules....50

2.3. The Critical Information Infrastructure (CII) and the Cyber-warfare....51

2.3.1. Protection to CII under the IHL....53

Conclusions....61

References....62

Appendices....68

Table of Figures

Figure 1 Military Cyber operations 15

Figure 2 Application of the Law of Armed Conflict Example 21

List of Tables

Table 1 Layers of Cyberspace 9

Application of the Martens Clause to cyber-warfare

"Mankind must put an end to war, or war will put an end to mankind"

-J. F Kennedy

Introduction

The history of humanity is marked by wars, battlefields, and anthropogenic disasters. In ancient times many thoughts about the war have been elaborated on. Some showed that finding peace was a sign of weakness or decadence and believed that the normal state between countries was war. Even more extremist beliefs refused the existence of war. Consequently, warfare was established as the beginning of international law. Ancient civilizations have known it as the law of war or better known as International Humanitarian Law (IHL), which purpose is to determine and "resolve the practical problems of armed conflict rather than the reasons for or legality of resorting to armed force" (Hongsheng, 2006, p.268).

China, Egypt, India, Greece, and Rome played an important role in constructing the law of war. In the past, countries already have been some prohibitions for war, such as do not use poisoned weapons, do not attack fleeing, or not poisoning the water. Many attempts to keep the peace, like The Hague Peace Conferences of 1899 and 1907, were probed. However, during World War II, States violated many laws of war. The answer to this behavior was to regulate new rules for conducting wartime. As a result, the States signed the four Geneva Conventions in 1949 and the two Additional Protocols of 1977. Over time many rules were incorporated into the construction of International Humanitarian Law. Still, with the advance of weapons, the arrival of gunpowder, firearms, and the era of technology, the atrocity of the war increased.

Nowadays, International Humanitarian Law does not have a definition of armed conflict because the fact of defining it could not bring the appropriate protection to the people. In armed conflicts, the law has protected the victims of war and their rights, no matter which side they belong to. The pretension is to provide all war victims minimum protection (Hongsheng, 2006). Still, nothing takes away the fact that war has always been a *shape-shifter* because it has transformed according to the political and social environment. The wars will not only develop on the land because technology changed the scenery of the wars, and the concept of cyberspace as new scenery of war was introduced in the law of war. As a result, in the last years, the methods of warfare have been changing until arriving the cyber-warfare.

Cyber warfare brings a new vision of war that requires an own study because the arrival of technology limited the application of International Humanitarian Law. Also, it is understood

as military activities developed in cyberspace conducted by a state against another to disrupt and destroy the computer and communication systems or data (Jordan, 2021a). The concern is how IHL could deal with the growing technology weapons and targets because every day, more human activities rely on a computer, and Information and communications technology (ICT) has a significant role in the military field of States.

This dissertation project will determine the scope of protection of the Martens Clause to the Critical Infrastructure Information (CII) in cyber-warfare, considering the little normative development. To argue this, the study (i) will identify how International Humanitarian Law regulates cyber operations as armed conflict; (ii) will examine the Critical Infrastructure Information (CII) vulnerability in cyber warfare.

The principal argument of this study is that the interpretation (with its doctrinaire, customary, and judicial elements) of the Marten Clause could delimit the normative framework of protection to CII in cyberwarfare cataloged previously as an armed conflict. In the first point, the cyberspace as new scenery of war and the progress of cyber operations in armed conflicts will be studied to recognize the elements that cyber warfare needs to be cataloged as an armed conflict. Moreover, the most dangerous cyberoperations that could be developed in a cyber warfare will be identified. In the second point, the cyberoperations under IHL will be studied to identify when it could be considered NIAC or IAC. Reviewing these topics will help focus on the debate on applying the Martens Clause in cyber-warfare the Martens Clause will be interpreted under article 31 of the Vienna Convention on the Law of Treaties and jurisprudence for understanding the purpose of the Clause given by the parties that signed that Hague Convention II to define its scope in cyber warfare. Also, the relationship between Critical Infrastructure Information (CII) and cyber warfare will be researched to comprehend its vulnerability against new methods and means of warfare.

The aim is to identify if there is protection for CII brought by the IHL or not. The methodology used in this dissertation will be deductive and analytic. Additionally, the documentary technique will collect and analyze data related to IHL, customary law, and Martens Clause. Finally, the hypothesis that this research involves and wants to test is if the missing normative to regulate cyber warfare makes that the scope of the Martens Clause brings protection to CII against cyber operations in the context of an armed conflict according to the parties that signed that Hague Convention II.

I. Regulation of the armed conflicts

1.1. Cyberspace as a new scenery of war

Trotsky's phrase was modified as a product of the implication of the high technology in war "You may not be interested in cyberwar, but cyberwar is interested in you"[1] (as cited in Yong-Soo & Aßmann, 2016, p.344). It makes clear the evolution of armed conflicts and the future sceneries of war. Also, research completed in 2014 by the U.S. Army[2] requested high-level advisers to describe the battlefield of 2050. The expert answers referred to:

> The presence of augmented and enhanced humans; ubiquitous robots operating in swarms and in teams with humans; automated decision-making and autonomous processes, whether for weapons or for the institutional systems used to command and control them; large-scale self-organization and collective decision-making by entities on the battlefield; modeling and simulation of opponent behavior; a highly contested information environment with spoofing, hacking, misinformation, and dense electronic warfare; laser and microwave weapons; and the targeting of specific individuals based upon their unique electronic and behavioral signatures. (Latiff, 2017, p.41)

Their answers do not look unreal because, nowadays, armed conflicts have been spread out in space and time. Even States have employed technology in the development of weapons like drones. Because of this, humankind has suffered some damaging attacks. Also, research answers mentioned that some "concepts like discrimination between combatants and noncombatants, weapon proportionality, and military necessity will take on new and as yet unknown meaning" (Latiff, 2017, p.48).

1.1.1. Characteristics of Cyberspace

By 1999 the Department for Disarmament Affairs (DDA) and United Nations Institute for Disarmament Research (UNIDIR), in a private discussion meeting, already talked about the "rapid technological and commercial developments in information and communications technology (ICT)[3] that have ushered in an "Information Age" (or a "Networking Age" which was linked to the Revolution in Military Affairs (RMA)[4].

The National Security Council of the U.S (2008), in a classified document of Cybersecurity Policy, defined cyberspace as "the interdependent network of information technology infrastructures and includes the Internet, telecommunications networks, computer

[1] The original statement was made by Leon Trotsky, the builder and the first commander of the Red Army. It was, "You may not be interested in war, but war is interested in you."
[2] See more on https://api.army.mil/e2/c/downloads/360952.pdf
[3] It refers to the technologies that simplify obtaining, storing, exchanging, and processing data and information. This includes the internet, wireless networks, and software applications that permit the interaction in the digital world.
[4] It refers to scaling conventional conflict by using new military technologies.

systems, and embedded processors and controllers in critical industries" (p.3). It is also known as an entirely non-legal domain which occupies the "novel fifth space of warfare" (Shreier, 2017, p.10). According to Melzer (2015), cyberspace is "a globally interconnected network of digital information and communications infrastructure, including the Internet, telecommunications networks, computer systems, and the information resident therein" (as cited in Kittichaisaree, 2017, p.2). In addition, the Tallinn *Manual 2.0* (2017) defines cyberspace as "the environment formed by physical and non-physical components to store, modify, and exchange data using computer networks" (p.564). Specifically, its anarchic character of being an uncertain "world" has made that the U.N General Assembly and States take its regulation as a priority.

The International Telecommunication Union (ITU) (2022) reported that "by the end of 2021, 4.9 billion people were online, some 63 percent of the world population" (p.21). As a result, cyberspace has evolved into a diary tool for humankind because it provides many services such as communication, shopping, business, government, security, and others that depend on the Internet.

In fact, cyberspace is composed principally of the Internet. Still, also it includes all "networks and devices connected by wired connections, wireless connections and those that appear to be not connected at all" (NATO, AJP-3.20, 2020, p.1). The constant flux of cyberspace suggests that it could be used by anyone for any purpose. That is why the reliance on digital space is increasingly notable not only for civil society services but also for military forces, and cyberspace was recognized by the military as the fifth domain of warfare where they need training, equipment, and organizing troops to operate in this cyber domain (Chapple & Seidl, 2022). Consequently, it needs to be regulated by IHL.

Even the U.N. Secretary-General emphasized that "information and communications technologies (ICTs) continue to rapidly transform societies, offering numerous opportunities while also posing significant risks" (United Nations, 2021, RES A/76/135, p.4). The significant risk is cyber warfare because states are "developing national strategies and engaging in cyber-attacks with alarming frequency," and there is a "stunning lack of international dialogue and activity with respect to the containment of cyberwar" (Schreier, 2015, p.7). International law has not yet wholly regulated cyber activities (Shany & Schmitt, 2020).

NATO in *AJP-3.20 Allied Joint Doctrine for Cyberspace Operations*[5] described cyberspace in three layers: the physical, logical, and cyber persona.

Physical	• It is composed of (a) tangible components such as computers, servers, routers, hubs, switches, wiring, hubs, and other machinery for data storage, data processing, and data transmission, (b) integrated information and communications technology components of other equipment like weapons or critical infrastructure (NATO, 2020). • It does not have boundaries, but its components belong to a geographical location (NATO, 2020). Physical components could be owned by private or public entities. • It consists "of the information technology devices and infrastructure in the physical domains that provide storage, transport, and processing of information within cyberspace, to include data repositories and the connections that transfer data between network components" (Department of the Army United States of America, 2021, FM 3-12, p.6).
Logical	• It is composed of elements expressed in code or data like applications, software, or other data components. In this way, the data circulates through the wired networks (NATO, 2020). • The geographical position of the hardware matters for law. Also, it is dependent on the physical layer otherwise it does not work (NATO, 2020).
Cyber persona	• Through the "abstracting data from the logical network layer using the rules that apply in the logical network layer to develop descriptions of digital representations of an actor or entity identity in cyberspace, known as a cyber-persona" (Department of the Army United States of America, 2021, FM 3-12, p.7). This layer functions by linking logical and physical layers. As a result, the cyber-persona will communicate (NATO, 2020).

Table 1
Layers of Cyberspace
Source: AJP-3.20 Allied Joint Doctrine for Cyberspace Operations
Author: Carolina Changoluisa, 2022.

Cyber-persona comprises IT[6] user accounts, which are automated or belong to humans. In this way, one individual (person or entity) could create and keep various cyber-personas (individuals can create different user accounts through multiple identifiers in cyberspace, such as email addresses, forums, chats, social networks, and others). However, one cyber-persona (user account) could have many users. For example, the entire staff members of an organization might use the same e-mail address (United States Army War College, 2021).

[5] It is the NATO doctrine to plan, execute and assess cyberspace operations (CO) in the context of Allied joint operations. Its purpose is to guide armed forces in planning and managing COs appropriately.
[6] It means information technology. A user account is an identity made by a person in a computing system.

According to Porche (2013, as cited in Porche III, 2020), the characteristics which made cyberspace "unique" are its (a) speed; (b) boundlessness; (c) democracy; (d) anonymity; (e) growth; and (d) dynamism. Cyberspace connects people globally, and the operations developed in this "scenery" are not constrained by geographical boundaries because the Internet goes through them. However, Even Heinegg (2013) affirmed that cyberspace is a *res communis omnium*[7] and:

> While, in view of the genuine architecture of cyberspace, it may be difficult to exercise sovereignty, the technological and technical problems involved do not prevent a State from exercising its jurisdiction over the cyber infrastructure located in areas in its sovereign territory. (p.126)

Furthermore, Neuman (2021) identified and described other critical characteristics of cyberspace (a) intangibility, (b) limited supervision and enforcement capabilities, and (c) a decentralized model of governance. The first refers to the "ubiquitous interconnectivity"[8] (Higson, 2016, as cited in Neuman, 2021, p.775). The activities in the cyber domain lacked physical manifestation because they developed through computers, servers, cables, or transmitters. The second indicates that the control of the cyber domain is not only exercised by States. The "routing of data within or between networks is not usually controlled by States and often does not occur in one particular central geographical location" (p.775). International legal subjects are the legal subjects of cyberspace. However, international public organizations, private organizations, associations, or corporations could make cyberspace activities (Korhonen & Markovich, 2015). The third showed that the elaboration of protocols and norms was decentralized with diverse contributors.

U.S Army War College (2021) added as unique cyberspace capabilities and characteristics the (a) reverse engineered, which allows cyberspace activities could be maintained, analyzed, and recorded with the aspiration to use them against adversaries or friendly nations; (b) no single national/ international ownership which is a problem because the cyberspace is not under the regulation of any nation or entity; (c) lack of cooperation and collaboration resulting in a problematic response about the operations made in the cyber domain because actors deny the cyber-attacks; (d) low-cost result in a fight without costly armament because defensive tools for network attacks can be found on the Internet without cost; (e) volatileness because the attack could be useless and change unexpectedly if the adversary fixes its vulnerabilities.

[7] It means common property.
[8] It seems to be everywhere.

The prosperity of a cyberspace attack depends on identifying the adversary's vulnerabilities and creating an attack based on them and its (f) unintentional cascading effects, considering that cyber operations develop in computer labs. Still, there is no certainty about how a process will behave or where it causes effects, given the great extent of cyberspace.

1.1.1.1.Military Cyber Domain and military cyber operations

Mainly, this investigation will focus on the cyber domain as the fifth warfare domain, where cyber operations used by military forces should be regulated by IHL. Military forces recognized that cyberspace has the same importance as other war sceneries, namely air, land, sea, and space. Intelligence, information, crime, and military operations are the sets of cyberspace activities that belong to the military. However, military operations stand out, but " there are aspects of intelligence, information, and criminal activities in cyberspace that do involve the military" (Crowther, 2018, p.88). The cyberspace activities in these sets could be (a) conventional, (b) moiety cyber and conventional, and (c) wholly cyber operations. See Appendix A for review a historical glimpse of cyberoperation cases[9].

Cyberoperations (COs) are "operations against or via a computer or a computer system through a data stream" (Backstrom & Henderson, 2012, p.503) and are often realized in the logical layer. Still, they also use elements from the other layers. In addition, the effects of COs could (a) affect all the layers, (b) affect outside cyberspace and affect physical entities, and (c) affect the human sense or decisionism. However, the activities outside cyberspace that affect cyberspace are not considered COs. Correspondingly, based on the portion of cyberspace, the cyber operations were divided into two categories, and the authorities, approval levels, and coordination considerations are linked with each type as follows. See Figure 1

- **Offensive Cyberspace Operations (OCO)** are "actions taken to deny, exploit, corrupt, or destroy an adversary's information or information functions" (Chapple & Seidl, 2022, p.64).

- **Defensive Cyberspace Operations (DCO)** are "actions taken to protect your own information and information systems from an adversary's attempt to deny, exploit, corrupt, or destroy them" (Chapple & Seidl, 2022, p.64).
  a network or part of cyberspace.

DCO has subdivisions: defensive cyberspace operations-internal defense measures (DCO-IDM) and cyberspace operations-response actions (DCO-RA). DCO-IDM purpose is to recognize and localize the cyber threats inside friendly networks and then apply defensive measures to eliminate or neutralize them. On the other hand, DCO-RA generates physical damage to the enemy systems because the operations are taken outside to defend

[9] See an explication of each cyberoperation in https://web.mit.edu/smadnick/www/wp/2017-10.pdf

The OCO and DCO are the most common in cyberspace, but there are operations proper by the USA Army and consequently made by the Department of Defense information network called:

- **Defense Information Network Operations (DODIN Ops)** are operations focused on "collecting, processing, storing, disseminating, and managing information on demand to warfighters, policymakers, and support personnel, whether interconnected or stand-alone" (Department of the Army United States of America, FM 3-12, 2021, p.2-4). DODIN Ops allows commanders or the army to share and manage information through information technology systems with reliable security end-to-end communication. Also, it tries to maintain the confidentiality of the information network using security barriers, such as data encryption, physical and technical barriers, security training, network monitoring, and others.

Indeed, military forces could use offensive operations, which can be destructive or nondestructive, to (a) achieve their objectives which could be military, political, or economic, and (b) prevent adversaries' attacks. Porche III (2020) remarked that it produces "some degree of trespassing occurs because their effects trespass boundaries of domestic or international law, such as personal property or international borders" (p.19). On the other hand, defensive actions, which can be passive or active, mitigate or avert offensive actions (Porche III, 2020).

Cyber operations are, by nature, offensive, defensive, or both. Also, it could have actions to (a) attack, (b) spy, (c) defend, (d) protect, (e) collect intelligence, surveillance, and reconnaissance (ISR)[10], (f) prepare operational preparation of the environment (OPE), and (g) build provision (Porche III, 2020). Specifically, of all actions that have cyber operations, only four are considered foremost:

1. **Shaping cognition** induces people's way of thinking through information. Someone who is connected to the Internet could have the power to shape the thoughts of others (Crowther, 2018).

2. **Cyber surveillance and reconnaissance (CSR)** gather data. The data that belong to (a) people from other countries or (b) nationals was gathered by States (Crowther, 2018).

3. **Operational preparation of the environment (OPE):** focus on "the conduct of activities in likely or potential operational areas to set conditions for mission execution" (DOD Dictionary of Military and Associated Terms, 2021, p.161). A "back door" is installed through OPE "in targeted computer systems so that they can return at a later time to execute an attack or devising specially designed software that will allow them to achieve an effect" (Crowther, 2018, p.90).

[10] The mission of ISR is "gather information regarding the enemy by observing their behavior and tracking movement" (U.S AIR National Guard, 2022). ISR is "an integrated operations and intelligence activity that synchronizes and integrates the planning and operation of sensors, assets, and processing, exploitation, and dissemination systems in direct support of current and future operations" (Dictionary of Military and Associated Terms, 2021).

4. **Cyberspace attacks** are actions made in cyberspace that create degradation, disruption, or destruction in cyberspace; these attacks are divided into (a) syntactic and (b) semantic. Syntactic operations involve the actual coding used in a piece of cyber programming (the syntax of the coding), and semantic operations seek to shape thoughts using language or semantics. To illustrate, the process could start when a semantic operation asks the target to "click on a link" and later when the link is activated, the attack shift to a syntactic attack by which the code invade the target's system and modify the target platform code (Crowther, 2018). Cyberattacks especially have two effects (a) manipulation and (b) denial. Manipulation focuses on reining or changing "adversary information, information systems or networks in a manner that supports the commander's objectives" (Crowther, 2018, p.90). Alternatively, denial degrades, disrupts, or destroys adversary information systems and limits the target's capacity or access.

Moreover, in cyberspace, armed forces could deal with threats known as *cyber threats or threat actors*. These actors can harm through the COs the (a) armed forces which belong to a State or (b) the national interest of a State, and they are divided into (a) Nation-State Threats or State actors, (b) Non-state actors; (c) Individual actors or Small Group Threat; and (d) Accidents or Natural Hazards.

First, State actors can conduct directly or by third parties (front companies[11] or hackers) defensive and offensive cyber operations against adversaries, resulting in a contest under the level of an armed conflict or open hostilities. Businesses, government departments, and armed forces are the COs targets developed by State actors. The capacity for accessing resources and personnel in cyberspace to attack other states has made this threat one of the riskiest (NATO, 2020). Secondly, Non-state actors consummate COs of their own will, but they could also perform them by order of a state (which does not have the tools to develop COs). The fact that states act through non-state actors could deny the state's demands. When is conduct made by a non-state actor attributable to a state? Only "if the state factually exercises effective control over that specific conduct of the nonstate actor" (NATO, 2020, p.6).

Thirdly, individual actors or small groups could attack a state's cyberspace exploiting their vulnerabilities to obtain access to their data and achieve the COs objectives. Additionally, individual actors might be criminals or insiders. Taking advantage of anonymity, cybercriminals might impinge on military COs. On the other hand, insiders[12] belong to a group

[11] In COs, the front organization acts as the face of another organization (state) or group with the purpose of concealing the activities ordered by the group or State. Definition adapted to the context of cyberwar.

[12] An example is the cause of a former U.S. Nuclear Regulatory Commission employee who pleaded guilty to a spear-phishing cyber-attack on the Department of Energy to damage a computer with sensitive nuclear weapon

or organization and use the knowledge of their work to help the enemy in their operations for disarming military systems or overpassing cyber security barriers. Finally, hazards are commonly caused by natural disasters or industrial accidents, which could produce illness, damage to the property, injuries or death to the personnel (military), and the disruption of the COs operations.

Even the USA Army recognized cyberspace threats (a) transnational threats, composed of authoritarian and illiberal regimes, or (b) state-sponsored hackers. And some countries like China, Russia, Iran, and North Korea have been added to the list. (United States Army War College, 2021). Moore (2022) remarked that:

> At the same time, traditionally potent actors such as the United States, Russia, and the People's Republic of China are all global leaders in the maturity of their offensive cyber doctrines. Instead of decreasing asymmetries, powerful actors can use offensive network capabilities to increase them. Weaker parties to the conflict also have less resource to spend on network defense and secure development of military resources. That means they must rely on commercially available solutions, imported military equipment, and ageing hardware. (p.172)

The threats are considered (a) enemies, (b) adversaries, (c) peer threats, and (d) hybrid threats. An enemy is regarded as a combatant and is treated under the law of war *(jus ad Bellum and jus in Bello).* Also, it is a hostile part, and the use of force is authorized against them. Alternatively, adversaries are described as a negative part of a friendly party (of a state), and the use of force could be conceived or envisaged. Indeed, in cyberspace, peer threats, enemies, or adversaries could have the same military capacity to make COs as the state or armed forces fighting against them. The parts define the type of armed conflict**.** This subject is going to be explained in the following pages concerning the Martens Clause.

A hybrid threat could be composed of regular forces, irregular forces, or criminals. The COs they do are diverse and complicated to recognize and associate responsibility with because the hostility comes from many actors situated in different geographical territories. The threats are characterized by its abroad, embedded, and diversity. Initially, "the nature of the threat in cyberspace is as broad as cyberspace itself" (Shreier, 2017, p.32). As a result, threats could affect critical national infrastructures or access to data. Diversity refers to the potentially hostile actors who will be well-organized gangs, front organizations, hackers, or criminals sponsored by a state. For that reason, "each poses a distinct threat, requiring a differentiated response" (Shreier, 2017, p.33).

---

information. Recovered from https://www.justice.gov/opa/pr/former-us-nuclear-regulatory-commission-employee-pleads-guilty-attempted-spear-phishing-cyber

Even, “various actors may cooperate, whether it be State alliances, States supporting groups, or criminal groups selling cyber capabilities to other actors” (International Committee of the Red Cross ICRC, 2018, p.14). Additionally, “the private sector was increasingly interested in “cyber capability development”, as is already the case with the development of traditional means and methods of warfare” (International Committee of the Red Cross ICRC, 2018, p.14). The responses are known as tactical-level actions determined by the variety of effects they generate. The cyberspace actions are (a) security, (b) defense, (c) exploitation, and (d) attack. See Figure 1

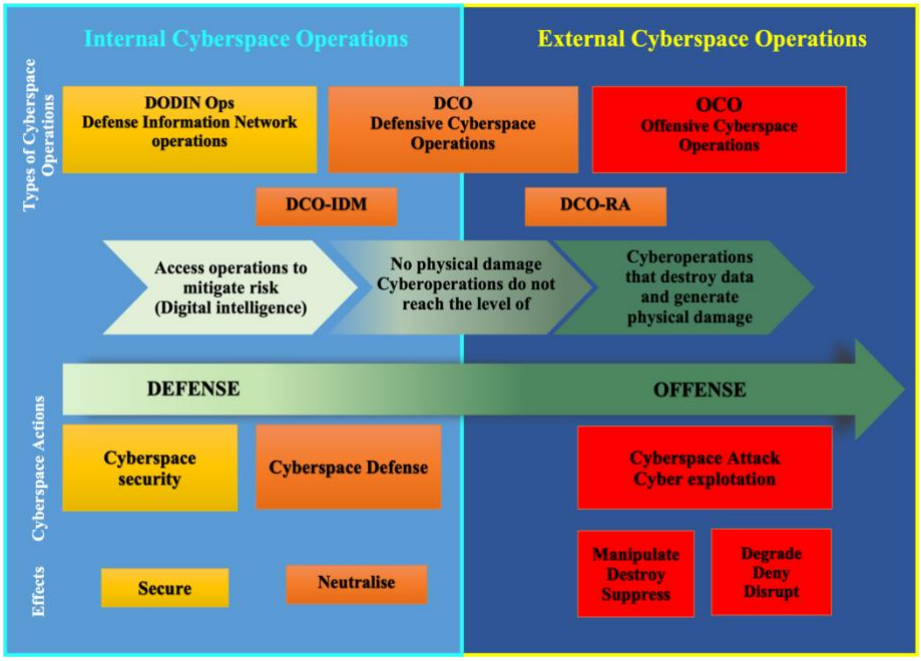


Figure 1
Military Cyberoperations
Source: Porche III & Department of the Army United States of America, FM 3-12, 2021
Author: Carolina Changoluisa, 2022.

All the actions for (a)protecting illegal access or damage to computers and (b) reducing the vulnerabilities are encompassed in cyberspace security. By contrast, cyberspace defense focuses on actions for protecting cyberspace from specific threats and trying to mitigate them. On the other hand, cyberspace exploitation actions help armed forces to qualify and prepare for future military operations. The goal is to map cyberspace to discover vulnerabilities in adversaries’ networks and develop COs based on that information. Cyberspace attacks generate degradation, destruction, or disruption in cyberspace and physical domains. How do armed forces recognize an efficacious cyberattack? It will be recognized if it complies with the requirements such as:

a. The ability to identify a vulnerability;
b. The ability to get and maintain access to a target through a vulnerability;
c. The ability to take advantage of that access by delivering and executing a payload.(Porche III, 2020, p.35)

Subsequently, COs cause effects not only in cyberspace but the conduction of COs made in the logical layer make the effects predominate there. Even cascading or collateral effects might damage military or civil critical infrastructure systems. Prominent among them are the effects of securing, isolating, containing, neutralizing, degrading, disrupting, and destroying (NATO, 2020). Accordingly, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security mentioned that "States should also take appropriate measures to protect their critical infrastructure from ICT threats" and recommended that States do not "conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure" (The United Nations, 2015, RES A/70/174, p.2).

Also, regarding the effects of COs, the ICRC "is particularly concerned about the potential human cost of cyber operations on critical civilian infrastructure, including health infrastructure" (2020, p.484). In other words, military COs might carry out a war. For that reason, it is necessary to keep in mind that "the goal of the conduct of war, in general, is not just to destroy or disable physical infrastructures and forces, but to achieve psychological effects, such as compelling an enemy to do one's will" (Clausewitz, 1982, as cited in Schulze, 2020, p.184). So, the best way to limit the effects of war is by asserting the IHL to regulate it.

II. Cyberwarfare: the protection of the Martens Clause

2.1.Cyberoperations: regulation under IHL

How does IHL regulate COs during armed conflicts? Does the IHL rule a cyber-attack? Which COs could be considered an "attack" as defined in IHL? First, cyber warfare (CW) has multiple definitions, one of which is "actions taken to adversely affect information and information systems while defending one's own information and information systems" (Schmitt, 2002, as cited in Granova & Slaviero, 2017, p.1086). In light of the preceding, for this research, CW can be understood as (a) an action that "includes a wide range of activities that use information systems as weapons against an opposing force" (Chapple & Seidl, 2022, p.41) which has as objective disrupt, degradant or destruct computing devices, its programming or data (Jordan, 2021b); and (b) a means and method of war "that consist of cyber operations

amounting to or conducted in the context of, an armed conflict, within the meaning of IHL" (International Committee of the Red Cross ICRC, 2013, p.1).

The ICRC report of the 32nd International Conference of the Red Cross and Red Crescent exposed that until that date, cyber warfare "has fortunately not led to dramatic humanitarian consequences" (International Committee of the Red Cross ICRC, 2015, p.39). However, during the last years, society has witnessed and has been affected by the growing use of cyber-attacks because of the advance in technology. Consequently, the surveillance and appraisement of cyber operations come from the accelerated evolution of cyberspace and cyber operations and the potential human cost of cyber operations.

Consequently, its application is based on the nature, effects, and circumstances of cyber operations (Gisel, Rodenha ̈user & Do ̈rmannet, 2020, p.289). The effects of COs will be explained in the second point of this research about CII. To illustrate, among the most recent cyber-attacks during 2022 were (a) Costa Rican ransomware[13] attack outside an armed conflict and (b) Russian cyber operations against Ukraine in the war framework. Under this rationale, the primary question for applying the IHL in cyber operations focuses on the following: Could international humanitarian law be applied to cyber operations? Applying IHL to cyber operations during armed conflicts is still object to debate for States. However, "through multilateral processes, States have achieved agreement on some aspects of the legal and normative framework regulating cyber operations" (Gisel, Rodenha ̈user & Do ̈rmannet, 2020, p.289).

Lin (2012) asserted that the Law of Armed Conflicts (LOAC) or IHL and the laws that regulate the use of force in international relations were created initially to cope with kinetic hostilities[14]. Still, they could be applied to cyber conflict. Among the things that LOAC regulates are (a) the protection of war victims and the conduct of hostilities in IAC and NIAC; (b) the belligerent occupation, where IHL should be applied in all circumstances no matter if the armed conflict has a harsh nature (Melzer, 2020); and (c) the relations between states in an armed conflict which may be neutral, belligerent or nonbelligerent are mainly important (U.S Department of Defence, 2015, as cited in Porche III, 2020).

[13] Last April Costa Rica was the target of a ransomware attack made the Conti group. Also, the attacks interrupted the government services. And the Conti group demanded a 20 million ransom for the government to recover the data. More information in: https://www.nbcnews.com/news/latino/costa-rica-assault-troubling-test-case-ransomware-attacks-rcna34083

[14] It is the traditional form of war which was "conducted through the application of physical force to disrupt, degrade, or destroy physical assets" (Dykstra, Inglis & Walcott, 2020, p.116). Recovered from: https://ndupress.ndu.edu/JFQ/Joint-Force-Quarterly-99.aspx

Furthermore, the LOAC is attached to the reason when states can use force (*jus ad bellum*) and minimize human suffering when a war is irresistible *(jus in bello)* (Greenberg, 1997, as cited in Porche III, 2020). However, the *jus in bello* differs from *jus ad bellum.* Consequently, Roscini (2014) considered that the resort of force must comply with the *jus ad bellum* provisions of the UN Charter and customary law, but also with *jus in bello.* Also, he mentioned that "breach of or compliance with one does not justify violations of the other" (Roscini, 2014, p.118).

The application of IHL does not rely on the qualification of the situation under the jus ad bellum. Even the resort to armed force " that is unlawful from the perspective of jus ad bellum is subject to the law of armed conflict" (Tallinn Manual 2.0, 2017, p.377). About the *jus ad bellum,* the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security confirmed and emphasized the application of international law and mainly the United Nations Charter for maintaining "peace and stability and promoting an open, secure, peaceful and accessible ICT environment" (The United Nations, 2013, RES A/68/98, p.2). Alternatively, about the *jus in bello,* they recognized the legal principles of humanity, necessity, proportionality, and distinction in using ICTs by States (The United Nations, 2015, RES A/70/174, p.13).

As a result, the ICRC saw this fact as satisfying in the 32nd International Conference of the Red Cross and Red Crescent report made in 2015. IHL does not define the term cyber operations, cyber warfare, or cyber war. Accordingly, ICRC *cyber operations during armed conflict* refer to "operations against a computer system or network, or another connected device, through a data stream, when used as means or method of warfare in the context of an armed conflict" (Gisel et al., 2020, p.297). Despite the debate about if the IHL applies to cyber operations during armed conflicts, in the ICRC´s view is undisputed that COs or cyber warfare are governed by IHL same as "any weapon, means or method of warfare used by belligerent in a conflict" (Gisel et al., 2020, p.298). It includes weapons, means, and methods of cyber warfare founded and linked to cyber technology. Even the jurisprudence of the ICJ, the IHL treaties, and many States and international organizations have endorsed this view.

Already in 2011, the ICRC settled that "the employment of cyber capabilities in armed conflict must comply with all the principles and rules of IHL, as is the case with any other weapon, means or method of warfare, new or old" (International Committee of the Red Cross [ICRC], 2015, p.40). In addition, customary IHL rules apply to all means and methods in a

war-fighting[15] domain which will be the used case as described in the Advisory Opinion on the legality of the threat or use of weapons by the ICJ mentioned that despite that nuclear weapons were invented after the IHL rules applicable in armed conflict and

> [..]it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and applies to al1 forms of warfare and to al1 kinds of weapons, those of the past, those of the present and those of the future.(International Court of Justice [ICJ], Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, par. 86)

Consequently, States and international organizations recognize the application of IHL to cyber operations during armed conflicts. Organizations like the European Union (EU) in 2013 recognized that the IHL "provide a legal framework applicable in cyberspace" (European Union [EU], 2013, 11357/13, p.4) as well as international law and some conventions. Also, NATO mentioned that their policy "recognizes that international law, including international humanitarian law and the UN Charter, applies in cyberspace" (North Atlantic Treaty Organization [NATO], Wales Summit Declaration, 2014, pa.72).

So, when States adopt IHL treaties, they "included rules that anticipate the development of new means and methods of warfare in IHL treaties, presuming that IHL will apply to them" (International Committee of the Red Cross ICRC, 2020, p.485). Moreover, articles 49(3) and 36 of the Additional Protocol mention that the Protocol's rules must be applied in any operation that could affect the civilians on the land. So, "there is little doubt that cyber warfare will be waged at least partly from infrastructure located on land against targets on land and that it risks affecting civilians on land" (International Committee of the Red Cross [ICRC], 2015, p.40). Subsequently, Additional Protocol I is going to rule cyber operations too. The ICRC, in the background document prepared by Laurent Gisel, senior legal adviser, and Lukasz Olejnik, scientific adviser on cyber, for the expert meeting about the potential human cost of cyber operations developed in November 2018, mentioned:

> After the UN Charter, the body of law most relevant with regard to the limits imposed upon the use of cyber military operations is IHL (also known as the law of armed conflict, LOAC). IHL seeks to limit the effects of armed conflict, protects people, such as civilians, who are not or are no longer participating in hostilities, and restricts the choice of means and methods of warfare. (International Committee of the Red Cross [ICRC], 2018, p.68)

Still, it is essential to notice that the application of IHL does not mean a militarization of cyberspace or cyber warfare. The applicable law for a resort to force by States "always

[15] The war domains are the air, land, sea, the outer space, and cyber domain.

remains governed by the UN Charter and customary international law, in particular the prohibition against the use of force" (Gisel et al., 2020, p.301). In addition, the UN Charter requirements for a resort to force, whether lawful or not, are independent of establishing of IHL to limit the conduct of hostilities. The purpose of applying IHL, independently and in additionally to the UN Charter, "is that any State that chooses to develop or use cyber military capabilities for either defensive or offensive purposes must ensure that these capabilities do not violate IHL" (International Committee of the Red Cross [ICRC], 2018, p.69).

Even the States could "decide to impose additional limits to those found in existing law and to develop complementary rules, in particular, to strengthen the protection of civilians and civilian infrastructure against the effects of cyber operations" (International Committee of the Red Cross ICRC, 2020, p.485). Moreover, in cases not encompassed by the IHL, "civilians and combatants remain protected by the so-called Martens Clause" (International Committee of the Red Cross ICRC, 2020, p.485). It implies protection under (a) the principles of international law derived from established custom, (b) principles of humanity; and the (c) dictates of public conscience. This topic will be reviewed in point two concerning the Martens Clause and its scope of protection for CII.

Additionally, the Tallinn Manuals supported the consensus about applying IHL in cyberspace. Consequently, the Tallinn Manual 2.0[16] (2017) in Rule 80 mentioned that "the law of armed conflict applies to cyber operations undertaken in the context of an armed conflict" (p.375). So, the armed conflict could be international or non-international. Also, it remarks that:

- The main condition for applying IHL to cyber operations is an armed conflict.
- The term cyber operations involve but is not only restricted to cyber-attacks.
- The IHL does not apply to cyber operations made in a situation that did not rise to the level of armed conflict[17].
- The arduous duty of identifying a cyber operation, its creator, its object of attack, or its effects. This is not a justification for not applying the IHL.

[16] The Manual was prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence. In 2013, the first version that encompasses the jus ad bellum and jus in bello was released. Moreover, it emphasizes cyber-to-cyber operations, *sensu stricto.* On the other hand, Tallin Manual 2.0, released in 2017, analyze some commentaries from the original Tallinn Manual about the use of force by States and how States should conduct their military operation during an armed conflict and its protection for persons, objects, and activities. Also, it focuses on some aspects of public international law that rule cyber operations during peacetime.

[17] That was the case of Estonia in 2007. See Appendix A and page 14 and 68 of https://web.mit.edu/smadnick/www/wp/2017-10.pdf

The Group of Experts who worked on the Tallinn Manual embraced the phrase *in the context of armed conflict* for referring to a "nexus between cyber activity in question and the conflict for the law of armed conflict to apply to that activity" (2017, p.376). Conversely, the experts had discrepant opinions about the nature of that nexus. In NIAC, the phrase *in the context of* is unclear because a "State retains certain law enforcement obligations and rights with respect to its territory in which the hostilities are taking place, notwithstanding the armed conflict" (p.377). In NIAC, if there is not a nexus with the armed conflict, the State must apply domestic and human rights law. The law of armed conflicts will not apply (Tallinn Manual 2.0, 2017, p.377).

There are some perspectives about the application of the law of armed conflict to cyber activities, such (a) IHL ruled "any cyber activity conducted by a party to an armed conflict against its opponent" (p.376); and (b) the cyber activity should have been "undertaken in furtherance of the hostilities that is, in order to contribute to the originator's military effort" (2017, p.376). To illustrate, Manual 2.0 (2017) propose as an example a cyber operation "conducted by State A's Ministry of Trade against a private corporation in enemy State B in order to acquire commercial secrets during an armed conflict" (p.376). See Figure 2.

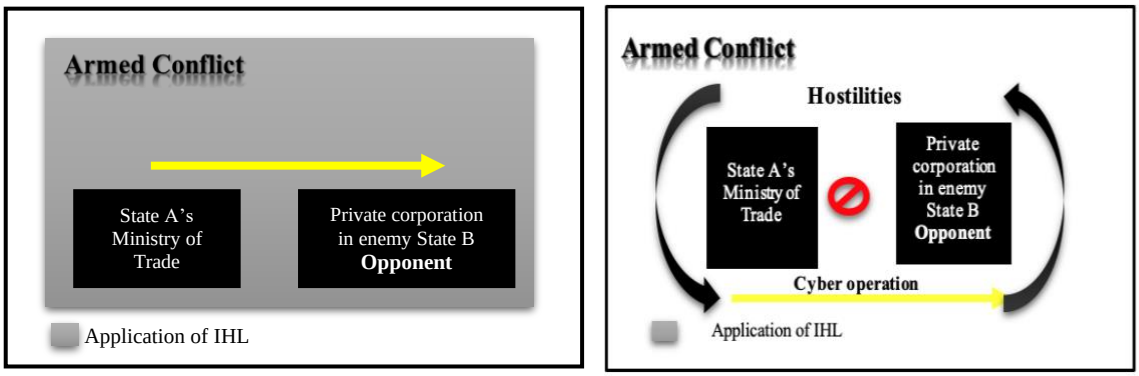


Figure 2
Application of the Law of armed conflicts: perspective A and B
Source: Tallinn Manual 2,0 (2017).
Author: Carolina Changoluisa, 2022.

Following perspective (a), the IHL should be applied to the cyber operation because it was conducted by a party to an armed conflict against its opponent. This perspective does not focus on the nexus between the conflict and the cyber activity and does not consider if the COs were realized for a military effort. Instead, point of view (b) contemplates the existence of a nexus between cyber operations and hostilities. If it is insufficient, the IHL will not t regulate the COs. In the example, the cyber operation's purpose is to acquire commercial secrets, so it will be debatable whether it could be related to the conflict. Also, IHL does not "embrace activities of private individuals or entities that are unrelated to the armed conflict" (Tallinn Manual 2.0, 2017, p.377).

Furthermore, the Manual commented that "armed conflict refers to a situation involving hostilities, including those conducted using cyber means" (p.375). So, the primary condition for applying the IHL to cyber operations is the existence of an armed conflict. However, the hostilities have a different threat for the IHL according to the type of conflict, established in Rule 82. Therefore, "the precise aspects of the law of armed conflict that apply depend on whether the conflict is international or non-international in nature" (Tallinn Manual 2.0, 2017, p.376). Moreover, if a rule of IHL does not regulate cyber activities, the Martens Clause must be applied in the activities that represent a legal vacuum (Tallinn Manual 2.0, 2017).

Given the above, the observations of the Tallinn Manual and Manual 2.0 could be summed up into six considerations. See Appendix B

It is essential to consider that Tallinn Manuals are not treaties. They are only referencing rules to apply in the conduction of cyber operations. As can be seen, IHL is the foremost framework that established restrictions or limitations for using COs during armed conflicts and protecting civilians against potential damage. Furthermore, its application is not a preventer for the State's labor about creating and developing international law that helps interpret existing rules (Gisel et al., 2020).

The second question for comprehending the applicability of IHL to COs is to understand when it crosses the threshold under IHL and the UN Charter. The nature of COs does not dismiss the bloodshed. Although the main objective of COs is to disrupt critical infrastructure, some COs could injure people directly or indirectly. In this way, some authors mentioned that COs need to trespass the threshold of (a) widespread scale and (b) death or injury of human beings as the intended effect of COs to be regulated by the law of armed conflicts (Jordan, 2021b). Consequently, cyber-attacks in cyberspace could be regulated under the *jus ad bellum* when a state justified it as self-defense. If cyber warfare has begun, the COs should be held under the *jus in bello* or IHL (Ashraf, 2021).

As given above, the application of IHL has an independent character of the use of force under the UN charter. So, when does IHL govern cyber operations?

> When cyber operations are conducted in the context of – and have a nexus to – an existing international or non-international armed conflict carried out through kinetic means, relevant IHL rules apply to, and regulate the conduct of, all parties to the conflict. (International Committee of the Red Cross, 2016, as cited in Gisel et al., 2020, p.303).

As shown in the attached text, there are two prevailing conditions for governing COs by IHL such as (a) the COs should be conducted in the context of an international armed

conflict developed by kinetic means, and (b) COs need to have a nexus to the conflict. Consequently, only the COs that support kinetic operations during armed conflicts "are the only type of operations that States have acknowledged and have considered being governed by IHL" (International Committee of the Red Cross, 2016, as cited in Gisel et al., 2020, p.303).

2.1.1. Cyber operations in and as international armed conflicts

Concerning IAC, Common Article 2 of the Geneva Conventions establishes:

> [..]The present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance. Although one of the Powers in conflict may not be a party to the present Convention, the Powers who are parties thereto shall remain bound by it in their mutual relations. (Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1949, art. 2)

This article reflected the customary law and included the application of the Hague Conventions in the cases of declared war or an armed conflict between States. Also, the article derived three cases about when would be applied IHL to cyber operations between States, as follows.

> 1) if they are preceded by a declaration of war made through cyber or traditional means of communication; (2) when the cyber operations occur in the context of an already existing international armed conflict and have a nexus with it; and (3) when they amount themselves to a global armed conflict, with or without the concomitant occurrence of kinetic hostilities. (Roscini, 2014, p.120)

The declaration of war requires the *animus bellandi*. So, "war in the legal sense is started exclusively by an 'overt act' by which a state manifests its intention to turn a state of peace into a state of war (animus bellandi)" (Wright, 1932, as cited in Roscini, 2014, p.120). *Animus bellandi* must be communicated through a declaration of war, as mentioned in the 1907 Hague Convention III. However, the parties could start the hostilities with the intention or aim of making a war leaving aside the declaration or ultimatum of war. Independent of the declaration form, which could be made through cyber means, only if the declaration has (a) the animus bellandi and (b) is authorized by an organ state, it could be understood as a declaration of war. In that case, the state parties may commit an internationally wrongful act as a treaty violation. However, having as a requirement an ultimatum of cyber war could be impossible because, apart from the nature of cyber operations, its "surprise and plausible deniability factors" (Roscini, 2014, p.122). Nowadays, the ultimatum only is seen as a formality and a symbolic act.

The declaration of war "creates a state of war in the legal sense between the belligerents, whether or not hostilities have commenced or actually follow" (Roscini, 2014, p.121). There are many consequences of a state of war, but the most important is the application of the IHL. Because it will govern the "cyber attacks[18] and cyber exploitation[19] conducted by the belligerents against each other after a declaration of war, whether or not kinetic hostilities occur" (Mancini, 2009, as cited in Roscini, 2014, p.122).

Cyber operations *in the context of* an existing IAC could be employed as force multipliers. As given above, the cyber operations accomplished in an armed conflict will be subject to IHL, and the term *in the context of* is still unclear. However, Roscini (2014) considered it relevant to relate this concept with the *belligerent nexus* related to the direct participation in hostilities under IHL proposed by the ICRC. Consequently, according to the ICRC view:

> Not every act that directly adversely affects the military operations or military capacity of a party to an armed conflict or directly inflicts death, injury, or destruction on persons and objects protected against direct attack necessarily amounts to direct participation in hostilities.(Melzer & International Committee of the Red Cross [ICRC], 2020, p.58)

Direct participation refers to an act linked to the hostilities conducted between parties to an armed conflict, so hostilities must be understood as (a) the resort to means and methods with the purpose of injuring the enemy, (b) individual attacks against the adversary and (c) they must be designed *to directly cause the required threshold to harm* in support of a party to an armed conflict and the detriment of another (belligerent nexus). Otherwise, if the act does not meet the requirements, the action will not be considered direct participation. The subjective intention and hostile intent are separate concepts of belligerent nexus because the nexus is associated with the objective purpose of the act, not with the state of mind of a person (Melzer & International Committee of the Red Cross [ICRC], 2020).

As a result, the nexus between the conflict and the cyber operations will be determined if "the cyber operations are conducted by a belligerent against another and cause or are reasonably likely to cause the required threshold of harm to the adversary" (Roscini, 2014, p.1123). Consequently, the hostilities must be governed by IHL.

---

[18] It has the purpose of disrupting, denying, degrading, or destroying information on a computer network or system. Example: manipulate or destruct the data on a computer to control military communications (Owens, Dam&Lin, 2009). Recovered from: https://h2o.law.harvard.edu/playlists/657

[19] It is the act make for monitoring or espionage computer systems. Also, it does not affect the normal functioning of the computer. Example: steal military secrets (Owens et al., 2009).

What happens if the cyber operations were conducted alone without kinetic operations in an armed conflict? The 1949 Geneva Conventions does not define the concept of armed conflict, but the Commentary of Common Article 2 mention that it could be understood as (a) a difference arising between two States and (b) leading to the intervention of members of the armed forces despite of the Parties denies the existence of a state of war (Pictect, 1952, as cited in Roscini, 2014). So, these two elements are essential for the existence of an IAC, and the animus bellandi is not longer a requirement. However, the notion of armed forces does not have a universal definition. According to Smitt (2002):

> What is relevant for the determination of the existence of an international armed conflict, then, is not who carries out the activity on behalf of the states involved, but what activity is typically associated with the armed forces, ie resort to armed force. (as cited in Roscini, 2014, p.127)

The ICTY, when defining the concept of international armed conflict and did not mention if there is a relation between resort to armed force and the use of armed force (*jus ad bellum)* or if the resort to armed force needs a minimal level of intensity for an IAC to exist. So, could the 'use of armed force' in the jus ad bellum sense also amounts to a 'resort to armed force" under the IHL? Beckett (2000) considered that "whether a cyber operation is a breach of Article 2(4)[20] of the UN Charter or an armed conflict are 'essentially synonymous', as 'any use of force is regulated by IHL" (as cited in Roscini, 2014, p.128). Many authors expressed that "the jus in bello applies whenever a state uses force in the sense of the jus ad bellum against another state" (Roscini, 2014, p.128).

In addition, they mentioned that not always the use of armed force is going to be an armed conflict. For example, training armed groups, the provision of military equipment or the funding by a state to rebels fighting against another state are not amount resort to armed force. Even there are actions related to the use of armed force (jus ad bellum) that are not a resort to armed force under the IHL, such as "the use of armed forces of one State which are within the territory of another State with the agreement of the receiving State" (RES 3324 as cited in Roscini, 2014). The existence of an IAC is not based on the use of force, according to Article 2(4). So, the existence is focused on the concept of belligerent hostilities that is understood as the application of means and methods of warfare.

> The notion of direct participation in hostilities essentially comprises two elements, namely that of "hostilities" and that of "direct participation" therein. While the concept of "hostilities" refers to the (collective) resort by the parties to the conflict to means and methods of injuring the

[20] All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations. Article 2(4) UN Charter.

> enemy, “participation” in hostilities refers to the (individual) involvement of a person in these hostilities

As given above, the IHL will govern cyber operations and all kinds of weapons, but for qualifying as a means of war, the cyber operation should injure the enemy. If the cyber operation is designed to infiltrate a computer system and steal data, it will not be a weapon and could not produce an IAC. Consequently, the ICRC expressed that only “destructive cyber operations may give rise to an armed conflict” and qualify as armed conflict. Many authors affirmed that IHL must be applied if:

- Hostilities are understood “in terms of consequences, i.e., destruction or damage to property or mental or physical harm to individuals” (Roscini, 2014, p.131).
- Network attacks are intended to cause injury, harm, death, or destruction.
- The COs are designed to affect the military operations of the other part of the conflict.
- The COs resulted in the medium or long-term interruption or the destruction “or long-lasting damage to computer systems managing critical military or civil infrastructure. It could conceivably be considered an armed conflict” (Roscini, 2014, p.131).

According to the intensity threshold regarding IAC, the ICRC emphasizes that there is no minimum intensity threshold for IAC. It does not matter the number of victims or how long the conflict last. The IHL must be applied to any shot fired, as Article 1 of the Additional Protocol mentioned, “the law must be applied to the fullest extent required by the situation of the persons and the objects protected by it” (as cited in Roscini, 2014, p.134). However, only the cyber operation that disrupts the correct functioning of military or civilian CII[21] could qualify as a “resort to armed force” and begin an IAC. Because these types of COs will have the same destructive effects as other traditional armed forces. It is essential to clarify that “this minimum threshold is not for the resort to armed force to be an international armed conflict, but for the cyber operation to be a resort to armed force” (Roscini, 2014, p.135).

On the other hand, the State practice and some humanitarian arguments emphasize that IHL “applies as soon as armed force is used between States, irrespective of the intensity of the violence” (Gisel et al., 2020, p.304). As a result, IHL will protect the persons overwhelmed by armed conflict. So, once States use armed forces, they must:

- manage their attacks at military objectives and not harm civilians or civilian objects
- safeguard civilians and their objects

[21] The private character of the targeted infrastructure is not an impediment to determining the existence of an IAC.(Roscini, 2014)

The protection should be for everyone who needs it, no matter if there are one or many civilians. Also, if the use of cyber operations between States has effects akin to the traditional means and methods of warfare, the IHL must be applied. To summarize, the experts of the Tallinn Manual 2.0 (2017) considered that cyber operations by themselves can cross the threshold of IAC under IHL (as cited in Gisel et al., 2020). And the ICRC agrees with it because cyber operations that could destroy civilian or military assets or in the death or injury of soldiers or civilians should not be treated differently from equivalent attacks conducted by traditional means and methods of warfare (kinetic warfare). In addition, there are only two cases when the law of IAC will apply to a conflict between a state and an armed group "when (a) the insurgents have been recognized as belligerents by the government against which they fight and (b) in the situations envisaged in Article 1(4) of Additional Protocol I" (Roscini, 2014, p.140). Consequently:

> Cyber operations amounting to resorting to armed force conducted by a national liberation movement in their struggle against colonial domination, racist régimes, or alien occupation would then potentially fall under the scope of application of Additional Protocol I for the states parties to it. (Roscini, 2014, p.140)

In this case, the application of Protocol I is necessary for a minimum threshold. It means that it will apply if the national liberation movement has a quasi-state level of organization (Roscini, 2014). However, identifying the threshold is still pending, like other considerations, such as what happens with cyber operations that do not physically harm objects. Could be this cyber operation considered a resort to armed force as IHL establishes and consequently could be governed by IHL? It is a theme of debate.

2.1.2. Cyber operations as international armed conflicts and non-international armed conflicts

In non-international armed conflicts, two main criteria are necessary: (a) the organization of the parties to the conflict and (b) the intensity of the violence. The NIAC is developed between governmental authorities and organized groups or only between the groups inside a state's territory. The main element is the nature of the belligerents, and the element of intensity is essential because "a non-international armed conflict will only exist if violence between two or more organized parties is sufficiently intense"(Gisel et al., 2020, p.305), and the application of IHL depends on the accomplishment of the requirements. However, determining the organization criterion could be a problem in armed groups; it requires a

particular specialized appraisal of the facts. Consequently, it is improbable, but not far-fetched, that cyber operations can fulfill the needed level of intensity.

The IHL applies to cyber operations that were conducted in an already existing NIAC, provided that the cyber operations have a nexus with the conflict. In the NIAC will be more challenging to identify ordinary crimes between cyber operations which are "equivalent" to hostilities. The legal framework of the NIAC is Common Article 3, but it does not determine any intensity threshold for applying it. But the commentary of the article provides some standards relate to the existence of a NIAC. Even some elements allow differentiating the NIAC from the insurrections or banditry. There are "(1) armed violence; (2) which is protracted; (3) and occurring between governmental authorities and armed groups, or between armed groups; (4) providing that the armed groups are organized" (Tallinn Manual, 2013, as cited in Roscini, 2014, p.151). Consequently, if the armed group has the capacity to make cyber attacks the element of the organization is covered. In addition, the absence of an organized group despite the fact that cyber operations could seriously damage the state infrastructure causes IHL can not to apply.

The element of armed violence may be interpreted as the concept of armed force, and all the aspects reviewed in the IAC must be applied to NIAC. What should be tested is the level or organization of the armed group and if the COs could qualify as protracted armed violence. The ICTY (2008) "has clarified that 'protracted armed violence' has to be interpreted as referring to the intensity of the conflict, and not to its duration" (as cited in Roscini, 2014, p.152). The intensity is not linked to a time element. The COs must generate damage to property, loss of life, or injury to persons is going to be a NIAC. Also, it may exist even if it has a short duration. Also, if there is (a) a sporadic attack or its nature is isolated to the NIAC or (b) the motivation of the armed group is political, it will not be an armed conflict by Article 1(2) of Additional Protocol II that applies in addition to the Common Article 3. In the absence of kinetic hostilities, only the COs that generate harm to critical infrastructures for a prolonged time could be governed by the law of NIAC (Roscini, 2014).

For instance, Common Article 3 is supplemented by Additional Protocol II. So, the Protocol must fulfill the following requirements:

I. It shall apply to all armed conflicts which are not covered by Article of the Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I).
II. It takes place in the territory of a High Contracting Party.
III. It is developed between its armed forces and dissident armed forces or other organized armed groups
IV. The organized groups should be under responsible command.

V. The organized groups should exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol. (Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977., 1949, art.1)

As a result, Additional Protocol II applies in the case of conflicts with a nature of high magnitude. So, if the NIAC did not reach the threshold of API II, the conflict would be governed by Common Article 3. In the cyber context could be more difficult the application of API II. Therefore, Article 3 "continues to apply as a 'minimum standard of humanity to all other armed conflicts" (Roscini, 2014, p.158) because it reflects basic humanitarian protections. Finally, all armed violence that does not reach the intensity of Article Common 3 will be ruled by international human rights law and domestic law.

The IHL does not govern cyber operations make outside of an armed conflict. However, there are some considerations about the application of IHL principles to cyber operations at any time. For example, the protection of persons not or no longer taking part in hostilities established in Common Article 3 could always be applied. Nevertheless, some principles, such as distinction and proportionality, could have problems in their application outside an armed conflict (Gisel et al., 2020).

2.2.Martens Clause: scope of protection to Critical Information Infrastructure (CII)

The Martens Clause has gone down in history as a principal instrument for the IHL development. It is a century-old declaration, but this has, at least so far, not made it less highly valued. For that reason, it is used for developing of IHL rules by States, courts, and some organizations like the ICRC, United Nations, and NATO, which have a particular concern about the effects of armed conflicts. Also, its importance in the field of IHL is linked to the aim of regulating "military situations occurring in the course of hostilities between conflicting parties that are not covered by existing international and national legal standards" (Ivanenko, 2022, p.2).

Critical infrastructure (CI) is vulnerable to attacks because it could affect the essential activities of human beings provided by them in the modern world. For that reason, it is necessary to create solutions to prevent and control those possible risks and threats that the use of cyberspace implies. For that reason, the Martens Clause will be interpreted under article 31 of the Vienna Convention on the Law of Treaties to define the scope of protection against cyber warfare and defining the crucial role of the Clause against the regulatory gaps for protecting the Critical Information Infrastructures (CII).

2.2.1. History and evolution of the Martens Clause

The Martens Clause was proposed by Fyodor Fyodorovich Martens, a representative member of the Russian Empire, at the First Hague Conference in 1899. Ivanenko (2022) considered that it is unusual that a treaty provision carries the name of the person who proposed it because it is viewed as a privilege in international law. However, Fyodor Martes was not an ordinary man, his actions have put his name beside great international law figures like Henry Dunant. Martens' reputation was based on three aspects: "his advocacy of international arbitration; his crusade for implementing humanitarian concepts, epitomized in the famous *Martens Clause*; finally, his pivotal role in creating *The Hague Tradition"* (Eyffinger, 2012, p.14).

Fyodor Martens was born in 1845 in Pernov, Russia. At the age of nine years old was sent to an orphanage in the city of San Petersburg. Then, in 1863 started his studies at the University of St. Petersburg. His academic background and talented mind made him deserve the appreciation from the Dean of the Faculty, professor I.Ivanovsky (Pustogarov, 1996). Consequently, he finished his studies and received the title of professor of international law. He entered the department of foreign affairs in 1869 and remained a permanent member and counselor until his death on June 20, 1909 ("Frederic de Martens," 1909).

Martens considered that the inviolability of life, honor, and dignity are rights recognized by each person, not because the rights were protected by the criminal law otherwise but because each human being has the right to the honor, dignity, and inviolability of life. In his career, he stood out for his humanity and justice ideals. As a result, he placed the human being at the center of international law. He affirmed the existence of a unique law throughout the history of nations: *the principle of respect due to human person*[22] (Pustogarov, 1996). He believed that respect for human rights is the appropriate criterion for determining the State's civilization degree and international relations. Moreover, when the States recognize that the human being is the source of civil and political rights, international law will reach a high degree of development, law, and order. So, protecting human beings is the purpose of the States and the objective of international relations. This idea is kept in the UN Charter and the Universal Declaration of Human Rights. As is evident, Martens's humanism doctrine was discordant with his country's militaristic spirit (Pustogarov, 1996).

Furthermore, in his opinion, the unique and compatible solution with the humanitarian purposes of the law was to limit the horror of war through the formulation of rules that all the

[22] The principle has a relation with the concept that recognizes the autonomy of human being.

States accepted. His thought disagreed with the pacifist of the epoch. By 1895, there were already 125 pacifist organizations distributed in countries like the United States, United Kingdom, France, Italy, and others. The pacifist organization's view was united to civilized states to peacefully resolve all conflicts and reduce the armaments for universal disarmament because weapons production was more advanced and harmful (Pustogarov, 1996).

However, the will of States was not predisposed to impose restrictions on the weapons and instruments of war or to introduce and make humanitarian rules to conduct the war despite the St Petersburg Declaration signed in 1868, the Geneva Convention of 1864, and the foundation of the ICRC in 1863 by Henry Dunant. It was only the first step to becoming aware of the rules of war because the process of formulating them was just starting (Pustogarov, 1996).

Once the Ministry of Foreign Affairs employed Martens in the position of collegiate secretary, he showed to the minister of foreign affairs, Alexander Mikhailovich Gorchakov, and the minister of war, Dmitry Alekseyevich Milyutin, “his first foreign policy proposal, regarding the holding of an international conference to adopt a convention on the laws and customs of war” (Ivanenko, 2022, p.9). Mertens’s job in preparing the proposal was influenced by the Franco-Prussian War and its brutality consequences. Martens believed that the devastating consequences of it were the incorrect interpretation of the international military laws and the unclear obligations of the parties in the conflict ” (Ivanenko, 2022).

By 1874, Martens elaborated a draft convention relating to the law and custom of war. The convention “aimed at formally limiting the means and methods of warfare, alleviating the suffering of the civilian population and reducing the destruction caused by military action” (Ivanenko, 2022, p.10). Also, it contained rules for the protection of civilians and non-combatants. The convention was a Russian initiative, and the Martens draft was exposed to the International Conference celebrated in Brussels in 1874. However, the Conference has not approved the convention because the idea of restricting the war through international law had resistance. The States approved the convention as a declaration and 20 years later became a convention in the Hague Conference. The results of the Conference did not discourage the Martens's work in the preparation of documents related to the ICRC, such as the review of the Geneva Convention in 1906 (Pustogarov, 1996).

In addition, all his work took him to conduct and organize the First Hague Peace Conference in 1899 after the failure of the Brussels Conference. Even he proposed the Program of the Conference. In 1898, the Russian Minister of Foreign Affairs sent a note to the representatives of states in St Peterburg with the proposal of celebrating a conference that

guaranteed peace and put limits to weapons development. As a result, some states supported the proposal, but Martens knew that any Power was willing to disarm. However, the proposal was supported by the peace movement, the ICRC, and the Red Crescent Movement (Pustogarov, 1996).

In the Hague Conference, Martens was chairman of the second commission tasked with the elaboration of a Convention on the Laws and Customs of War on Land. So, the commission-based their work on his previous draft convention made for Brussels Conference. In addition, after many weeks of debate, the delegates of each country agreed on the text of the fifty-six articles of the Convention. However, before the final vote for approving it, Édouard Descamps and a group of Europe states were against the principles of the rights and the occupying forces' duties, and he demanded a right to armed resistance against occupying forces (Ivanenko, 2022). The delegates could not agree about the status of civilians bearing against an occupying force. So, Martens proposed a solution due to the Martens Clause that was included in the Preamble of the Hague Conventions II of 1899 concerning the laws and customs of war on Land as follows.

> Until a more complete code of the laws of war is issued, the High Contracting Parties think it right to declare that in cases not included in the Regulations adopted by them, populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilized nations, from the laws of humanity, and the requirements of the public conscience. (Hague Convention II, 1899)

The solution was accepted by all the parties, and the complete text of the Convention was approved. As a result, the signed conventions in the First Hague Conference impacted in the development of international law. Even some clauses of the Hague Conventions have contributed to the growth of some branches of international law. Finally, the Martens's work on the draft convention to the Brussels Conference was not in vain because it allowed laying the groundwork to limit the war through the Martens Clause and the other articles of the convention. Moreover, its international recognition allowed the Clause to be part of international law “as a separate provision in a range of instruments, sometimes with editorial adjustments or with evolved content widening the scope of its protection” (Ivanenko, 2022, p.13).

As a result, it has been included in the Hague Convention of 1907, the Geneva Conventions of 1949, the Additional Protocols, the Preamble to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons, the Resolution XXIII of the Tehran Conference of Human Rights, and other instruments. Also, it has been analyzed in the Nuremberg jurisprudence and was cited in many treaties that regulate the means and methods

of war. After all, as Meron (2000) established, the Martens Clause "originated as supplementary or residual protection, based on the sources of morality and of law, pending a comprehensive codification of the law of war" (p.78).

2.2.2. Interpretations: restrictive, ample, moderate, and jurisprudential

Salter (2012) considered that the Clause had constituted one of the origins of international law generally and international humanitarian and human rights law in particular. In addition, the Martens Clause has helped in the development of customary international and the protection of individuals and groups in an armed conflict. At the First Hague Convention, the Martens Clause was stipulated to regulate the status of civilians against an occupying force. Since then, it has been the object of many interpretations, and it has been concluded that the Clause outstretches to all parts of international law. However, to date, the Clause has not had an official interpretation.

The most accepted interpretations of the Clause are (a) the restrictive interpretation that assimilates the Clause as redundant and part of international custom (b) the moderate stance that recognizes the use of the Clause for interpreting treaties, but it does not conceive that it has specific prohibitions, and (c) the ample interpretation that recognizes in the Martens Clause independent sources of law, and (d) as a judicial interpretative aide.

The restrictive interpretation mentions that customary international law is applicable after the approval of a conventional norm. On the other side, the ample interpretation maintains that because of the small number of international treaties about the law of armed conflicts, the Martens Clause stipulates that the things that are not prohibited by a treaty are not allowed *ipso facto*[23]. In addition, conduct in an armed conflict should not only be judged based on treaties and customs. The principles of international law that are mentioned in the Clause should be taken into account, too (Ticehurst, 1997).

In addition, the International Court of Justice in the Legality of the Threat or Use of Nuclear Weapons Advisory Opinion (1996) made references to the Martens Clause. However, it did not help in the task of comprehending the Clause, but the arguments made by States and some dissenting opinions gave an opening to new interpretations. In some declarations request for Advisory Opinion, the Russian Federation's position was that the Martens Clause was considered inapplicable because by 1949 and 1977, there was already a convention to regulate the armed conflicts (The Geneva Conventions). This position rest importance to "underplay

[23] It means immediately.

customary law in favour of treaty law" (Salter, 2012, p.407). In addition, Salter (2012) affirmed that:

> A restricted mode of interpretation could also maintain the scope of the Clause is confined to the specific treaty (or treaties in post 1899 versions) to which it formed a part, and thus applies only to signatories" is also a restrictive interpretation. (p.408)

Arguments that justify these positions are related to the fact that the Martens Clause was contained only in the Preamble to the Hague Convention II, not in the substantive body. Consequently, the preambles "do not establish in themselves any distinct and directly applicable norms" (Greenwood, 1995, as cited in Salter, 2012). In this way, the restrictive interpretation "underplays the force of customary international law despite its frequent recognition and application by judges" (Salter, 2012, p.411) and refuses the development of the Clause through jurisprudence.

Even the redaction of the clause is open to restrictive interpretations based on "traditional positivistic concerns for optimizing 'legal certainty' and doctrinal 'determinacy', and thereby cutting down the scope of broadly defined general principles especially those with moralistic and natural law aspects and/or connotations" (Pustogarov, 2010, as cited in Salter, 2012, p.410). The positivistic views deny the moralistic concepts such as humanity and dictates of public conscience because if these categories are recognized as law, they will generate arbitrary judicial decisions. In this case, "the Clause is no more than a principle, or meta-rule of interpretation" (Salter, 2012, p.49).

Regarding the moderate stance, the United Kingdom's position accepted the application of the Martens Clause. The Clause proved that the lack of a treaty prohibiting the use of nuclear weapons did not mean that their use might be legal. But the UK submitted that the clause does not on its own establish the illegality of nuclear weapons (United Kingdom Written Statement, p.48). Because to rule it an express prohibition would be needed. However, for Ticehurst (1997) this conception is a restrictive interpretation of the Clause because the UK only mentions the Clause as an existing remembrance of customary rules did not include in specific treaties.

On the other hand, the statement of the Clause in the Hague Convention II and its incorporation in the Geneva Convention of 1949 and their Additional Protocols of 1977 is linked to its validity as "a living part of international law" (Weeramantry, 1996, p.484). This argument about the importance and validity was confirmed in the Nauru case. It mentioned that the Martens Clause has full validity because it has been recognized in many treaties regarding the law of war (Ticehurst, 1997).

Regarding to the recognition to the Martens Clause as a customary international humanitarian law the Judge Koroma in his Dissident Opinion mentioned that:

> With regard to the applicability of Additional Protocol 1 of 1977 to nuclear weapons, the Court recalled that even if not al1 States are parties to the Protocol, they are nevertheless bound by those rules in the Protocol which, when adopted, constituted an expression of the pre-existing customary law, such as, in particular, the Martens Clause, which is enshrined in Article 1 of the Protocol. (Koroma, 1996, p.565)

Also, the Inter-American Court of Human Rights, in the Case of Barros Altos, recognized that the addition of the Clause in many conventions of IHL is sufficient reason for it to be considered as a material source of IHL (Tocino, 2018). As a result, the inclusion of the Clause in the basic text of the Protocol suggests that the Martens Clause reaches the status of *jus cogens* norm of customary and humanitarian treaty law. And, despite the Clause not including in specific treaties the status of the preemptory norm, it has "the direct force of a juridical norm of international humanitarian law possessing universal and binding authority" (Pustogarov, 2010, as cited in Salter, 2012, p.411).

Judge Shahabudden, in his Dissident Opinion, gave an ample interpretation of the Clause and mentioned that the International Court of Justice determined that the Martens Clause is a customary rule with its own regulatory status. It means that the Clause has norms to regulate the conduct of States. It is not a remembrance of customary rules, the Martens Clause has its regulatory status that allows it to work independently of the other rules. Also, he explained that the principles of international law mentioned in the Clause were born from three different sources (a) the usages established between civilized nations, (b) the laws of humanity, and (c) the requirements of the public conscience (Ticehurst, 1997).

Before the Hague Convention II, some treaties recognized the principles of humanity and conscience. But the value given in the Hague Convention was the recognition as part of customary international law with an independent validity of treaty law. Despite the fact that it is in the Preamble. The Clause is a general legal norm is not limited to a specific case. As a result:

> [..] the Martens Clause proclaimed for the first time that there may exist principles or rules of customary international law resulting not only from state practice, but also from the laws of humanity and the dictates of public conscience. (Salter, 2012, p.423)

For that reason, in the case of unclear or inexistent rules of armed conflict, the judges thought a justification could "fill the legal gaps with decisions guided by the Clause's broad principles of IHL" (Salter, 2012, p.422). In addition, the interpretation mentioned that the

principles of humanity are independently existing general norms capable of supplying gaps and deficiencies in more specific treaty measures (Salter, 2022).

Also, the relative and variable nature of the norms of the Martens Clause allows "judicial applications in novel contexts exceeding the scope of pre-existing rules or case law" (Salter, 2012, p.422). As a result:

> The Clause articulates principles of international law under which considerations of humanity can, by themselves, directly exert independent legal force to govern state conduct. This applies even in cases where no relevant doctrinal rule has been expressly provided. (Salter, 2012, p.426).

Regarding the Martens Clause as a source of law in the Legality of the Threat or Use of Nuclear Weapons Advisory Opinion (1996), the ICJ included the Clause as one of the cardinal principles of IHL next to (a) the protection of the civilian population and (b) the prohibition of unnecessary suffering. Also, Judge Shahabuddeen recognized the Clause as a directly applicable general principle. So, the principles of humanity and dictates of public conscience as principles of international law are constant. However, in time, even they could justify a method of warfare or weapon in one epoch and prohibit it in another (Salter, 2012).

In contrast, the Clause seen as a judicial guideline implicates that "is an aide for judges seeking to resolve disputes between two of more possible interpretations of an ambiguous or imprecise legal rule and/or a situation" (Slater, 2012, p.413).To illustrate, during the Proceeding at Nuremberg, the court stipulated that in case of a disagreement between an interpretation that follows the principles of humanity and one against them, the first interpretation should be recognized. In some specific treaties where the concept of principles of humanity are already defined, the Clause is "used as guidelines for determining the proper interpretation to be placed upon vague or insufficiently comprehensive international principles or rules" (Cassese, 1981, as cited in Salter, 2012, p.414).

Even the President of the ICTY Antonio Cassese, mentioned that " the Clause should be judicially interpreted and applied primarily as a principle of judicial interpretation" (Prosecutor v Kupresˇkic´ et Al (Judgment) ICTY 95-16-T, 2000). Furthermore, when the Clause is used as a judicial aid, its interpretation could facilitate the emergence of new customary rules on IHL, and do not matter if the state practice is missing. In addition, the Clause has helped in the task of general instruction about international rules. Because international principles and rules must be:

> interpreted and applied in the interpretative context of Clause's principles, and thus in a manner that establishes the optimal coherence between them and a viable interpretation of what is consistent with broader principles of 'humanity' and the dictates of 'public conscience'. (Salter, 2012, p.416).

For example, the Advisory Opinion of the Inter-American Court of Human Rights (2017) argued that the principles mentioned in the Clause have an independent validity and are contrary to international law and the progressivity of rights that States adopt conduct for limited asylum because the limitation set aside the laws of humanity, the dictates of public conscience, and universal morality.

Moreover, despite the absence of codification of customary law rules and the little consistency of the state practice to create customary rules, the interpretation of the Martens Clause extends the scope of protection of some rules. For example, the Clause helped in the interpretation of the prohibition of reprisals against civilians and civilian property for IAC. The humanitarian justification was the base for extending the protection to civilians because, pending further development of custom by States, the protection offered by the Clause could be set aside (Slater, 2012). Also, it can be seen in the ICC Rome Statute that criminalizing some genocide acts as violations of principles of humanity is the result of the interpretative aid (Salter, 2012).

> In this respect, the interpretative application of this clause facilitates judges engaging actively in the 'progressive' politics of the ever-greater enforcement of international human rights, with the added advantage of not ever having to expressly abandon their more traditional stance of non-political neutrality. (Salter, 2012, 419)

As a result, the Martens Clause has permitted the development of judicial law-making through the interpretation of judges. On the contrary, the restrictive interpretation could not justify how later case law has adopted the Clause as a supporting aide in jurisprudence and its recognition as independent principles. In addition, there is a stance relating to positive law and natural law. It establishes that the States which does not follow conventional rules or do not admit the development of a customary rule they do not obligate by the rules that do not accept. So, they are not responsible for their non-compliance. In contrast to the positive law, the natural law is universal and binding for all people and States. The Nuremberg Trial accepted this conception and admitted the validity of natural law in the 20th century (Ticehurst, 1997).

Finally, the ample interpretation could be the answer to extend the protection of the Martens Clause to CII because there are still problems of how to apply IHL involving cyber-attack as a conflict. Even the Clause could provide minimum guarantees of humanity in all situations of cyberwarfare; however, one interprets it.

2.2.3. Interpretation under the Vienna Convention

To understand the scope of the Martens Clause to the CII, it will be reviewed under the rules of interpretation of international treaties set out in the 1969 Vienna Convention on the Law of Treaties. Article 31 mentions the general rule of interpretation for treaties as follows.

> 1. A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose.
> 2. The context for the purpose of the interpretation of a treaty shall comprise, in addition to the text, including its preamble and annexes:
>
> (a) any agreement relating to the treaty which was made between all the parties in connection with the conclusion of the treaty;
>
> (b) any instrument which was made by one or more parties in connection with the conclusion of the treaty and accepted by the other parties as an instrument related to the treaty.
>
> 3. There shall be taken into account, together with the context:
>
> (a) any subsequent agreement between the parties regarding the interpretation of the treaty or the application of its provisions;
>
> (b) any subsequent practice in the application of the treaty which establishes the agreement of the parties regarding its interpretation;
>
> (c) any relevant rules of international law applicable in the relations between the parties.
>
> 4. A special meaning shall be given to a term if it is established that the parties so intended. (Vienna Convention Law of Treaties, 1969)

2.2.3.1. Literal Interpretation

First, the Vienna Convention Law of Treaties (1969), in its article 31(1), commented that a treaty must be interpreted in good faith in harmony with the ordinary meaning (a) to the terms of the treaty and according (b) to its object and purpose. The goth faith is linked with (a) the obligation *pacta sunt sevanda* of the States to fulfill its rules in good faith according to the general rules of international law governing interpretation treaties and (b) the assignment for interpreting the treaty to properly and honest performance of the treaty (Gardiner, 2015). Linderfalk (2007) mentioned that this provision describes three distinct ways of interpretation, which are “the interpretation using conventional language (ordinary meaning), interpretation using context, and interpretation using the object and purpose of the treaty” (p.61). Treaties should be interpreted as a whole, not only through the meaning of the words. The interpretation must respect their objective and purpose (Gardiner, 2015).

The ordinary meaning adduces the meaning of the words in conventional language. Furthermore, the judicial opinions have stipulated that “the ordinary meaning” of a treaty is to be determined not by everyday language alone, but by everyday language and technical language considered as one single whole” (Linderfalk, 2007, p.67). For the duty of interpretation, it is necessary to (a) have familiarity with the language's lexicon and (b) know the morphological, syntactical, and pragmatic rules of the language used for the treaty. In addition, according to article 31(4), a term will have “a special meaning” if it is the parties'

intention. Consequently, the meaning of the terms will classify into two types (a) the conventional meaning based on the language practice or (b) non - conventional meaning, that is:

> Founded only on the parties' own semantic stipulations: the parties may have felt compelled to introduce a new term in the treaty; or – probably more likely – they may have selected a term that already exists, but for one reason or another – implicitly or explicitly – they have agreed to give the term a new semantic content, better suited to the purposes at hand. (Linderfalk, 2007, p.64).

The Hague Convention II will be a supplementary tool for the literal interpretation of the Martens Clause. The Convention's original language is French, which was translated into English, and other languages for its comprehension, so for analyzing the literal interpretation, French and English language sources will be used to determine some meanings of the words. The original text in French mentions:

> En attendant qu'un Code plus complet des lois de la guerre puisse être édicté, les Hautes Parties contractantes jugent opportun de constater que, dans les cas non compris dans les dispositions réglementaires adoptées par elles, les populations et les belligérants restent sous la sauvegarde et sous l'empire des principes du droit des gens, tels qu'ils résultent des usages établis entre nations civilisées, des lois de l`humanité at des exigences de la conscience publique. (Hague Convention II, 1899)

In addressing this issue, we start identifying the ordinary meaning of the words that belong to the Martens Clause. So, the Clause will be divided into three parts.

a) *En attendant qu'un Code plus complet des lois de la guerre puisse être édicté* (Until a more complete code of laws of war is issued)[24]

The ordinary meaning of words

The review of each word will be in French, with the translation of each definition.

En attendant: the word *attendant* is a conjugation of the verb *attendre.* It does not have a technical or special meaning agreed upon by the treaty's parties. According to conventional language, it refers to the action of:

- staying in one place until someone arrives (Larousse, 2022, definition 1).
- deferring until something happens, until a specific date (Larousse, 2022, definition 3).

Even there is a French expression, *En attendant,* that means *"*temporarily, until the moment when what is expected will happen" (Larousse, 2022).

Code: refers to a "collection of laws and regulations that govern an area of law" (Larousse, 2022, definition 2).

[24] English official translation.

Plus: is an adverb that means a higher degree or value (Larousse, 2022, definition 1).

Puisse: is a subjunctive verb of the word *pouvoir (power).* It means "having the possibility, the physical, material" (Larousse, 2022, definition 1).

Êdicte: is a verb which means publish a law, promulgate a law, or proscribe them in official form (Larousse, 2022, definition1). Even a synonym could be the word issued, which means "to put forth or usually distribute officially" (Merriam-Webster, n.d., definition 1). In a technical sense, the 'promulgation' of international law could be realized through the adoption of the text of a treaty by States participating in its elaboration. Relating to the translation in English, the word has the same meaning as in French.

Lois de la Guerre (Law of war) is an expression that refers to the "set of conventions, rules, and customs intended to humanize war" (Larousse, 2022). In a technical sense, the expression was used to designate the laws that ruled the war. As given in the first chapter, the IHL is the law of war or *jus in bello* that have as its purpose to conduct the hostilities and the protection of war victims. The Departament of Defense (2015) mentioned in the Law of War Manual of the USA that "International humanitarian law is an alternative term for the law of war that may be understood to have the same substantive meaning as the law of war" (p.7). Even it could have a relation with other bodies of law, such as:

> (1) law of war rules superseding rules in other bodies of law concerning armed conflict; (2) construing the rules in other bodies of law to avoid conflict with law of war rules; (3) law of war rules informing the content of general standards in other bodies of law, should such standards be construed to apply to armed conflict; and (4) law of war treaties explicitly incorporating concepts from other bodies of law. (Office of General Counsel Departament of Defense, 2015, p.9)

Also, since 1977 the term international humanitarian law has been used by States to describe the field of law as a whole. Nowadays, IHL is a widespread term, and many states refer to it, such as the United Nations Security Council, the General Assembly of the UN, the International Court of Justice (ICJ), and the International Committee of the Red Cross (ICRC). However, armed forces still use the term 'law of war' or 'law of armed conflict' (Hampson, 2018)

About the objective and purpose of the treaty:

> On August 12/24, 1898, The Russian Minister of Foreign Affairs, Count Mouravieff, handed to the diplomatic representatives at Petrograd a circular note proposing a conference of the Governments having diplomatic representatives at the Imperial Court, to consider "a possible reduction of the excessive armaments which weight upon all nations". (Russian Circular Note, 1898, as cited in Brown Scott, 1915, p.vi[25])

[25] Handed to the Russian Circular Note proposing the First Peace Conference.

In addition, he mentioned that the moment was favorable for seeking, “by means of international discussion, the most effective means of ensuring to all peoples the benefits of a real lasting peace” (Russian Circular Note, 1898, as cited in Brown Scott, 1915, p.xiv). Because the preservation of peace has been an aim for the States and he made a call for the States to accomplish their supreme duty of “checking these increasing armaments and in seeking the means of averting the calamities which threaten the entire world” (Russian Circular Note, 1898, as cited in Brown Scott, 1915, p.xiv).

Also, in the Circular Count Moravieff emphasized the objectives of the proposed conference:

(a) Put limits to the increase of military and naval armaments

(b) Discussion of the possibility of preventing armed conflicts by the pacific means at the disposal of international diplomacy.

All the points to be discussed following the Program Proposed by the Imperial Government of Russia to the Governments invited to the First Peace Conference had a relation to the law of war as follows.

> Program Proposed by the Imperial Government of Russia to the Governments invited to the First Peace Conference
>
> 1.An understanding stipulating the non-augmentation, for a term to be agreed upon, of the present effective armed land and sea forces,as well as the war budgets pertaining to them; preliminary study of the ways in which even a reduction of the aforesaid effectives and budgets could be realized in the future.
>
> 2. Interdiction of the employment in armies and fleets of new firearms of every description and of new explosives, as well as powder more powerful than the kinds used at present, both for guns and cannons.
>
> 3. Limitation of the use in field fighting of explosives of a formidable power, such as are now in use, and prohibition of the discharge of any kind of projectile or explosive from balloons or by similar means.
>
> 4. Prohibition of the use in naval battles of submarine or diving torpedo boats, or of other engines of destruction of the same nature; agreement not to construct in the future war-ships armed with rams.
>
> 5. Adaptation to naval war of the stipulations of the Geneva Convention of 1864, on the base of the additional articles of 1868.
>
> 6. Neutralization, for the same reason, of boats or launches employed in the rescue of the shipwrecked during or after naval battles.
>
> 7.Revision of the declaration concerning the laws and customs of war ellaborated in 1874 by the Conference of Brussels, and not yet ratified.
>
> 8. Acceptance, in principle, of the use of good offices, mediation, and voluntary arbitration, in cases where they are available, with the purpose of preventing armed conflicts between nations ; understanding in relation to their mode of application and establishment of a uniform practice in employing them. (Russian Circular Note, 1898, as cited in Brown Scott, 1915, p.xviii).

The parties of the Hague Convention knew that all the rules adopted in the conference were not enough to rule the armed conflicts. The previous experience with the Conference of Brussels was learning for them. The initiative made by Czar Alexander II with the purpose of

examining the draft of an international agreement concerning the laws and customs of war submitted to 15 European States by the Russian Government was not ratified by States as a binding convention. However, the project was an essential step in the codification of the laws of war (Schindler & Toman, 1988). The Hague Conference only was a first step in preserving the peace as Moravieff mentioned:

> This conference would be, by the help of God, a happy presage for the century about to open. It would converge into a single powerful force the efforts of all the States which sincerely wish the great conception of universal peace to triumph over the elements of disturbance and discord. It would at the same time cement their agreement by a solemn avowal of the principles of equity and law, upon which repose the security of States and the welfare of peoples. (Russian Circular Note, 1898, as cited in Brown Scott, 1915, p.xvi).

Moreover, the paper Instructions to the American Delegates to the Hague Conference of 1899 recognized the Convention as a "fruitful field discussion and future action for the prevention of armed conflict by pacific means " (as cited in Brown Scott, 1916, p.8). Even years later, on October 1904, the Secretary of State of the United States considered that the Hague Conference on May 18, 1899, was an emblematic fact in the history of nations. So, the work of the parties generated "the acceptance by the signatory Powers of Conventions for the peaceful adjustment of international difficulties by arbitration, and for certain humane amendments to the laws and customs of war"[26] (Brown Scott, 1915, p.xxi). Accordingly, the results of the Convention did not have an effect on disarming the armed forces. It was evidenced in the use of poison gas and other means of war that Germany did in the First World War. The rules were limited because of their general and no restrictive nature (Jeannesson, 2020).

To conclude, the Clause, when referring to *Until a more complete code of laws of war is issued* shows the concern of the parties for maintaining the peace and the legal gaps that the Convention could leave. In addition, it can understand as a call to action to the States to codify the IHL. This call to action functioned because in 1907 was adopted the Second International Peace Conference and the agreements originated in 1864 and updated in 1949 about the Humanitarian Law of Armed Conflicts known as the Geneva Conventions.

b) *les Hautes Parties contractantes jugent opportun de constater que, dans les cas non compris dans les dispositions réglementaires adoptées par elles* (the High Contracting Parties think it right to declare that in case not included in the regulation adopted by them[27])

The ordinary meaning of words

[26] Diplomatic Correspondence of the Secretary of State of the United States to the American Diplomatic Representatives accredited to the governments signatory to the acts of the First Hague Conference.
[27] Official English translations.

Hautes parties contractantes (H.P.C): means the "members of delegations engaged in negotiations; signatory parties to a pact or agreement" (Larousse, 2022). Generally, the treaties had been adopted by States, and they are considered a party which means "a State which has consented to be bound by the treaty and for which the treaty is in force" (Vienna Convention Law of Treaties, 1969). Also, the term "is a diplomatic formula for designating the parties to an international agreement" (Arthur, 1941). However, there is a question about whether the term refers only to the States that ratified the treaty or signed the treaty but did not ratify it. Even to the States that never ratify it.

The term High Contracting Parties for the Geneva Conventions are the States that have ratified the Conventions and consequently are bound to respect the treaty despite the fact they do not ratify it. The action of 'respect and to ensure respect' means that States, their armed forces, the people, and groups acting on their behalf should respect the treaty. Even the High Contracting Parties that are not a party to an armed conflict must "ensure respect for the Conventions by other High Contracting Parties and non-State Parties to an armed conflict" (Commentaries to the Convention II for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 2017). The obligation to respect and ensure respect is part of customary international humanitarian law. For that reason, the obligation is not only limited to the Geneva Conventions. The obligation encompasses all the rules of IHL.

Also, the declarations to abstain from the use of bullets that expand or flatter easily in the human body at the Hague Convention II stipulated that:

> []..the Convention is binding on the contracting Powers in the case of a war between two or more of them. It shall cease to be binding from the time when, in a war between the contracting Powers, one of the belligerents is joined by a non-contracting Power. (Brown Scott, 1899, p.19)

Consequently, the Hague Convention II is only an obligatory rule for the States who ratified it. The Hague Convention II was ratified by 26 States, and 22 countries signed an adhesion to the treaty. Also, 16 States signed the Convention but have not yet ratified among them is Ecuador. See the tables of signatures, ratifications, and adhesions[28]. However, the Hague Regulations respecting the Laws and Customs of War on Land are considered

[28] See https://bit.ly/3gVXo7R .Taken of the book by Brown Scott, J. (Ed.). (1915). The Hague Conventions and Declarations of 1899 and 1907 Accompanied by Tables of signatures, Ratifications and Adhesions of the various Powers, and Texts of Reservations (Second). New York, United States: Oxford University Press. Pages 230-234.

customary international law, binding on all States independently of their acceptance of them. According to this, the Martens Clause is part of customary IHL.

Jugent: is a verb from the word *juger* (to judge).

De constater que: is a verb that means notice, but technically for law, the meaning is to record or to certify (Collins French Dictionary, 2022, definition 2)

Compris: is the verb in the past tense of *comprendre* (understand). Also, *non compris* means excluding (*Collins French Dictionary*, 2022)

dispositions réglementaires adoptées par elles: refers to the arrangements adopted in the Hague Convention II. The First Hague Conference opened on 18 May 1899 until July 29,1899, and it consisted of three main treaties and three additional declarations[29]:

- Convention (I) for the Pacific Settlement of International Disputes
- Convention (II) with respect to the Laws and Customs of War on Land
- Convention (III) for the Adaptation to Maritime Warfare of the Principles of the Geneva Convention of 22 August 1864

So, to review the program proposed by the Imperial Government of Russia the heads of State represented in the hall of the Conference were divided into Three Commissions:

> The First Commission shall take charge of Articles 1, 2, 3, and 4 of the circular of December 30, 1898.
> The Second Commission shall take charge of Articles 5, 6, and 7 of the said circular.
> The Third Commission shall take charge of Article 8 of the same circular.
> Each Commission may be subdivided into subcommissions. (Brown Scott, 1899, p.19)

Fiódor Fiódorovich Martens was the President of the Second Commission. See Appendix C for checking the members of the Commission in the representation of each State. The Commission had the duty to "examine the Geneva Conventions of 1864, to its extension to maritime war and the revision of the draft Declaration elaborated by the Brussels Conference of 1864" (Brown Scott, 1899, p.383). For that reason, Mr. Martens subdivided the Commission, the first to examine the questions relating to the Red Cross and the second for analyzing the Brussels project regarding the laws of war.

The Second Commission had four meetings between May 23, 1899, to July 5, 1899, until the text of each article respecting the laws and customs of war on land was adopted

[29] The declarations are: (I) Declaration concerning the Prohibition of the Use of Bullets which can Easily Expand or Change their form inside the Human Body such as Bullets with a Hard Covering which does not Completely Cover the Core or containing Indentations. (II)Declaration concerning the Prohibition of the Discharge of Projectiles and Explosives from Balloons or by other new analogous methods.
(III) Declaration concerning the Prohibition of the Use of Projectiles with the Sole Object to Spread Asphyxiating Poisonous Gases.

without any observations (Brown Scott, 1899). However, there were some subjects that the Conference set aside, such as "questions affecting the rights and duties of neutrals, the inviolability of private property in naval warfare, and the bombardment of ports, towns, and villages by a naval force" (Brown Scott, 1915, p.vi). So, Mr. Martens, when referring *in a case not included in the regulation adopted by them*, is linked to the idea that despite the work made in the meetings of the Conference, there are many rules set aside because (a) a change made in the adoption of the article and the sense of the text change or (b) the Hague Convention II did not adopt rules outside the Program Proposed by the Imperial Government of Russia.

c) *les populations et les belligérants restent sous la sauvegarde et sous l'empire des principes du droit des gens, tels qu'ils résultent des usages établis entre nations civilisées, des lois de l`humanité at des exigences de la conscience publique* (populations and belligerents remain under the protection and empire of the principles of law of nations, as they result from the usages established between civilized people, from the laws of humanity, and from the requirements of the public conscience[30])

In the Hague Conventions of 1907, the term populations were replaced with *inhabitants*, the term principles of the law of nations were replaced with *international law*, and the term requirements to *dictates* (Meron, 2000).

The ordinary meaning of words

les populations (populations- inhabitant): refers to the number of people or inhabitants that live in the country or region (Merriam-Webster, 2022, definition 1). A synonym is a community or citizenry. For IHL, a civilian is a person that does not belong to the armed forces. Also, the civilian populations are protected from the dangers of military operations.

Regarding the law of cyberspace, the Tallinn Manual 2.0 (2017), civilians lost their protection from attacks while they directly participated in cyber operations. No treaty or customary law prohibits civilians from participating in hostilities during an IAC or NIAC (Rule 91). In the case of NIAC, civilians are "those individuals who are not members of the State's armed forces, dissident armed forces, or other organized armed groups" (Tallinn Manual 2.0, 2017, p.414). Moreover, the civilian population shall not be the object of cyber-attack. In case of doubt about a person's civilian status, the person should be considered a civilian (Tallinn Manual 2.0, 2017, p.424).

Les belligérants (belligerants): The term was used to refer (a) the States taking part in a war or (b) the individuals authorized to use armed force. Also, it is used to refer to individual

[30] Official English translations and the first text of the Hague Convention II.

insurgents who control the territory of a State. The special meaning given by the parties of the treaty is mentioned in article 3 of the Hague Convention II that stipulated "the armed forces of the belligerent parties may consist of combatants and non-combatants" (1899, art.3). In the case of combatants, they have the right to participate directly in hostilities.

Nowadays, the IHL introduces the term combatant to identify the population that is part of the armed conflict. The Tallinn Manual 2.0 (2017) in Rule 96 identify as an object of cyber-attacks:

> (a) members of the armed forces;
> (b) members of organized armed groups;
> (c) civilians, if and for such time as they take a direct part in hostilities, and
> (d) in an international armed conflict, participants in a levée en masse. (p.425)

It is essential to mention that the "members of the armed forces who are medical or religious personnel, or who are hors de combat, are not subject to attack" (Tallinn Manual 2.0, 2017, p.415). Consequently, individuals are *hors de combat* if they have not participated in hostilities or them sick. However, if a member of the armed forces continues participating in COs, it is not *hors de combat.*

restent(remain): means "maintaining oneself, continuing to be in the same position" (Larousse, 2022, definition 5).

sauvegarde (protection): refers to a "protection granted by an authority" (Larousse, 2022, definition 1).

principes du droit des gens, tels qu'ils résultent des usages établis entre nations civilisées, des lois de l`humanité at des exigences de la conscience publique **(**the principles of law of nations, as they result from the usages established between civilized people, from the laws of humanity, and the requirements of the public conscience): the principles of humanity could be interpreted in the sense that it prohibits the means and methods of war that are not necessary for obtaining a military advantage. Pictet (1986) understood the concept of humanity in the sense that humanity requires choosing the detention against the injury, the injury against the death, and, as far as possible, not attacking the not *hors de combat* (as cited in Ticehurst, 1997). In addition, the principles of the law of nations are a guarantee provided under the doctrine of military necessity (Ticehurst, 1997).

Regarding the requirements of public conscience, it refers to the draft law projects, declarations, resolutions, and communications made by people and qualifies institutions for evaluating the law of war. Also, the declarations should limit the courses that have knowledge of the cause and constitute evidence of the public conscience (Ticehurst, 1997).

According to Meron (2006), the public conscience could be reviewed from two perspectives they can be seen as (a) public opinion that shapes the conduct of the parties to a conflict and promotes the development of international humanitarian law, including customary law" (Meron, 2006, p.23) and as (b) a reflection of *opinion juris*. As a result, these two perspectives had been recognizing by judges.

On a literal reading, the Clause could support its condition as a residual legal.

> That is, a norm which only comes into play in contexts where there appear to be 'gaps' in the laws of war developed by the Hague Regulations. On this interpretation, the Clause is confined to operating as no more than an a contrario device, reminding states that even where there is no formal and express obligation [..], there can still be international law duties, possibly backed up with criminal sanctions. (Salter, 2012, 409)

However, following the dissident opinion of Judge Weemantry and the ample interpretation of the Clause, the true essence of the Clause keeps the following thought.

> The Martens Clause clearly indicates that, behind such specific rules as had already been formulated, there lay a body of general principles sufficient to be applied to such situations as had not already been dealt with by a specific rule. (Weeramantry, 1996, p.484)

In addition, Van Den Boogaard (2013) defined the principles of international law as the general perception behind specific rules. The Advisory Committee of Jurists, in the drafting of article 38 of the Statue of the Permanent Court, put into consideration the problem that in the future, the ICJ could find a dispute do not govern by a treaty or any customary law that could be applied to it. In this way, the Commission agreed to use the general principles of law recognized by civilized nations (Thirlway, 2019). Its primary function is supplementary because it fills gaps in treaties or customary law (Henckaerts, 2020).

> The general principles of law are classified into two categories: a) principles that regulate substantive conduct and their application to private parties and States; b) norms that regulate the exercise of sovereign or adjudicative powers and therefore apply only to States and international tribunals.(Charles T. Kotuby Jr. & Sobota., 2017, p.1)

Also, principles are born from (a) domestic law; and (b) general considerations or the generalization of a specific treaty. This way, the principles' recognition is not constructed by the State's will. However, the States contribute to their development. The principles introduce some considerations into international law, especially those that guide the interpretation of treaties (Wolfrum, 2012). Article 31 3c of the Vienna Convention exposes that interpreting a treaty must consider "any relevant rules of international law applicable in the relations between the parties" (Vienna Convention Law of Treaties, 1969, art.31).

The ICJ (1949) Corfu Channel Case confirmed this application when mentioning that the obligations of the Albania authorities in notifying British warships of the existence of a minefield in Albanian territorial water are based on the following:

> […] not on the Hague Convention of 1907, No. VTII, which is applicable in times of war, but on certain general and well-recognized principles, namely: elementary considerations of humanity, even more, exacting in peace than in war; the direction of the freedom of maritime communication; and every State's obligation not to allow its territory knowingly to be used for acts contrary to the rights of other States. (p.22)

By its independent operation, courts, and tribunals appeal to principles for interpretation in an international dispute. Also, some of these principles have a triple legal basis because they are based on treaties and customary law in addition to being a principle of law. For that reason, soldiers must apply these principles to any situation they are confronted with because of the role principles play in international law.

2.2.3.2.Context

In addition to the text, as part of the context, it should be considered any agreement relating to the treaty must accomplish four conditions such as:

> (1) the phenomenon must be included in the extension of the expression “agreement”; (2) it must be a question of an agreement “relating to the treaty”; (3) the agreement must have been made “between all the parties”; and (4) it must have been made “in connexion with the conclusion of the treaty”. (Linderfalk, 2007, p.134)

The parties should accept the affinity between the treaty and other agreements to consider it as part of the context. This consideration is not an obligatory requirement because determining the “relationship between the treaty are the intentions of their parties” (Linderfalk, 2007, p.135). Also, the agreement should have the state's intention for creating a law. Correspondingly, the provisions of a treaty should be interpreted in harmony with other provisions of the treaty, its preamble, and annexes, as well as with other agreements concluded between the same parties that expand or modify the treaty or with the unilateral interpretative declarations made by each state and that the rest accept as a related instrument to the treaty (Linderfalk, 2007).

In the Final Act of the Conference, the States agreed to submission for signature by the plenipotentiaries on the text of the Conventions and Declarations enumerated and annexed to the Act. The Three Declarations were:

1. To prohibit the discharge of projectiles and explosives from a balloon or by other similar new methods.

2. To prohibit the use of projectiles, the only object of which is the diffusion of as asphyxiating or deleterious gases.
3. To prohibit the use of bullets which expand or flatten easily in the human body, such as bullets with a hard envelope that does not entirely cover the core or is pierced with incisions.

We can conclude that the primary purpose is the maintenance of general peace and a possible reduction of excessive armament. The Russian circular note mentioned that through the Conference, the States could "seeking the most effective means of ensuring to all peoples the benefits of a real and lasting peace and above all of limiting the progressive development of existing armaments" (Brown Scott, 1915, p.v). As a result, the Conferences establish rules.

2.2.3.3.The object and purpose of the treaty

The treaty's object refers to its aim, and its purpose relates to its motive. For determining the object of the treaty is necessary to review the Preamble of the Convention respecting the Laws and Customs of War on the lad as follows.

> Thinking it important, with this object, to revise the general laws and customs of war, either with a of defining them more precisely, or of laying down certain limits for the purpose of modifying their severity as far as possible;
> Inspired by these views, which are enjoined at the present day, as they were twenty-five years ago at the time of the Brussels Conference in 1874, by a wise and generous foresight;
> Have, in spirit , adopted a great number of provisions, the object of which is to define and govern the usages of war on land.
> In the view of the high contracting Parties, these provisions, the wording of which has been inspired by the desire to dimmish the evils of war so far as military necessities permit, are destined to serve as general rules of conduct for belligerents in their relations with each other and with populations. (Hague Convention II, Preamble, 1899)

To sum up, the two main objectives of the Hague Convention were (a) defined and governed the usages of war on land and (b) to rule the conduct of belligerents and their relations with populations. Moreover, Eyffinger (2012) mentioned that:

> The object of the articles, imbued with the best of humanitarian considerations, was to reduce the evils of war for the harmless population of invaded countries. To minimize civil unrest, the invaded country was advised to acknowledge *in limine* all rights and claims advanced by the invader. At the same time its population was ordered to abstain from participating in hostilities. (p.26)

On the other hand, the objective of the Clause was "provide residual humanitarian rules for the protection of the population of occupied territories, especially armed resisters in those territories" (Meron, 2000, p.18). The acceptance of the agreement was at risk because the

Belgian delegate Descamps was against the articles treating not only the duties but also the rights of occupying powers. He mentioned that the small countries would reach a state of occupation. Consequently, they were against any limitations in a situation against occupiers. Martens defined this moment as a crisis, and in the fourth meeting of the Second Commission on July 5, 1899, he read the declaration, and the sub-commission immediately adopted it for submission to the Conference (Brown Scott, 1899). In addition, relate to the effects of the Clause:

> Delegates concluded that the introduction of the Martens Clause had broken an early diplomatic impasse by providing additional substantive legal protections for civilians by appropriately controlling military behaviour. (Salter, 2012, p.429)

2.2.3.4.Rules of interpretation under article 31.1: subsequent agreement, subsequent practice, and relevant rules.

The interpretation of the Martens Clause is unclear, and for that reason, as Salter (2012) mentioned that "is necessary for judges to consider the implications of the Clause's total trajectory from 1899 to the present" (p.412). Specifically, there is no agreement relative to the interpretation of the Martens Clause. However, the subsequent practice of the parties has done that that Clause was incorporated in some conventions that governed the use of means and methods of warfare, the conduct of hostilities, and occupation.

Also, it was included in Second Conference in 1907. The Martens Clause was not incorporated in the Geneva Conventions of 1949, but the Convention alludes to the Clause to regulate the denouncement of the convention. However, the Additional Protocols recognize the Clause as an independent rule for the protection of civilians. Referring to treaties, the Clause has been "re-affirmed in slightly different wording by numerous 20th Treaties and Conventions" (Salter, 2012, p.405), including the 1949 Geneva Conventions and the 1977 API I and API II.

Also, the Clause was used in interpreting some cases such as Nicaragua v. United States, The Prosecutor v. Kupreskic, Constitucional Conformity of Protocol II, in the Report of Autonomous Weapon Systems, and the Colombia Peace Agreement. However, despite recognition of the Clause in treaty law, its value lies in the recognition as customary law that binds all the States. Finally, the Tallinn Manual recognized the Martens Clause as customary law, and its function is to rule activities representing a legal vacuum.

The Tallinn Manual 2.0 affirmed that:

> The law of armed conflict applies to the targeting of any person or object during armed conflict irrespective of the means or methods of warfare employed. Consequently, basic principles such

> as distinction and the prohibition of unnecessary suffering apply to cyber operations. (2017, p.414)

Consequently, we can conclude following this rule, and the ample interpretation of the Clause that situates it next to the cardinal principles of IHL, each source of it such as the dictates of public conscience, the laws of humanity, and the requirements of public conscience, must be respect in the cyber warfare.

2.3.The Critical Information Infrastructure (CII) and the Cyber-warfare

The concern for protecting critical infrastructure in many countries is reflected through programs, plans, and legislative measures. Already in 2010, the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security established that the problems of the 21st century had a relation with the field of information security because the growing use of technology had created new vulnerabilities and opportunities for destabilization the national infrastructure, individuals, and governments. Furthermore, they mentioned that the development of communications technologies as tools of warfare and for intelligence and political purposes made by States it will increase in the future (United Nations, 2010, RES A/65/201).

Consequently, Information and Communications Technology (ICT) is everywhere, and its nature is not absolute civil or military. It depends on the use given by the user. Moreover, because of the massive interconnectivity of telecommunications and the Internet, ICT could become the target of misuse. In the same way, using ICT in critical infrastructure "creates new vulnerabilities and opportunities to create instability" (United Nations, 2010, RES A/65/201, p.7).

First, the Critical Infrastructure (CI) are physical "key systems, services, and functions whose disruption or destruction would have a debilitating impact on public health and safety, commerce, and national security, or any combination of these" (International Telecommunication Union, 2008, as cited in García Zaballos, 2016, p.36). Also, it could be defined as the essential organizational and physical structures of a nation and economy that their failure would generate in "sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences" (Germany, 2009, as cited in García Zaballos, 2016, p.36).

In addition, the Commission of the European Communities (2004) mentioned that critical infrastructures are involved in many sectors of the economy, like transport, energy,

food supply, communication, financial activities, and others. As a result, the critical infrastructures that are necessary for the perfect operation of the public and private sectors are:

- Power plants and networks
- Communications and information technologies (software, internet, hardware)
- Finance (insurance)
- Water (storage, reservoirs, treatment, networks)
- Health (hospitals, health care, and blood supply centers)
- Food (food industry)
- Transportation
- Production, storage, and transport of dangerous goods
- Military and defense systems, civil protection
- Public agencies and administration
- Media

However, the critical infrastructures vary depending on the specifics of the national situation in a particular country. Consequently, some sectors may become critical if there are risks that could threaten their delivery and operation. In addition, critical infrastructures have types of interdependencies such as (a) physical that is when an infrastructure depends on the material of the other, (b) cyber, which allows transmitting the information through the CI, (c) geographic, when the operation of the CI depends on the local environment, and (d) logical that is any dependency not physical, cyber, or geographic (García Zaballos, 2016, p.36). As a result, their protection could not be isolated, and many efforts in the level of defense are required.

On the other hand, Critical Information Infrastructures are "systems, belonging to the Information and Communication Technology, which are critical - not just for their own sakes, but for other CI that rely on them" (Esposito Amideo & Scaparra, 2017). It could be defined as networks; some examples of CII are the Internet or terrestrial and satellite networks. Also, there are critical elements in the delivery of service systems, so a failure in a CII may produce harmful effects on the critical infrastructures that depend on it. The disruptive events that could affect the CII are (a) physical attacks or (b) cyber-attacks.

Correspondingly, there are some scenarios in armed conflicts that could be developed:

1. The parties could realize kinetic attacks and therefore destroy the critical physical infrastructure. In that case, the service delivery will be paralyzed because the CII cannot connect. For example:

   > [..] the 2001 World Trade Center attacks crippled communications by destroying telephone and Internet lines, electric circuits, and cellular towers. This caused a cascade of disruptions at all levels, from fuel shortages to transportation and financial services interruptions. (Esposito Amideo & Scaparra, 2017, p.76)

2. The parties that only through cyber-attacks or cyber operations disrupt the CII and the functioning of services such as energy supply, telecommunications, financial systems, and drinking water.

Nickolov (2005) identified as CII attacks the (a) unauthorized access to sensitive or confidential information, (b) the destruction, modification, or substitution of critical infrastructure software, and (c) the limitation of the access for preventing or mitigating the effects of the attacks. As a result, the effects of cyber warfare can persist for long durations, or the damage to physical systems can be irreparable. Also, it may directly affect public safety and cause the loss of human lives. Therefore, it is necessary to apply techniques to protect critical information infrastructures. As a result, the Group of Governmental Experts considered that the solution is:

> [..]ensuring global information and communication technology security, assisting developing countries in their efforts to enhance the security of their national information and communications infrastructure, information, critically important, and remedy the current disparity in the security of information and communication technologies. (United Nations, 2010, RES A/65/201, p.8).

Other measures to protect CII are:

1. Establishing a national cyberspace security response system.
2. Developing a national cyberspace security threat and vulnerability reduction program.
3. Creating national cyberspace security awareness and training programs.
4. Securing government systems.
5. Strengthening national security and international cooperation on cyber security. (Nickolov, 2005, p.110)

Moreover, the Group of Experts in the RES A/76/135 reaffirmed the observation of developed and elaborated additional binding obligations regarding using ICTs by States. Also, they recommended that States implement national ICT policies, strategies, and programs for improving critical infrastructure protection. And increase the bilateral, regional, and multilateral cooperation to foster common understandings of existing and emerging threats and the potential generated by the malicious use of ICT.

2.3.1. Protection to CII under the IHL

So, how could IHL protect civilians against its effects? The ICRC (2020), in the *Position Paper: International humanitarian law and cyber operations during armed*

conflicts[31], ratified their position that cyber operations yield the parties to the conflict many alternatives as a means or method of warfare, and military forces could use COs for supporting military operations, but parties need to consider their risks. So, military forces must accomplish their aims without harming civilians or causing destruction to civilian infrastructure. As explained above, the objective of IHL rules for conducting the hostilities is to protect civilians, opposite to their effects. Instead, "IHL prohibits directing cyber-attacks against civilian infrastructure, as well as indiscriminate and disproportionate cyber-attacks" (International Committee of the Red Cross [ICRC], 2019).

For that reason, defining if a cyber operation amounts to an "attack" as defined in IHL is essential for the application of the rules:

> [..]deriving from the principles of distinction, proportionality, and precaution, which afford important protection to civilians and civilian objects. Concretely, rules such as the prohibition on attacks against civilians and civilian objects, the prohibition on indiscriminate and disproportionate attacks, and the obligation to take all feasible precautions to avoid or at least reduce incidental harm to civilians and damage to civilian objects.

It is because many IHL rules only apply to cyber operations that qualify as attacks. The concept of attacks is defined in Protocol I (1977) as "acts of violence against the adversary, whether in offense or in defense". According to that, there are some views from states and the ICRC about what types of cyber operations are attacks.

1) Cyber operations or their effects that "cause injury or death to persons or damage or destruction to objects" (ICRC, 2015, as cited in Gisel et al., 2020) are attacks under the IHL. To illustrate, a cyber operation against an electricity network cut the service in a hospital, and as a result, many people in intensive care died.
2) Cyber operations that do not physically damage an object are attacks under IHL when they "interfere with functionality and if restoration of functionality requires replacement of physical components" (Gisel et al., 2020, p.313).
3) Cyberoperations will be considered attacks if "the restoration of functionality requires the reinstallation of the operating system or particular data" (Gisel et al., 2020, p.313).

However, these considerations are still the subject of discussion for states and organizations like the ICRC, which accepted the position that attacks under the IHL could be an operation for disabling a computer network. It does not matter if the object is disabled "through destruction or other way" (ICRC, 2015, as cited in Gisel et al., 2020, p.313). Therefore, States must work on a common opinion about this subject. They must consider

[31] CRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security, November 2019. Recovered from: https://international-review.icrc.org/articles/ihl-and-cyber-operations-during-armed-conflicts-913

"inter alia, whether a cyber activity results in kinetic and irreversible effects on civilians, civilian objects, or civilian cyber infrastructure, or non-kinetic and reversible effects on the same" (United States Submission to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2014, as cited in Gisel et al., 2020, p.315).

Lin (2012) commented that some principles are part of the *jus in bello.*

> The principle of military necessity (military operations must be intended to assist in the military defeat of the enemy and must serve a concrete military purpose), the principle of distinction (military operations may be conducted only against 'military objectives and not against civilian targets), and the principle of proportionality (the expected incidental loss of civilian life, injury to civilians or damage to civilian objects must not be disproportionate to the anticipated military advantage). (p.525)

But, in the same manner as the UN Charter, the Four Geneva Conventions do not yield information about how the above principles could be applied in any cyber conflict (Lin, 2012). To understand this, we need to analyze the scope of each principle. IHL is based on a balance between military necessity and humanity. For that reason, it recognizes that "in order to overcome an adversary in wartime, it may be militarily necessary to cause death, injury, and destruction" (Melzer, 2020,p.17). However, it does not mean that the belligerent could develop an unrestricted war because the principle of humanity limits the means and methods of warfare. Also, it implies that "those who have fallen into enemy hands be treated humanely at all times" (Melzer, 2020,p.18). Consequently, the balance between military necessity and humanity can be understood considering the principles of distinction, precaution, proportionality, and unnecessary suffering.

Melzer (2020) affirmed that the principle of distinction is the kernel of IHL. It implies that States should have a unique and main objective during a war to weaken the enemy's military forces. Furthermore, as is established in Additional Protocol I:

> To ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and, accordingly shall direct their operations against military objectives. (Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 1977, art. 48)

The principle is part of customary law and is applicable in NIAC and IAC. Also, military operations covered all actions made by armed forces related to hostilities. In case of doubt, the civilian status of a person is presumed. Even the attacker should verify the non-civilian nature of targets. On the other hand, there is a controversy about the rule for protecting objects. A civilian object is "all objects which are not military objects" (PAI I, art.52). Also,

the military objectives offer the attacker an effective contribution to military action. So, its requirements need to be analyzed in each case (Ambos, 2015). However, the major problem with applying the principle of distinction is the "interconnectivity between military and civilian computer systems and the mostly dual-use of cyber infrastructure" (Tallin Manual 2.0, 2017, as cited in Ambos, 2015, p.169). As a result, the protection of the principle of distinction is limited because the computer system could use for civilian and military purposes. For the principle, an object is civilian or military, not both. Consequently, there are two conceptions related to this subject:

- "a per se civilian computer system loses its civilian status if 'it is used to make an effective contribution to military action" (Tallin Manual 2.0, 2017, rule 102)
- Dual-use objects "are qualified as military objectives since they normally contribute to military purposes" (Tallin Manual 2.0, 2017, rule 102)

A consequence of the principle of distinction is the prohibition of indiscriminate attacks. Although it is difficult to determine the civilian and military cyber infrastructure, cyber operations against them could have unlimited effects (Ambos, 2015). Conversely, cyber tools could not be considered necessarily indiscriminate; from a technical point is a challenge that cyber operations affect only the targeted. However, it is possible, but it requires meticulous planning and use. Also, it is essential that "a cyber operation that is technically discriminate is not necessarily lawful, whether during or outside of an armed conflict" (International Committee of the Red Cross [ICRC], 2020, p.486).

The principle of proportionality is part of customary international law and will apply to IAC and NIAC. It establishes (a) limits to the use of means and methods of war and (b) prohibits generating injury or unnecessary suffering to civilians and civilian objects. So, the damage to civilians "must not be excessive in relation to the concrete and direct military advantage expected" (Phillips, 2013). Also, it will apply to COs that produce excessive collateral damage because the collateral effects are considered unnecessary suffering. The main rule is that "IHL prohibits directing cyber-attacks against civilian infrastructure, as well as indiscriminate and disproportionate cyber-attacks" (ICRC, 2019, p, 20).

On the other hand, the principle of precaution objective is "minimize civilian harm to the greatest extent possible" (Ambos, 2015, p.173). From this principle, the following duties can be derived (a) the verification of the target's nature, (b) the effects of COs must be limited as far as possible, and (c) anticipating the civilians if the cyber-attack could affect them. In addition, according to military necessity, the use of force must be linked to accomplishing a

legitimate military purpose. It does not be understood as authorization for doing acts prohibited by IHL. Hence, weakening the military capacity of the other party in a conflict is the only legitimate military purpose (Phillips, 2013).

About the protection of data as an object the ICRC mentioned:

> Moreover, data have become an essential component of the digital domain and a cornerstone of life in many societies. However, different views exist on whether civilian data should be considered as civilian objects and therefore be protected under IHL principles and rules governing the conduct of hostilities. In the ICRC's view, the conclusion that is deleting or tampering with essential civilian data would not be prohibited by IHL in today's ever more data-reliant world seems difficult to reconcile with the object and purpose of this body of law.21 Put simply, the replacement of paper files and documents with digital files in the form of data should not decrease the protection that IHL affords to them. (International Committee of the Red Cross ICRC, 2019, p.21)

As a result, Bannelier (2014) mentioned that the data would be covered by the principle of distinction when the alteration of data produce physical damage to civilians and their objects. Also, the act should accomplish all the requirements mentioned above to be considered an attack. Finally, a legal void in this subject is made evident. There are still some key issues that generate some problems with applying the IHL principles; consequently States must solve it because human dependency on technology is growing.

The ICRC report of the expert meeting about the potential human cost of cyber operations developed in November 2018 supported to settled into consideration four concerns related to the human cost of cyber operations:

> a) the specific vulnerabilities of certain types of infrastructure
> b) the risk of overreaction due to a potential misunderstanding of the intended purpose of hostile cyber operations
> c) the unique manner in which cyber tools may proliferate
> d) the obstacles that the difficulty of attributing cyber-attacks creates for ensuring compliance with international law. (International Committee of the Red Cross ICRC, 2018, p.6)

There are two ways that cyber operations might disturb infrastructure, which is (a) the affection of the delivery of essential services to civilians, such as health care or electrical grids, and (b) the physical damage to them. In this case, they could affect the following:

-The delivery of healthcare

- Industrial control systems and their critical infrastructure

-The reliability of core internet services[32]

Healthcare is digitalized, and some hospital medical devices are connected to IT. Consequently, their digital dependency makes them an easy target of attack. The cyber-attacks

[32] It refers to services provided by the Core Network, which is the network that allows those who are connected to the provision of services and their data transmission functionality.

that could affect the healthcare sector are attacks that affect (a) medical facilities, (b) medical devices in hospitals, and (c) biomedical devices connected to a network. The healthcare sector is moving to digitalization and interconnectivity for their internal operations and the commutation between other actors in the industry, such as laboratories or suppliers (International Committee of the Red Cross [ICRC], 2018).

However, the healthcare sector does not have a robust cyber security posture to mitigate the effects of COs. This stance could be justified by the fact that people have not witnessed a crisis in health care. But the expert meeting of the ICRC affirmed the existence of a trend of attacks against hospitals because hospitals are more likely to pay a ransom[33] to recover the patient's information. A solution proposed by the ICRC to protect the vulnerability of the medical sector and humanitarian organizations to cyber operations is the incorporation of a digital emblem to protect entities in the ICT environment. Also:

> A 'digital emblem'[34] would identify the digital components (assets, services, and data) of protected entities. It would signal that under IHL these entities must not be targeted and must be protected against harm. It would not provide any other cyber defence or security and would signal protection only against disruption and destruction. (International Committee of the Red Cross [ICRC], 2022, p.15)

On the other hand, on the industrial control systems and their critical infrastructure, the harmful effect can be caused directly by manipulating the industrial process (i.e., taking over control) or indirectly by deceiving the control systems about the state of the process (reducing their ability to monitor processes or interfering with safety systems). And when the objective is to disable the system, facility, or service for a long time, the attack may need to cause physical damage. Consequently, if the attack affects a specific node[35] that depends on a sub-system node the delivery of the main service could be affected.

Regarding the reliability of core internet services, the Distributed Denial-of-Services (DDoS) attacks have been used against civilians' essential services by affecting the network's availability, which means people cannot access the internet, data, or applications. As a result, the attacker can force the victim or the target to stop any delivery service or downgrade (Gu & Liu, 2012). Consequently, civilians could suffer devastating effects.

---

[33] Ransomware is a type of malicious software that block the access to a system. A case relates to a ransomware attack are all made by the Orangeworm group in some countries such as United States, Europe and Asia. Recovered from: https://www.2-viruses.com/hospitals-worldwide-orangeworm

[34] The project relate to the digital emblem was released by the ICRC on November 3, 2022. See the conference in https://www.icrc.org/en/event/digitalizing-red-cross-red-crescent-and-red-crystal-emblems-benefits-risks-and-possible

[35] Network node is the connection point among devices that received information and transmits data from one point to other.

Also, COs may be divided because of their purpose in (a) access operations or known as computer network exploitation operations (CNE) that have as a duty the reconnaissance or surveillance of data and (b) effects operations or computer network attack operations (CNA) that have therefore the tampering of data, the interruption of a system or device or the destruction of a system. The problem with these kinds of COs is their intention's most arduous recognition work because the response varies depending on the attack. Given the above, cyber operations have consolidated as a threat to elements of civilian infrastructure (International Committee of the Red Cross [ICRC], 2018). This thought is based on three aspects:

- **Overreacting and escalating response**: is based on the challenging work of detecting the authentic objective of the COs, which could be for causing physical damage or not (International Committee of the Red Cross [ICRC], 2019).
- **Uncontrollable proliferation**: the COs are used by the most advanced States, but once a cyber tool is stolen or leaked, it could be multiplied several times by enemies or adversaries (which could be States, non-State armed groups, or non-State actors) for use in a pernicious way (International Committee of the Red Cross [ICRC], 2019).
- **Difficult attribution to responsibility:** identifying the actors who violate the IHL through a cyber-attack in cyberspace is problematic because the party that launched a COs could deny their guilt.

The civilian harm made by COs is enormous because they impact essential network systems. For that reason, the States "should have mitigation strategies in place for all military cyber capabilities that they consider developing to minimize the risk of civilian harm associated with the deployment of such capabilities" (International Committee of the Red Cross [ICRC], 2020a). The IHL limits set for cyberwarfare must be considered as a mitigation strategy. Some main limitations to the protection of cyberinfrastructure are:

- Attacks must be limited to military objectives. In case of doubt about the nature of an object used for civilian purposes and used for military action, it must be presumed its nature as a civilian object (Gisel et al., 2020).
- It is an illegal attack to destroy, remove or render useless objects indispensable to the civilian population's survival.

Also, Tallinn Manual 2.0. (2017) established in Rule 99 that "Civilian objects shall not be made the object of cyber-attacks Cyber infrastructure may only be made the object of attack if it qualifies as a military objective" (p.434).

-The principle of proportionality prohibits attacks – including cyber-attacks which may be expected to cause excessive incidental harm to civilians and civilian infrastructure.

-The principle of distinction prohibits cyber-attacks directed against civilian objects such as hospitals, critical civilian infrastructure, and civilian public administrations.

However, whether the Internet and the CII could be considered indispensable to the civilian population's survival is still debatable. The cyberinfrastructure allows the functioning of some services. Still, the law needs to answer the question of the circumstances for cyberinfrastructure to be considered an indispensable object for civilians. In that case, the ample interpretation of the Martens Clause can help determine the protection of CII.

Conclusions

- It is evident that International Humanitarian Law has a legal gap for regulating the cyberoperations in the context of armed conflict. Therefore, the principles such as the (a) humanity, (b) distinction, (c) military necessity, (d) proportionality, (e) neutrality, and (f) limitation, continue to apply, moreover considering that they are based on treaties and customary law in addition to being principles of law. Therefore, they must be considered as a tool that yield protection to civilians, and the parties to the conflict in the scope of cyber operations.
- Since the promulgation of the Martens Clause in the Hague Convention of 1899, the normative force of the Martens Clause has been consolidated through jurisprudence and international treaties. However, it is its recognition as a custom of IHL that allows its application, even though a State has not ratified the treaties that contain it. The principles of international law, principles of humanity and the customs of civilized nations extend the protection for critical information infrastructures. As a result, the interpretation of the Martens Clause as part of the law of armed conflicts allows the parties will be protected by the norms of international.

- Cyber operations between States are increasingly part of our daily life, and international law must face this global challenge. It is well known that the lack of regulation of cyber operations allows in a certain way free will to meet any objectives (not only military) of each State and for that reason it is too tempting to waste it. However, in the absence of international law rules that specifically regulate state cyber operations, it is essential that States rule it thought intergovernmental processes and try to reach consensus about a framework for cyber operations as NIAC or IAC. Moreover, it is fundamental the academic exercises, such as the Tallinn Manuals and the efforts of the ICRC to accomplish it, continue to be considered to guide the understanding and decisions of the States particularly within the framework of negotiations such as in the United Nations or any regional meetings.

References

Ambos, K. (2015). International criminal responsibility in cyberspace. In Tsagourias & Buchan (eds.), *Research handbook on international law and cyberspace* (pp. 152–181). Cheltenham: Edward Elgar Publishing Limited.

Arthur, K. (1941). Interpretation of the Term "High Contracting Parties" in the Air Traffic Convention. *The American Journal of International Law*, *35*(1), (pp.132–135). DOI: https://doi.org/https://doi.org/10.2307/2192605.

Ashraf, C. (2021). Defining cyberwar: towards a definitional framework. *Defense & Security Analysis*, *37*(3), (pp.274–294). DOI: https://doi.org/10.1080/14751798.2021.1959141.

Backstrom, A., & Henderson, I. (2012). New capabilities in warfare: an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. *International Review of the Red Cross*, *94*(886), (pp.483–505). DOI: https://doi.org/10.1017/S1816383112000707.

Bannelier, K. (2014). Is the principle of distinction still relevant in cyberwarfare? In Tsagourias & Buchan (eds.), *Research handbook on international law and cyberspace* (pp. 427–456). Cheltenham: Edward Elgar Publishing, Inc.

Brown Scott, J. (1899). *The Proceedings of the Hague Peace Conferences Translations of the Official Texts, Prepared in the Division of International Law of the Carnegie Endowment for International Peace*. New York, United States: Oxford University Press.

Brown Scott, J. (Ed.). (1915). *The Hague Conventions and Declarations of 1899 and 1907 Accompanied by Tables of signatures, Ratifications and Adhesions of the various Powers, and Texts of Reservations* (Second). New York, United States:Oxford University Press.

Brown Scott, J. (1916). *Instructions to the American Delegates to the Hague Peace Conferences and their Official reports, with an introduction*. New York, United States: Oxford University Press.

Brus, M. M. T. A. (2018). Soft Law in Public International Law: A Pragmatic or a Principled Choice? Comparing the Sustainable Development Goals and the Paris Agreement. In P. Westerman, J. H. S. Kirste, & A. R. Macko (Eds.), *Legal Validity and Soft Law* (pp. 243–266). Cham: Springer.

Chapple, M., & Seidl, D. (2022). *Cyberwarfare: Information operations in a connected world*. Burlington, United States: Jones & Bartlett Learning.

Charles T. Kotuby Jr., & Sobota., L. A. (2017). *General Principles of Law and International Due Process*. Pittsburgh, United States: Oxford University Press.

Collins French Dictionary. (s.f).constater que. In Collins Dictionary. Recovered From 30 October, 2022, in https://www.collinsdictionary.com/es/diccionario/frances-ingles/constater-que.

Collins French Dictionary. (s.f) compris. In In Collins Dictionary. Recovered from 30 October, 2022, in https://www.collinsdictionary.com/es/diccionario/frances-ingles/compris_1

Commentaries to the Convention II for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea. Geneva, 12 August 1949. (2017).Recovered from https://ihl-databases.icrc.org/ihl/full/GCii-commentary.

Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Geneva, 12 August 1949.

Corfu Channel case, Judgment of December 15th, (1949).

Crowther, A. (2018). National Defense and the Cyber Domain. In D. Wood (Ed.), *2018 Index of U.S. Military Strength* (pp. 83–97). Washington: The Heritage Foundation.

Dykstra, J., Inglis, C., & Walcott, T. S. (2020). Differentiating Kinetic and Cyber Weapons to Improve Integrated Combat. *Joint Force Quarterly*, *99*, (pp.116-123).Recovered from https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-99/jfq-99_116-123_Dykstra-Inglis-Walcott.pdf?ver=g74GeG8vGw7Qnee0ZByJIg%3D%3D.

Esposito Amideo, A., & Scaparra, M. P. (2017). A Synthesis of Optimization Approaches for Tackling Critical Information Infrastructure Survivability.In Havarneanu, G and Setola, R and Nassopoulos, H and Wolthusen, S, (Eds.), *Critical Information Infrastructures Security* (pp.75–87). Cham: Springer.

European Union [EU]. (2013). Draft Council conclusions on the Commission and the High Representative of the European Union for Foreign Affairs and Security Policy Joint Communication on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace 11357/13.25. June 2013.

Eyffinger, A. (2012). Friedrich Martens: A Founding father of the Hague Tradition. Fourth Friedrich Martens Memorial Lecture. *KVÜÕA Toimetised*, *15*, (pp.13–45).Recoverred from https://www.ceeol.com/search/article-detail?id=131466.

Frederic de Martens. (1909). *American Journal of International Law*, *3*(4), (pp.983–985). DOI: https://doi.org/10.2307/2186432

García Zaballos, A. (2016). *Best Practices for Critical Information Infrastructure Protection (CIIP)*. (pp.1–93). Recovered from www.iadb.org.

Gardiner, R. (2015). *Treaty Interpretation*. 2nd ed. United Kingdom: Oxford University Press.

Ghiba, M.-D. (2019). Hard Law and Soft Law in International Humanitarian Law. International Scientific Conference "Strategies XXI. *Bucharest*, 15 (2), (pp. 200–205). Recovered from https://www.proquest.com/conference-papers-proceedings/hard-law-soft-international-humanitarian/docview/2371664774/se-2?accountid=13357.

Gisel, L.,¨user, T. R., &¨rmann, K. Do. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, *102*(913), (pp.287–334). DOI: https://doi.org/doi:10.1017/S1816383120000387.

Granova, A., & Slaviero, M. (2017). Cyber Warfare.In J.Vacca (Ed.), *Computer and Information Security Handbook* (pp.1085–1104). Massachusetts: Morgan Kaufmann.

Gu, Q., & Liu, P. (2012). Denial of Service Attacks. In H.Bidgoli (Ed.), *Handbook of Computer Networks* (pp.454-468). United States: John Wiley and Sons.

Hague Convention II) with Respect to the Laws and Customs of War on Land. The Hague, 29 July 1899.

Hague, J. (2018). What Is Legal Validity? Lessons from Soft Law. In P. Westerman, J. Hage, S. Kirste, & A. R. Mackor (Eds.), *Legal Validity and Soft Law* (pp. 19–45). Cham: Springer Cham.

Hampson, F. J. (2018). Law of War/Law of Armed Conflict/International Humanitarian Law. In M. Bowman & D. Kritsiotis (Eds.), *Conceptual and Contextual Perspectives on the Modern Law of Treaties* (pp. 538-577). Cambridge: Cambridge University Press.

Heinegg, W. H. von. (2013). Territorial Sovereignty and Neutrality in Cyberspace. *International Law Studies*, *89*(1).(pp.123-156).Recovered from https://digital-commons.usnwc.edu/ils/vol89/iss1/17

Henckaerts, J.-M. (1999). Study on customary rules of international humanitarian law: Purpose, coverage and methodology. *International Review of the Red Cross*, *81*(835), (pp.660–668). DOI: https://doi.org/10.1017/S156077550005985X

Henckaerts, J.-M. (2020). History and Sources. In B. Saul & D. Akande (Eds.), *The Oxford Guide to International Humanitarian Law* (pp.1-29). United Kingdom: Oxford University Press.

Henckaerts, J. M. (2005). Study on customary international humanitarian law: A contribution to the understanding and respect for the rule of law in armed conflict. *International Review of the Red Cross*, *87*(857), (pp.175–212). DOI: https://doi.org/10.1017/S181638310018124X.

Hongsheng, S. (2006). The Evolution of Law of War. *The Chinese Journal of International Politics*, *1*(2), (pp.267–301).DOI: https://doi.org/10.1080/03050629308434821.

Inter-American Court of Human Rights[IACHR]. (2017). *Advisory Opinion N°4-3-21/2016*. Recovered from https://www.corteidh.or.cr/sitios/observaciones/oc25/51_medina_plasc.pdf.

International Committee of the Red Cross [ICRC]. (1977). *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: Martinus Nijhoff Publishers.

International Committee of the Red Cross [ICRC]. (2004). *What is International Humanitarian Law?*. Recovered from https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf.

International Committee of the Red Cross [ICRC]. (2015). *32nd International Conference of the Red Cross and Red Crescent. International humanitarian law and the challenges of contemporary armed conflicts 32IC/15/11*, (pp.2-60). Recovered from https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts.

International Committee of the Red Cross [ICRC]. (2018). *The Potential Human Cost of Cyber Operations,* (pp.3-51). Recovered from https://www.icrc.org/en/document/potential-human-cost-cyber-operations.

International Committee of the Red Cross [ICRC]. (2020a). *Avoiding civilian harm from military cyber operations during armed conflicts,* (pp.4-54).Recovered from https://issat.dcaf.ch/download/159724/3342565/4539_002-ebook.pdf.

International Committee of the Red Cross [ICRC]. (2020b). ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyb. *International Review of the Red Cross*, *102*(913), (pp.481–492).DOI: https://doi.org/doi:10.1017/S1816383120000478.

International Committee of the Red Cross [ICRC]. (2022). *Digitalizing the red cross, red crescent and red crystal emblems benefits, risks, and possible solutions,* (pp.5-39). Recovered from https://www.icrc.org/en/document/icrc-digital-emblems-report.

International Committee of the Red Cross [ICRC]. (2013). *Cyberwarfare and international humanitarian law: the ICRC's position,* (pp.2-4). Recovered from https://www.icrc.org/en/doc/assets/files/2013/130621-cyberwarfare-q-and-a-eng.pdf.

International Committee of the Red Cross [ICRC]. (2019). *Report 33IC/19/9.7 International humanitarian law and the challenges of contemporary armed conflicts Recommitting to protection in armed conflict on the 70th anniversary of the Geneva Conventions,* (pp.2-62).Recovered from https://rcrcconference.org/app/uploads/2019/10/33IC-IHL-Challenges-report_EN.pdf.

International Court of Justice[ICJ]. (26 November 1986) Military and Paramilitary Activities in and against Nicaragua [Nicaragua v. United States of America].

International Court of Justice [ICJ]. (8 July 1996). Legality of the Threat or Use of Nuclear Weapons Advisory Opinion.

International Telecommunication Union [ITU]. (2022). *Global Connectivity Report 2022,* (pp.2-162).Recovered from https://www.itu.int/itu-d/reports/statistics/global-connectivity-report-2022/.

Ivanenko, V. (2022). The origins, causes and enduring significance of the Martens Clause: A view from Russia. *International Review of the Red Cross,* (pp.1–17).DOI: https://doi.org/10.1017/S1816383122000273.

Jeannesson, S. (2020). The International Hague Conferences of 1899 and 1907. In *Encyclopédie d'histoire numérique de l'Europe [online]*. Recovered from ttps://ehne.fr/en/node/12230.

Johnson, D. R., & Post, D. (1996). Law and Borders - The Rise of Law in Cyberspace. *Stanford Law Review*, *48*(5), (pp.1367). DOI:https://doi.org/10.2307/1229390.

Jordan, W. J. (2021). *Controlling Cyberwarfare: International Laws of Armed Conflict and Human Rights in the Cyber Realm* (Thesis for de degree of Doctor). University of Waterloo).

Kittichaisaree, K. (2017). Introduction: Perspectives of Various Stakeholders and Challenges for International Law. In P.Casanovas and G.Sartor (Eds.), *Public International Law of Cyberspace* (pp.1-21). Cham: Springer International Publishing Switzerland.

Korhonen, O., & Markovich, E. (2015). Mapping power in cyberspace. *Research handbook on international law and cyberspace* (pp.46-68*)*. Cheltenham: Edward Elgar Publishing Limited.

Koroma. (1996). *Dissident Opinion of the Juzge Koroma Threat or Use of Nuclear Weapons Advisory Opinion* (p. 565).Recovered from https://www.icj-cij.org/en/case/95.

Larousse. (2022).attendant.In Larousse French Dictionary. Recovered 30 October 2022, in https://www.larousse.fr/dictionnaires/anglais-francais/attendant/563687.

Larousse. (2022).code. In Larousse French Dictionary. Recovered 30 October 2022, in https://www.larousse.fr/dictionnaires/francais/code/16882.

Larousse. (2022).plus. In Larousse French Dictionary. Recovered 30 October 2022, in https://www.larousse.fr/dictionnaires/francais/plus/61811.

Larousse. (2022). Edictê. In Larousse French Dictionary. Recovered 30 October 2022, in https://www.larousse.fr/dictionnaires/francais/édicter/27837.

Larousse. (2022).Lois de la guerre. In Larousse French Dictionary. Recovered 30 October 2022, in https://www.larousse.fr/dictionnaires/francais/guerre/38516#179901.

Larousse. (2022). Hautes parties contractantes. In Larousse French Dictionary. Recovered 30 October 2022, in https://www.larousse.fr/dictionnaires/francais/haut/39207#172875.

Larousse. (2022). restent. In Larousse French Dictionary. Recovered 30 October 2022, in https://www.larousse.fr/dictionnaires/francais/rester/68766.

Larousse. (2022). sauvegarde. In Larousse French Dictionary. Recovered 30 October 2022, in https://www.larousse.fr/dictionnaires/francais/sauvegarde/71207.

Latiff, R. (2017). *Future War Preparing for the new global battlefield*. New York, United States: Alfred A. Knopf Publishing Group.

Lin, H. (2012). Cyber conflict and international humanitarian law. *International Review of the Red Cross*, *94*(886), (pp.515–531). DOI: https://doi.org/10.1017/S1816383112000811.

Linderfalk, U. (2007). *On the Interpretation of Treaties The Modern International Law as Expressed in the 1969 Vienna Convention on the Law of Treaties*. Sweden, Netherlands :Springer Netherlands.

Melzer, N. (2020). *International Humanitarian Law A comprehensive Introduction*. Geneva, Switzerland: International Committee of the Red Cross.

Melzer, N., & International Committee of the Red Cross [ICRC]. (2020). *Interpretative Guidance in the Notion of Direct Participation in Hostilities under International Humanitarian Law*. Geneva, Switzerland: International Committee of the Red Cross.

Meron, T. (1996). The Continuing Role of Custom in the Formation of International Humanitarian Law. *American Journal of International Law*, *90*(2), (pp.238–249). DOI: https://doi.org/10.2307/2203686.

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.

Merriam-Webster. (2022). les populations. In Merriam Webster. Recovered 30 October 2022, in https://www.merriam-webster.com/dictionary/issue.

Moore, D. (2022). *Offensive Cyber Operations Understanding Intangible Warfare*. London, United Kingdom: Hurst & Company, London.

National Security Council of the U.S. (2008). *National Security Presidential Directive Nspd-54* .

Homeland Security Presidential Directive/hspd-23.Recovered from https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

NATO, & UK Ministry of Defence Crown. (2020). *Nato standard AJP-3.20 Allied Joint Doctrine for Cyberspace Operations*. Recovered from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf.

Neuman, N. (2021). Neutrality and Cyberspace: Bridging the Gap between Theory and Reality. *International Law Studies*, *97*(1), (pp. 765- 802). Recovered from https://digital-commons.usnwc.edu/ils/vol97/iss1/33.

North Atlantic Treaty Organization [NATO]. (2014). *Wales Summit Declaration*.

Office of General Counsel Departament of Defense. (2015). *Department of Defense Law of War Manual*.Recovered from https://dod.defense.gov/Portals/1/Documents/pubs/DoD%20Law%20of%20War%20Manual%20-%20June%202015%20Updated%20Dec%202016.pdf?ver=2016-12-13-172036-190

Office of the Chairman of the Joint Chiefs of Staff. (2021). *Dictionary of Military and Associated Terms*. Recovered from https://irp.fas.org/doddir/dod/dictionary.pdf.

Owens, W. A., Dam, K. W., & Lin, H. S. (2009). *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, United States: The National Academies Press.

Phillips, G. K. (2013). Unpacking cyberwar The Sufficiency of the Law of Armed Conflict in the Cyber Domain. *JOINT FORCE QUARTERLY*, *70*, (pp.70-75). Recovered from https://ndupress.ndu.edu/portals/68/documents/jfq/jfq-70/jfq-70_70-75_phillips.pdf.

Pictet, J. (1966). The principles of international humanitarian law. *International Review of the Red Cross*, *6*(66),(pp. 455–469). DOI: https://doi.org/10.1017/S0020860400011451

Polański, P. P. (2017). Cyberspace: A new branch of international customary law? *Computer Law and Security Review*, *33*(3), (pp.371–381). DOI: https://doi.org/10.1016/J.CLSR.2017.03.007.

Porche III, I. (2020). *Cyberwarfare An Introduction to Information-Age Conflict*.Norwood, Unites States: Artech House.

Prosecutor v Kupresˇkic´ et al (Judgment) ICTY 95-16-T. (2000).

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977.

Pustogarov, V. (1996). Fiódor Fiódorovich Martens (1845–1909) — humanista de los tiempos modernos. *Revista Internacional de La Cruz Roja*, *21*(135), (pp.324–339). DOI: https://doi.org/10.1017/s0250569x00021026.

Romero, D. (2019). Soft Law: ¿El "Caballo de Troya" del Derecho Internacional de los Derechos Humanos ? *Lecciones y Ensayos*, *102*, (pp.191–214). DOI: http://www.derecho.uba.ar/publicaciones/lye/revistas/102/soft-law.pdf.

Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law*. Oxkord, UK: Oxford University Press.

Salter, M. (2012). Reinterpreting competing interpretations of the scope and potential of the martens clause. *Journal of Conflict and Security Law*, *17*(3), (pp.403–437).DOI: https://doi.org/10.1093/jcsl/krs013.

Schindler, D., & Toman, J. (Eds.). (1988). *The Laws of Armed Conflicts*. Boston, United States: Martinus Nijhoff Publishers.

Schulze, M. (2020). Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *2020 12th International Conference on Cyber Conflic (CynCon)*,

(pp.183–197). DOI: https://doi.org/10.23919/CyCon49761.2020.9131733.
Shany, Y., & Schmitt, M. N. (2020). An International Attribution Mechanism for Hostile Cyber Operations. *International Law Studies*, *96*, (pp.197–222).Recovered from https://digital-commons.usnwc.edu/ils/vol96/iss1/8/.
Shreier, F. (2017). *On Cyberwarfare DCAF HORIZON 2015 WORKING PAPER No. 7*. Geneva Centre for the Democratic Control of Armed Forces (DCAF).Recovered from https://www.dcaf.ch/sites/default/files/publications/documents/OnCyberwarfare-Schreier.pdf.
Statue of the International Court of Justice. Article 38b. 26 June 1945.
The Department of the Army United States of America. (2021). *FM 3-12 Cyberspace Operations and Electromagnetic Warfare*. Recovered from https://irp.fas.org/doddir/army/fm3-12.pdf.
Tallinn Manual *2.0.* On the international law applicable to cyber operations. In M. Schmith (Ed.). New York, United States: Cambridge University Press.
The United Nations. (2010). *General Assembly Resolution A/65/201*.
The United Nations. (2013). *General Assembly Resolution A/68/98* .
The United Nations. (2015). *General Assembly Resolution A/70/174*.
The United Nations. (2021). *General Assembly resolution A/76/135*.
Thirlway, H. (2019). *The Sources of International Law* (Second). New York, United States:Oxford University Press.
Ticehurst, R. (1997). La cláusula de Martens y el derecho de los conflictos armados. *Revista Internacional de La Cruz Roja*, *22*(140), (pp.131–141). DOI: https://doi.org/10.1017/s0250569x00021919.
Tocino, I. M. (2018). La importancia de la cláusula martens en la regulación del uso de drones durante conflictos armados. In *Lecciones y Ensayos*, *101*(1), (pp. 175–203). Recovered from http://www.derecho.uba.ar/publicaciones/lye/revistas/101/la-importancia-de-la-clausula-martens-en-la-regulacion-del-uso-de-drones-durante-conflictos-armados.pdf.
United States Army War College. (2021). *Strategic Cyberspace Operations Guide*.Recovered from https://csl.armywarcollege.edu/USACSL/Publications/Strategic_Cyberspace_Operations_Guide.pdf.
Van Den Boogaard, J. C. (2013). Fighting by the principles: Principles as a source of international humanitarian law. *Armed Conflict and International Law: In Search of the Human Face: Liber Amicorum in Memory of Avril McDonald*, (pp.3–32).DOI: https://doi.org/10.1007/978-90-6704-918-4_1/COVER.
Vienna Convention Law of Treaties, 23 May 1969.
Weeramantry. (1996). *Dissident Opinion of the Juzge Weeramantry Threat or Use of Nuclear Weapons Advisory Opinion* (p. 484). Recovered from https://www.icj-cij.org/en/case/95.
Wolfrum, R. (2012). Sources of International Law. In *The Max Planck Encyclopedia of Public Internation Law*, (pp. 299–313). Recovered from https://opil.ouplaw.com/home/MPIL.
Yong-Soo, E., & Aßmann, J. S. (2016). Cyberwar: Taking Stock of Security and Warfare in the Digital Age. *International Studies Perspectives*, *17*, (pp.343–360).DOI: https://doi.org/10.1111/INSP.12073.

Appendices

Appendix A

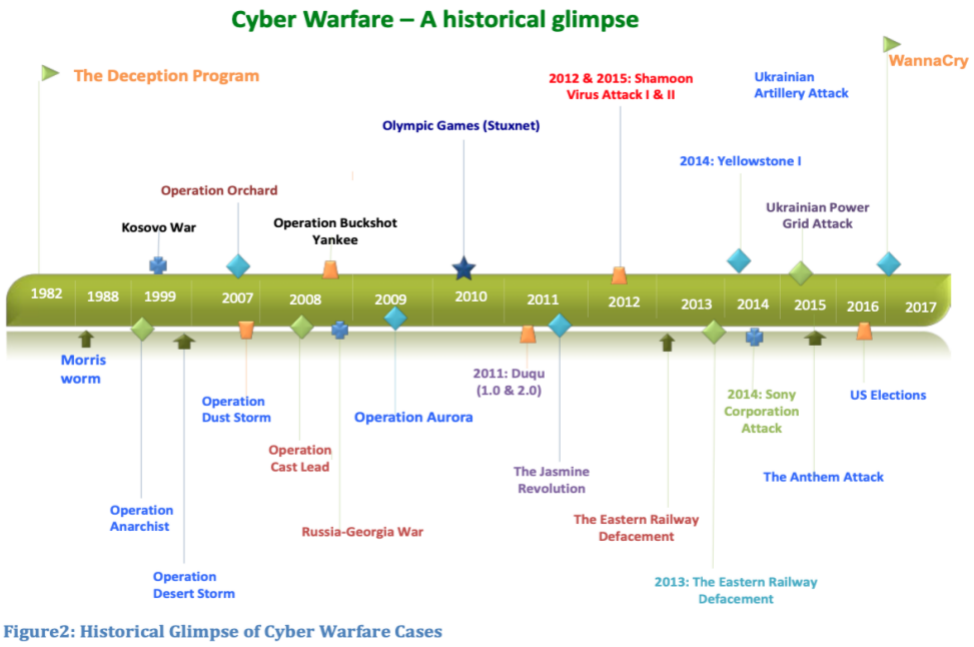


Figure2: Historical Glimpse of Cyber Warfare Cases

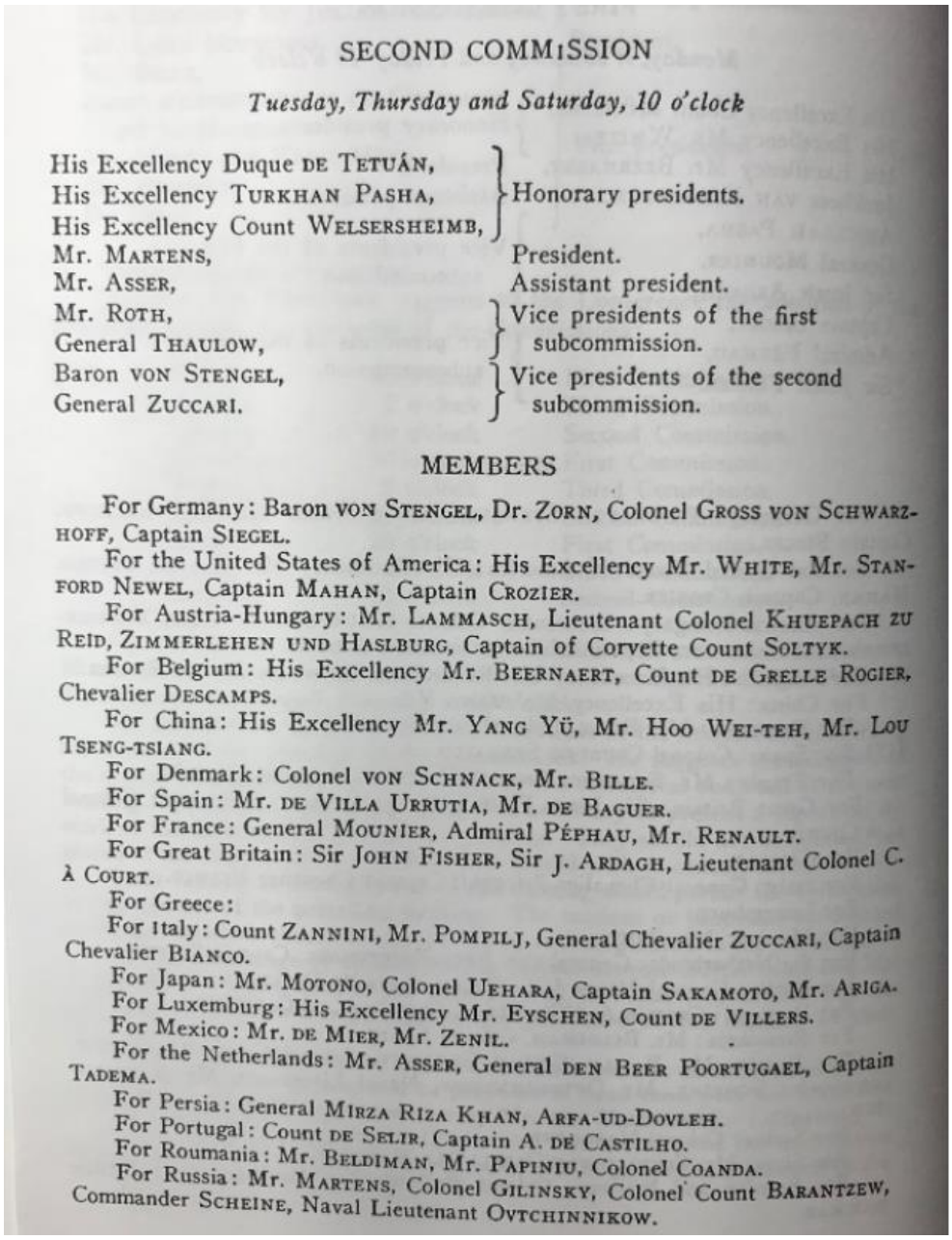
Figure 1
Cyber Warfare- A historical glimpse
Source: Cyber Warfare Conflict Analysis and Case Studies (2017).
Author: Mohan B.Gazula, 2017.

Appendix B

	RULES	Tallin 2.0	Tallin Manual
1	The IHL regulates cyber operations during an IAC or NIAC	Rule 82 IAC Rule 83 NIAC	Rule 22 IAC Rule 23 NIAC
2	In kinetic hostilities "amounting to an armed conflict, the applicable law of IAC or NIAC will govern cyber operations undertaken in relation to that conflict" (p.376).	Rule 82 IAC Rule 83 NIAC	Rule 20
3	COs are not limited to cyber-attacks. The operations could be any of those explained in the previous point **(1.2.1.2).**	Rule 92	Rule 30
4	The cyber operations that could affect the delivery of humanitarian assistance are ruled by IHL "even if they do not rise to the level of an *attack*".	Rule 145	Rule 86
5	COs are subject to geographical limitations imposed by the relevant provisions of international law applicable during an armed conflict.	Rule 81	Rule 21
6	Principles: a) Distinction b) Superfluous injury or unnecessary suffering c)Proportionality	Rule 93 Rule 104 Rule 113	Rule 31 Rule 42 Rule 51

Table 1
Rules for regulating Cyber operations by Tallinn Manual 2.0
Source: Tallinn Manual 2,0 (2017).
Author: Carolina Changoluisa, 2022.

Appendix C



SECOND COMMISSION

Tuesday, Thursday and Saturday, 10 o'clock

His Excellency Duque DE TETUÁN,
His Excellency TURKHAN PASHA,
His Excellency Count WELSERSHEIMB, } Honorary presidents.
Mr. MARTENS, President.
Mr. ASSER, Assistant president.
Mr. ROTH,
General THAULOW, } Vice presidents of the first subcommission.
Baron VON STENGEL,
General ZUCCARI. } Vice presidents of the second subcommission.

MEMBERS

For Germany: Baron VON STENGEL, Dr. ZORN, Colonel GROSS VON SCHWARZHOFF, Captain SIEGEL.

For the United States of America: His Excellency Mr. WHITE, Mr. STANFORD NEWEL, Captain MAHAN, Captain CROZIER.

For Austria-Hungary: Mr. LAMMASCH, Lieutenant Colonel KHUEPACH ZU REID, ZIMMERLEHEN UND HASLBURG, Captain of Corvette Count SOLTYK.

For Belgium: His Excellency Mr. BEERNAERT, Count DE GRELLE ROGIER, Chevalier DESCAMPS.

For China: His Excellency Mr. YANG YÜ, Mr. HOO WEI-TEH, Mr. LOU TSENG-TSIANG.

For Denmark: Colonel VON SCHNACK, Mr. BILLE.

For Spain: Mr. DE VILLA URRUTIA, Mr. DE BAGUER.

For France: General MOUNIER, Admiral PÉPHAU, Mr. RENAULT.

For Great Britain: Sir JOHN FISHER, Sir J. ARDAGH, Lieutenant Colonel C. À COURT.

For Greece:

For Italy: Count ZANNINI, Mr. POMPILJ, General Chevalier ZUCCARI, Captain Chevalier BIANCO.

For Japan: Mr. MOTONO, Colonel UEHARA, Captain SAKAMOTO, Mr. ARIGA.

For Luxemburg: His Excellency Mr. EYSCHEN, Count DE VILLERS.

For Mexico: Mr. DE MIER, Mr. ZENIL.

For the Netherlands: Mr. ASSER, General DEN BEER POORTUGAEL, Captain TADEMA.

For Persia: General MIRZA RIZA KHAN, ARFA-UD-DOVLEH.

For Portugal: Count DE SELIR, Captain A. DE CASTILHO.

For Roumania: Mr. BELDIMAN, Mr. PAPINIU, Colonel COANDA.

For Russia: Mr. MARTENS, Colonel GILINSKY, Colonel Count BARANTZEW, Commander SCHEINE, Naval Lieutenant OVTCHINNIKOW.

For Serbia: Mr. MIYATOVITCH, Dr. VELJKOVITCH.

For Siam: Mr. CORRAGIONI D'ORELLI, Mr. E. ROLIN.

For Sweden and Norway: General THAULOW, Colonel BRÄNDSTRÖM.

For Switzerland: Dr. ROTH, Mr. ODIER.

[18] For Turkey: NOURY BEY, General ABDULLAH PASHA, Admiral MEHEMED PASHA.

For Bulgaria: Dr. STANCIOFF.

Figure 2
List of Members of the Second Commission of the Hague Convention II
Source: The Proceedings of the Hague Peace Conferences (1899). Page 24-25.
Author: James Brown Scott, 1899.