UNIVERSIDADE CATÓLICA PORTUGUESA

HOW INTERNATIONAL (HUMANITARIAN) LAW INFLUENCES THE RULES OF ENGAGEMENT IN MILITARY CYBER OPERATIONS?

Bárbara Vieira Reis

Master's in Law

Faculdade de Direito | Escola do Porto

2024

UNIVERSIDADE CATÓLICA PORTUGUESA

HOW INTERNATIONAL (HUMANITARIAN) LAW INFLUENCES THE RULES OF ENGAGEMENT IN MILITARY CYBER OPERATIONS?

Bárbara Vieira Reis

Supervisor: Maria Isabel Cantista de Castro Tavares

Master's in law

Porto Faculty of Law

2024

ACKNOWLEDGEMENTS

Aos meus pais, Felisbela e António, sem eles nada disto seria possível. A todo o esforço, apoio e motivação que sempre me deram, de forma incondicional. Estarei sempre grata por todas as oportunidades que me facultarem, e por sempre me deixarem voar!

À minha irmã Camila, aquela que sempre esteve ao meu lado para me dar força, que sempre acreditou em mim mesmo nos momentos em que não me achei capaz, e que sempre me disse que tudo o que eu quisesse, era possível!

À minha querida avó Josefina, aquela que sempre acreditou que eu estava destinada a grandes feitos, que todos os dias me deu carinho e me motivou a seguir os meus sonhos, ainda que isso implicasse estar longe. Obrigada pela imensidade de amor, e pela força que me deste para superar todas as dificuldades!

Por fim, mas não menos importante, à Marta, uma das minhas melhores amigas, e aquela que mais me ouviu e motivou neste longo caminho. Estou muito agradecida por ter feito esta caminhada ao teu lado, e decerto que os nossos caminhos se vão continuar a cruzar!

ABSTRACT

This dissertation aims to investigate the influence of International Humanitarian Law on the Rules of Engagement, in military cyber operations.

Through a deductive methodology, it will be examined how legal norms apply and necessitate to adapt to rules of engagement, to address the challenges of cyberspace.

The study highlights the complexities of applying international principles, in a domain where civilian and military infrastructures often collide. It highlights the variableness in state practices and interpretations and suggests ways forward for enhancing coherence and compliance with international humanitarian law in cyber conflicts.

The motivation for addressing this topic relies on the increasing significance of cyberspace in modern warfare, which poses unseen legal and ethical challenges, and where significant achievements can be reached, and critical threats mitigated.

Keywords: International Humanitarian Law; Military Cyber Operations; Rules of Engagement;

RESUMO

Esta dissertação tem como objetivo investigar a influência do Direito Internacional Humanitário nas Regras de Empenhamento. em ciberoperações militares.

Através de uma metodologia dedutiva, será analisada a forma como as normas jurídicas se aplicam e necessitam de ser adaptadas às regras de empenhamento, de forma a fazer face aos desafios do ciberespaço.

Este estudo salienta também as complexidades da aplicação dos princípios de direito internacional, num domínio onde as infraestruturas civis e militares frequentemente coincidem. Salientar-se-á também a diversidade nas práticas e interpretações dos diferentes Estados, sendo sugeridos possíveis caminhos a seguir para reforçar a coerência e o cumprimento do Direito internacional humanitário nos ciberconflitos.

A motivação para abordar este tema assenta na importância crescente do ciberespaço na guerra moderna, o qual coloca desafios jurídicos e éticos nunca antes vistos, e onde ainda é possível alcançar resultados significativos e atenuar possíveis ameaças.

Keywords: Direito Internacional Humanitário; Operações Cibernéticas Militares; Regras de Empenhamento;

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AI - Artificial Intelligence

AJP - Allied Joint Publication

AP - Additional Protocol

CBMS - Capacity-Building Measures

CISO - Chief Information Security Officer

DDoS - Distributed Denial of Service

EU - European Union

GC - Geneva Conventions

GGE - Group of Governmental Experts

ICJ - International Court of Justice

ICRC - International Committee of the Red Cross

ICT - Information and Communications Technology

IHL - International Humanitarian Law

IL - International Law

IP - Internet Protocol

LOAC - Law of Armed Conflict

MCO - Military Cyber Operations

MS - Member States

NATO - North Atlantic Treaty Organization

OSCE - Organization for Security and Co-operation in Europe

ROE - Rules of Engagement

U.S - United States of America

UK - United Kingdom

UN - United Nations

VPN - Virtual Private Network

WEF - World Economic Forum

I. INTRODUCTION

This dissertation will address how International Law (IL), and mostly International Humanitarian Law (IHL) reflects and affects the creation and applicability of rules of engagement (ROE) in cyberspace operations.

The method used to carry out this study will be deductive, starting with an analysis of what already exists in the legal norms, and then delving into how ROE should be adapted according to IHL.

The concept of ROE will be deduced by the author of this paper after analyzing the definition used by the North Atlantic Treaty Organization (NATO) and the European Union (EU). However, it should be noted that ROE do not exist only in the context of military operations, but on the contrary are a constituent part of the entire process preceding each operation, constituting a key element to be developed from the strategic to the tactical level.

ROE are dependent on the type of operation that they are required for, as well as on the type of mandate they are given. While the ultimate objectives may be different, both IHL and ROE dictate the permissible conduct concerning the use of force in military operations. Consequently, some types of ROE reflect and are directly influenced by the corresponding rules of IHL. For instance, the case of ROE derived from the principles of distinction and proportionality, or others related to methods and means of warfare, as will be shown later in this paper.

While IHL applies to cyberspace operations, how each state applies it remains under their discretion. However, the application of IHL and the limits it imposes on ROE, raises problems in some areas of application, the grey areas. The application of IHL in cyberspace and its most significant flaws will also be part of our analysis.

The existing different perspectives and principles of IHL significantly influence the formulation of ROE by each state. These differences coupled with the nuances of cyberspace and existing *caveats*, dictate limits within each state's ROE. On the other hand, even though there is no standard applicable ROE to cyber, there is a lowest common denominator within the NATO countries, as will be shown.

This dissertation will also question whether such divergence in the formulation of ROE and its limits does not assume, in countries that belong to NATO and/or the EU, a

distancing and differentiation factor from the values defended by them, which formally share values and a common goal. Integrating the principles of IHL into ROE can capacitate member states (MS) of organizations like NATO and the EU with a set of similar guiding principles, especially since the standardization of ROE may not be a feasible solution given the general complexity of cyberspace and national *caveats*. These alternative offers flexibility to adapt to the various cyberthreats and operational scenarios, while also fortifying the groundwork for coherence in the interpretation and application of ROE in cyberspace.

An essential aspect not to forget during the development of this dissertation is the existence of the Martens Clause. Martens Clause determines that when facing cases not covered by any existing IL treaties, civilians and combatants are always protected under the general principles of international and customary law. These clauses ensure that fundamental humanitarian principles always act as protection in situations where legal norms are still developing, as they are in cyberspace and cyber-ROE, providing a moral framework that controls state conduct.

II. CYBER WARFARE: INTERNATIONAL LAW, RULES OF ENGAGEMENT AND EMERGING CHALLENGES

The rapid development of technology and the increasing interconnectedness of our modern society have given rise to a new frontier: cyberspace. This virtual realm transcends physical boundaries and has emerged as a platform for individuals, states, and organizations to engage in a diverse range of activities.

As the new reality continues to unfold, it has become increasingly clear that a legal framework is necessary to govern the behavior and actions of these players, in cyberspace[1]. To address this need, IL has been making efforts to apply it to this virtual sphere. Although there are currently no specific tailored rules that govern cyberspace[2], governments and international organizations have begun to recognize that existing IL must apply to this domain.

Several countries including the Netherlands[3], Germany[4], Estonia[5], and France[6] have already recognized cyberspace as a domain of operations in their military doctrines. These nations recognize the strategic importance of military cyber operations (MCO) and their implications for national security. These countries have begun establishing the foundation for cyber-ROE, as these military manuals show an understanding of the three constitutive components of ROE, and this initial first step is fundamental to facilitate the formulation of future comprehensive and robust cyber-ROE[7].

[1] Attacks on these infrastructures have the power to paralyze a country, disrupt electoral processes, and cause physical damage in infrastructures - reason why the World Economic Forum (WEF) rated cyber-attacks as the 7th risk that worsened the most since the start of COVID-19, with a 435% increase in ransomware in 2020.
[2] Except the Budapest Convention on Cybercrime.
[3] (Netherlands, Appendix: International law in cyberspace, 2019, p. 1).
[4] (Office & Defence, 2021, p. 1) and (Office F. F., 2020).
[5] (CCDCOE, Estonian contribution on how international law applies to the use of ICTs by states for part of an annex to the UN GGE (2019-2021) consensus report, 2021).
[6] (Armées, DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE CYBERESPACE, 2019).
[7] On the other side, the lack of recognition other countries, indicates a significant barrier to achieve a global harmonization of cyber policies.

In contrast, countries like Russia[8] and China[9] have not recognized cyberspace as a distinct domain of operations in their military doctrines. This demonstrates these nations view cyberspace with a different strategic lens[10].

The fact some countries include cyberspace in their military doctrines and others don't, underscores the complex nature of this domain, demonstrating the hesitance among certain nations to openly expose their cyber strategy due to the sensitive nature of MCO.

IL is crucial in establishing the regulatory environment of cyberspace yet, the quick rate of technical development as well as the difficulties of implementing laws across borders, have produced substantial gaps and obstacles in this field. The fundamental concerns involving the application of IL to cyberspace include state silence, interpretive obstacles, attribution, and lack of transparency. However, as a sign of development, some governments have begun to voice their opinions, and as we transition to a more detailed exploration of military rules, the topic applied to cyberspace will be examined.

It becomes imperative to have in mind how the current legal principles influence the formulation and application of specific military directives, such as ROE. The interconnection between IL and ROE highlights how the first adapts and applies within new military frameworks, emphasizing the need for and importance of aligning operational military strategies, with international legal principles in cyberspace.

Having a conceptual introduction to ROE is mandatory, as they are one of the means used to control all activities directly related to the use of military force, whether facing situations involving its effective use or just a threat or provocative action[11]. These directives reflect the political and military plans of a state and are a way to achieve national and international interests. It is important to note that, to act legally, the operations and tasks established for each mission cannot be more permissive than what is determined by the operation's ROE.

[8] (Excellence, 2021, pp. 5-7).
[9] (China, 2015).
[10] This approach can be found in their policy documents and international statements, where they advocate for strict controls within MCO.
[11] Examples of situations that constitute threats or provocative actions, in the traditional domain, are related to the use of weapons and identification of targets, or, in the case of provocative actions, to the deployment of forces or carrying out of exercises near the adversary's borders. In the cyber domain, a clear provocative action would be for a state to remotely access the military system of another state, without its consent, and exfiltrate classified information.

NATO and the EU have established a definition for this concept. For both[12], ROE are "directives to military forces (including individuals) that define the circumstances, conditions, degree, and manner in which force, or actions that might be construed as provocative, may be applied"[13].

Considering a certain legal conjecture, ROE are designed to help achieve political-military objectives and cannot be seen as a way of assigning tasks and/or giving tactical instructions.[14] The Commander in charge of the mission has the responsibility to ensure his subordinates acknowledge and understand the ROE attributed to the operation, and to avoid any doubt that may arise at a decisive moment.

Except in situations of self-defense, in times of peace or crisis management, ROE capacitates the forces in charge of the mission, with the authority to regulate the use of force[15]. This means that in times of peace ROE legitimizes the use of force[16], whereas in times of crisis management or armed conflict, they serve to limit it[17]. However, the use of force is obliged to respect the legal obligations imposed by IL, more specifically the rules applicable to IHL.

Despite that, this does not mean that MS loses their sovereignty since national legislation sets limitations or provides its instructions, *caveats*[18]. Each MS is allowed to determine how it will behave and whether it will follow the international organization's guidelines, while also complying with its national legislation. Such limitations or additional directions are permissible if they are not more permissive[19] than those approved for the operation that follows and respects IHL[20].

There is a general difficulty in adapting and applying the long and solidified rules of IL to the new hostilities revolving around the new methods and means of cyber warfare[21]. The fundamental nature of these rules requires them to be comprehensive and futuristic,

[12] (SERVICE, 2014, paragraph 34, point c).
[13] (NATO, 2003, p. 2, paragraph 2).
[14] (NATO, MC 0362/2 FINAL, 2019).
[15] (NATO, MC 0362/2 FINAL, 2019).
[16] (NATO, ATrainP-4: TRAINING IN NATO RULES OF ENGAGEMENT, 2022, pp. B-8).
[17] IBIDEM, p. B-9.
[18] (NATO, MC 362/1, 2003, p. 3, paragraph 5).
[19] (NATO, ATrainP-4: TRAINING IN NATO RULES OF ENGAGEMENT, 2022, pp. B-13).
[20] (Stinissen, Minárik, Pissanidis, Veenendaal, & Glorioso, 2015, p. 6).
[21] (Tulilahti, 2020, p. 30).

as they establish behavioral norms that will be employed in numerous unknown future scenarios.

To accomplish this, the law must not only define specific rules for all supposed circumstances that seem possible to arise with time[22]. Instead, they must also be comprehensive and adaptable to the new outcomes, while respecting their specific characteristics. Nevertheless, it may be more challenging to adapt to the ever-changing and unconventional nature of the cyber domain, which is uncertain and unpredictable, making it harder to apply IL effectively.

Facilitating the interpretation and application of IL to specific incidents (in this case, to the cyber domain) proves to be a more feasible task through the process of judicial interpretation carried out by national courts, coupled with legislative amendments[23]. However, because nations are motivated by distinct and frequently conflicting interests and motivations, the process of adaptation under IL is significantly more difficult. The process of establishing an international norm cannot be initiated by a singular state's legislature, as it requires the collective proclamation of willingness to adhere to such a norm by multiple governments, transforming it into customary law[24].

When concretely mentioning changes in IHL, it proves to be much more difficult. One of the main reasons is that IHL deals with complex and sensitive issues related to war and violence, which will evoke contrasting positions between states. As a result, reaching a consensus on how IHL should be applied, in specific situations can be challenging. When transferring to the cyber domain, even more challenges arise.

In addition, the foundational principles of IHL heavily rely on treaties that were established decades ago and may not adequately take into account the emerging forms of cyber warfare and the development of new types of cyber weaponry and tactics[25]. This results in a contextual and temporal gap between the formulation of legal norms and their (effective and necessary) implementation[26].

[22] (Diamond, Applying International Humanitarian Law to Cyber Warfare, 2014, p. 69).
[23] (Sachariew, s.d., p. 179).
[24] (ICRC, Customary International humanitarian law: questions & answers, 2005).
[25] For example, the Geneva Conventions which for the cornerstone of IHL were adopted in 1949, and despite have been amended over the years, they still do not fully address concerns such as cyberattacks and asymmetric warfare.
[26] (Diamond, Applying International Humanitarian Law to Cyber Warfare, 2014, p. 70).

It is essential to acknowledge the rapid advancement of technology and the consequences of it. The rising threats of cyber operations can jeopardize human well-being, thereby emphasizing the necessity of clarifying the appropriate application of basic key principles of IHL in cyberspace.

Traditional concepts like “military objective”, “attack”, and “armed attack” once seen, do not come closer to the same ones in cyberspace. The lack of clarity in such basic yet fundamental concepts makes it difficult to apply IHL frameworks to cyber warfare[27]. IHL was designed to apply to methods and means of warfare involving the use of physical force, in the physical world, which consequently reflects on the not-so-well adaptability to address hostilities in the context of cyberspace, where conflicts involve the manipulation of data[28]. Naming the actors involved in an attack[29], specifying the targets, and determining the real extent of caused damage[30], are also some other unique challenges that cyberspace presents to the application of IHL, as will be discussed later.

All these adversities result in a simple consequence: the non-enforcement and compliance of IHL, which turns out to have significant legal and technical difficulties.

Despite that, some ways could help minimize this problem. One of the solutions (and probably the easiest, if states would collaborate), is reinforcing a unified understanding of the constitutive terminology under which IL and IHL principles apply in cyberspace[31]. Once those basic concepts are clearly defined, it is easier to adapt or even create a legal framework. International collaborative efforts should be pursued with definitions under the auspices of an international and recognized body like the United Nations.

The author of this dissertation also defends the possibility of creating cyber-specific addends to the already existing treaties. As a matter of example, it could be introduced a New Additional Protocol to the Geneva Conventions on Cyber operations, which could outline specific protections to be granted to civilian data and objectives, and potentially define lawful cyber warfare tactics that comply with IHL.

[27] (Laurent Gisel, 2020, pp. 316-318).
[28] IBIDEM, pp.317-319.
[29] (ICRC, International Humanitarian Law and the challenges of contemporary armed conflicts Report, 2011, p. 36).
[30] (Laurent Gisel, 2020, p. 296).
[31] (Tulilahti, 2020, p. 29).

However, only continuing to create new legal frameworks may not be the most suitable long-lasting solution to address the evolving challenges in cyberspace and other domains that will eventually emerge. Instead, to complement these new frameworks and make them effective, it is necessary to establish mechanisms for periodic reassessment of these cyber laws and their application, to ensure they remain enforceable and relevant considering the overall advancements.

III. INTERNATIONAL LAW, CYBERSPACE, AND STATE'S POSITIONS

The intersection between cyberspace and IL leads to a fundamental question: how does IL apply and how do states navigate their rights, responsibilities, and interests within it?

States having an active or passive voice emerges as an essential factor when analyzing the government's viewpoints, on cyberspace legal frameworks. It allows for a more in-depth examination of the complex interaction between power dynamics and state positions, offering significant perspectives on the emerging environment of cyberspace governance, by showing how having an active or passive voice impacts the state's interpretation and execution of IL in the digital era.

The principal aspects that are going to be examined regarding their different positions, are the ones directly related to their behavior in cyberspace[32]. Thus, this comparative analysis will focus on sovereignty, due diligence, and non-intervention, safeguarding the knowledge of other existential controversial topics such as attribution, countermeasures, the use of force, and self-defense.

a. SOVEREIGNTY

The subject of sovereignty in cyberspace is a complicated and multidimensional concept, characterized by a wide range of viewpoints that each country addresses through the lens of its unique objectives, national interests, and historical background. Consequently, cultural norms, legal frameworks, and geopolitical factors all influence their attitude toward the concept.

[32] (Roguski, 2020, p. 4).

The notion of sovereignty is mostly based on customary law[33] however, it is established in several international legal documents and treaties[34], including the United Nations Charter[35] (UN Charter) which forces states' cyber operations to respect it[36].

Despite not being clearly defined as a separate principle in the text of the Geneva Conventions (GC), it is indirectly recognized in Article 2 of the IV GC, which upholds the concept of territorial integrity by recognizing the applicability of the Convention inside the state's borders, independent of other parties recognition[37].

Sovereignty is a basic tenet of IL that defines interactions between sovereign states, and it is historically connected with the state's authority and control over its territory[38]. However, since sovereignty might be interpreted and utilized differently in the context of cyberspace (in part because cyberspace transcends physical borders), that can generate doubts on how traditional concepts like sovereignty, are interpreted in the digital environment[39].

Among the various viewpoints expressed by different states, it is important to note the existence of two different approaches: sovereignty interpreted as a principle, from which some prohibited rules derive[40], not constituting a primary rule of IL; and sovereignty as a rule, where states are obligated to respect another state's sovereignty (territorial or digital), otherwise would be committing an international wrongful act.

The vast majority of the EU MS seems very unified in this matter, mainly because AJP-3.20 mentions sovereignty as a rule, and as a consequence, that reflects the position of the more than thirty MS belonging to NATO[41].

---

[33] (CCDCOE I. G., 2017, rule 1, paragraph 3).
[34] Vienna Convention on the Law of Treaties and International Covenant on Civil and Political Rights.
[35] According to article 2, number 1 of the UN Charter, "the Organisation is based on the sovereign equality of all its members."
[36] (UN GGE REPORT, 2015, paragraph 27).
[37] (ICRC, IV GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIMES OF WAR, 1949).
[38] (Tsagourias & Buchan, Research Handbook on International Law and Cyberspace (2nd edition), 2021, pp. 12-13).
[39] IBIDEM, p.14, "(…) the lack of borders in cyberspace deprives sovereigns of the ability to exercise their power over defined peoples and territories and deprives sovereign power from the legitimising effect of consent."
[40] Non- intervention and prohibition of the use of force.
[41] (NATO, Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations, 2020, p. 20, note 26).

For example, the United Kingdom places significant emphasis on responsible state behavior and compliance with IL[42], notably on the principles of territorial integrity and non-intervention[43]. For them, sovereignty is merely seen as a principle, which results in contending that any limitation on state activities, whether in cyberspace or elsewhere, should be explicitly defined either through customary IL or through a treaty binding on the parties involved[44].

From China's position, it is easily concluded the emphasis is given to the principle of exclusive national sovereignty in cyberspace, and the importance of advocating for its authority to regulate and govern activities within its borders[45]. China embraces the notion of cyber sovereignty as part of its strategy, claiming its power and jurisdiction over cyberspace inside its boundaries[46], contrary to what is defended by the Group of Experts on the Tallinn Manual, which agreed that "no State may claim sovereignty over cyberspace"[47].

Similarly[48], Russia places immense importance on the notion of exclusive national sovereignty in cyberspace, claiming the right to govern and control online activity within its borders[49]. The government has been vocal about the significance of retaining state control over the flow of information and has enacted a variety of internet limitations and monitoring measures to that end[50].

The United States of America's (U.S.) position remains a bit unclear. However, they affirm that state sovereignty must be considered in the conduct of cyberspace operations, and when a state considers undertaking actions in cyberspace, it must respect other's equal sovereignty[51].

---

[42] Regarding NotPetya, the UK along with the U.S., attributed the cyberattack to Russia, stating that it violated the principle of sovereignty and, consequently IL.
[43] (UK Foreign, 2021, paragraphs 8-10).
[44] IBIDEM, paragraph 10.
[45] (Creemers, 2020, p. 7).
[46] (China, 2015).
[47] (CCDCOE I. G., 2017, rule 1, paragraph 7).
[48] China and Russia have explored deeper cyber cooperation through initiatives such as the "Bilateral Cooperation Mechanism on Cyberspace". Their mutual ideals on exclusive national sovereignty and control over cyberspace is shown in their partnership.
[49] (Giles, 2012).
[50] (Excellence, 2021, p. 12).
[51] (Assembly, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Expert, 2021, p. 139).

On the other hand, France[52], Estonia[53], The Netherlands[54], Germany[55] , and the Czech Republic[56], among others[57], defend sovereignty as a rule that entails rights and obligations, and when violated, either by a cyber operation or any kinetic way, they will likely be classified as an internationally wrongful act.

However, despite the most common agreement on seeing sovereignty as a rule, when looking further at the actual application of the concept to cyberspace, there are clear differences between these states - their position differs when determining whether a cyber operation may be classified as a violation of another states' sovereignty.

In cyberspace, according to the Group of Experts of the Tallinn Manual, a violation of sovereignty occurs when a state conducts a cyber operation that disrespects or neglects, another state's sovereignty[58]. Despite being clear that a cyber operation that has large and catastrophic repercussions similar to a traditional armed attack or use of force against a state, would be classified as a breach of sovereignty, the picture becomes more obscure with less intense cyber operations, in whose there is still no agreements on the criteria and threshold that would qualify those, as a sovereignty violation[59].

In this matter, the Tallinn Manual provides valuable insights to evaluate the criteria of possible sovereignty violations in cyberspace. According to it, death[60], injury[61], physical damage[62], loss of functionality[63], and interference with governmental functions[64] are some of the factors to consider when assessing a possible sovereignty infringement.

However, one thing not mentioned in the manual is the threshold for determining sovereignty violations, leaving room for different national positions, as will be seen further. This ambiguous threshold shows the importance of recognizing that sovereignty

[52] (Toolkit, s.d.).
[53] IBIDEM.
[54] IBIDEM.
[55] IBIDEM.
[56] IBIDEM.
[57] IBIDEM.
[58] (CCDCOE I. G., 2017, p. 17, rule 4).
[59] Some countries need tangible effects or impediments, whereas others view factors such as loss of functioning, interference with governmental functions, or any cyberattack attributable to a state, to constitute violations of sovereignty.
[60] (Tsagourias & Buchan, Research Handbook on International Law and Cyberspace (2nd edition), 2021, p. 22).
[61] IBIDEM.
[62] (CCDCOE I. G., 2017, rule 4, paragraph 11 and 12).
[63] (CCDCOE I. G., 2017, rule 4, paragraph 11).
[64] IBIDEM.

violations in cyberspace go beyond physical harm, impacting national norms and internal state rights and interests.

Countries that stand for a lower threshold are adept at the penetration-based approach, asserting that any intrusion of computer networks within a state's jurisdiction, undermines their sovereignty[65]. This perspective shows the importance that certain countries attribute to some cyber operations beyond the tangible effects, evaluating any unauthorized intrusion as a significant violation of their sovereignty.

In this matter, seems important to highlight France's position. France has a very firm stance on digital sovereignty. They claim jurisdiction over information systems, associated objects, and material operated or processed through electronic communication networks within their jurisdiction[66]. They also define cyberattacks and consider any cyberattack attributed to a state to constitute a breach of sovereignty, even if it fails or does no harm[67].

While some argue that having a low threshold is imperative to prevent attempts to diminish sovereignty and facilitate conflict escalation, others contend that because of the different interpretations and importance given to this principle, their approach is *minimis*.

The *minimis* approach declares that while conducting cyber operations, the sovereignty of other states must be maintained, but there is a *de minimis* threshold for cyber activities that must be crossed for them to be identified as a breach of sovereignty[68].

This is the position advocated by the Tallinn Manual[69] and the Netherlands[70], defending that not all breaches automatically constitute a violation of sovereignty, but only those with a certain degree of infringement on the target State's territorial integrity, or by interfering with or usurping inherently governmental functions[71].

From the discussion above, it's clear that trying to determine the meaning and extent of sovereignty is very complicated. The divergence of perspectives and values of each country, except regarding fundamental core sovereignty aspects, highlights the need to

[65] This is the position of states like France, Russia and China.
[66] This means that France's jurisdiction extends over data centers, servers and all digital material created within its borders, respectively.
[67] (Armées, p. 6, paragraph 1.1.1).
[68] (Roguski, 2020, p. 4).
[69] (CCDCOE I. G., 2017, rule 4, paragraphs 10-11).
[70] (Netherlands, Letter to the parliament on the international legal order in cyberspace:, 2019, p. 3).
[71] (CCDCOE I. G., 2017, rule 4, paragraph 10).

assess whether there has been a violation, on a case-by-case basis. However, comprehending cyber sovereignty remains the basis for exploring other principles of IL, as due diligence, since sovereignty imposes "rights upon States and imposes obligations on them"[72] as will be seen.

b. DUE DILIGENCE

The term "due diligence" has recently received a lot of traction in the cyber world. This interest in the topic derives from the ongoing difficulties in precisely and legally attributing hostile cyber actions, to specific actors.

The use of anonymizing and rerouting techniques, such as VPNs and IP spoofing software, has compounded the issue of attribution even more[73]. These considerations have resulted in a complicated environment, in which establishing the origins of cyber-attacks is extremely challenging. To face these rising cyber threats and uncertainty, the concept of due diligence appears as a possible avenue for establishing responsibility, peace, and security in cyberspace.

Essentially, due diligence requires nations to make efforts to avoid, mitigate, and rectify any expected cyber damage that may originate from, or pass through their territory. States would be defenseless against cyber-attacks originating in foreign places if this requirement did not exist, especially in circumstances where establishing state culpability becomes difficult. As a result, nations are expected to make reasonable efforts, considering their national capabilities and access to information, to guarantee that their territory is not used for damaging cyber activities[74].

However, while the notion of due diligence may seem an obvious and straightforward obligation for all states to adhere to, diverse views exist regarding the nature of this principle[75].

On one side of the debate, the 2015 report of the Group of Governmental Experts (GGE), sustains that states "should not conduct or knowingly support ICT activity

[72] (JUSTICE, Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania), p. 43). As an example, the obligation to terminate harmful cyber activities that are being conducted from a state's territory.
[73] (Buchan, 2016, pp. 430-431).
[74] (EU, 2020, "The European Union and its Member States call upon every country to exercise due diligence and take appropriate actions against actors conducting such activities from its territory, consistent with international law (…) in the field of Information and Telecommunications in the Context of International Security.)"
[75] ((UNIDIR), 2021, p. 1).

contrary to its obligations under IL"[76].
This clearly defines due diligence as a "voluntary, non-binding standard"[77], regarding responsible state behavior in cyberspace.

Contrastingly, the experts of the Tallinn Manual presented a different viewpoint, asserting that a broad norm or concept equivalent to due diligence already exists within customary IL. This norm requires a state to "exercise due diligence in not allowing its territory, or cyberinfrastructure under its governmental control, to be used for cyber operations that infringe on the rights of other states and result in significant adverse consequences"[78]. For them, the principle of due diligence derives from existing IL[79] and centers on the state's responsibility not to knowingly allow its territory to be exploited for activities that violate the rights of other states[80].
This commitment relies on the principle of sovereignty, granting a state exclusive authority over its territory, while simultaneously imposing a duty to intervene when its territory is used in a way that violates the rights of others.

Examining different countries' positions on due diligence applied to cyberspace, starting with the U.S., their approach revealed to be very cautious in considering due diligence a general obligation under IL, not having identified any specific state practice and *opinio juris*[81].
Despite only recognizing due diligence as a concept with a significant role in the realm of international relations, with no establishment and binding obligation to which states are inherently bound to adhere when facing harmful activities that arise from their territory, the U.S. has a clear approach.
In their view, when a State is made aware of those potentially harmful acts, it is responsible for taking reasonable and acceptable steps to reduce, face, and prevent any additional harm[82].

[76] (UNIDIR, 2019, p.3, paragraph 13 (f)).
[77] (Antonio Coco, 2021, p. 773).
[78] (CCDCOE I. G., 2017, rule 6).
[79] (Library, 2015, p. 8, paragraph 13, c).
[80] IBIDEM, paragraph 28 (e).
[81] (Assembly, Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Expert, 2021, p. 141).
[82] (CCDCOE, CyberLaw Toolkit, s.d.).

In alignment with the U.S., countries like Israel[83], New Zealand[84], the UK[85] , and Canada[86], also consider due diligence a voluntary and non-binding principle, even though stressing the necessity of taking proactive actions to counter harmful acts that originate on their territory or fall under their authority. Nevertheless, these positions acknowledge and promote responsible state behavior, as established in the 2021 UN GGE report[87].

On the other side, following the Tallinn Manual's approach and emphasizing that the principle of due diligence is an obligation of conduct[88], this view has been gaining some followers among States like Estonia[89], Finland[90], France[91], Germany[92], and the Netherlands[93].

According to the Corfu Channel principle, there is a requirement that states need to fulfill - their territory is not being intentionally used for activities that constitute violations of other states' rights[94].

However, there appears to be an extensive amount of ambiguity and inconsistencies surrounding the legal basis, content, and scope of due diligence within cyberspace. As already mentioned, this duty derives from the state's sovereign rights over its territory, creating the obligation to protect the rights of other states therein[95]. This obligation emerges as soon as the state becomes aware, or should be aware, that

[83] (Schöndorf, 2020, p. 404, "However, we have not seen widespread State practice beyond this type of voluntary cooperation, and certainly not practice grounded in some overarching opinio juris, which would be indispensable for a customary rule of due diligence, or something similar to that, to form").
[84] (Trade, 2020, p. 3, "An agreed norm of responsible state behaviour provides that states should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. Whether this norm also reflects a binding legal obligation is not settled").
[85] (Office, 2011, "The UK recognises the importance of States taking appropriate, reasonably available, and practicable steps within their capacities to address activities that are acknowledged to be harmful in order to enhance the stability of cyberspace in the interest of all States. But the fact that States have referred to this as a non-binding norm indicates that there is not yet State practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace.")
[86] (Canada, s.d., "Canada does not consider that the UN GGE consensus in 2015, and subsequently, on voluntary, non-binding norms touching on this matter precludes the recognition of a binding legal rule of due diligence under customary international law. Canada continues to study this matter.")
[87] (Assembly, Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2021, p. 10, paragraph 30, a).
[88] (CCDCOE I. G., 2017, rule 6, "A State must exercise due diligence in not allowing its territory (…))"
[89] (CCDCOE, National position of Estonia, 2021).
[90] (Affairs, 2020, pp. 4-5, "States have an obligation not to knowingly allow their territory (…))"
[91] (CCDCOE, National position of France, 2019).
[92] (CCDCOE, National position of Germany, 2021).
[93] (Netherlands, 2019, p. 4, "The Netherlands, however, does regard the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act.")
[94] (ICJ, 1949, p. 22).
[95] (ICJ, 1949, p. 22,"and every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.".)

those acts are coming or passing through their territory[96]. However, a breach of this obligation only occurs when the harm happens, existing no penalty for non-compliance until then[97].

To adapt the Corfu Channel to cyberspace, the Tallinn Manual created Rule 6, which outlines the key elements that characterize the formulation of this obligation in cyberspace (type of harm[98], followed by the threshold of harm[99], the scope of preventive duties[100] , and the requirement of knowledge[101]).

However, the Manual does not clearly define "serious adverse consequences"[102], leading to a certain ambiguity around the threshold for triggering due diligence obligations and around these previously mentioned key elements.

To better comprehend these implications, the manual mentions that “merely affecting the interests of the target State, as in the case of causing inconvenience, minor disruption, or negligible expense, is not the type of harm envisaged; thus, not every use of a state’s territory that produces negative effects for a target State implicates the due diligence principle"[103]. We can consequently conclude that “serious adverse consequences” refer strictly to substantial disruptions or damages caused by cyber operations, including economic impacts, threats to national security, and harm to public health and safety. And so, only effective disruptions or damages will likely qualify under this rule, leaving the ones with fewer impacts outside of this scope[104].

To further complicate the application of this principle in cyberspace, the manual argues against a requirement for states to take preventative measures, "given the difficulty of mounting comprehensive and effective defenses against all possible cyber threats it would be unreasonable to assert that an obligation of prevention exists in the cyber context"[105] and such a requirement “would impose an undue burden on states”[106].

[96] (CCDCOE I. G., 2017, rule 6, paragraph 8).
[97] (CCDCOE I. G., 2017, rule 6, paragraph 17).
[98] (CCDCOE I. G., 2017, rule 6, paragraph 26).
[99] (CCDCOE I. G., 2017, rule 6, paragraph 25).
[100] (CCDCOE I. G., 2017, rule 7, paragraph 8).
[101] (CCDCOE I. G., 2017, rule 6, paragraphs 37-39).
[102] (CCDCOE I. G., 2017, rule 6, paragraph 25).
[103] (CCDCOE I. G., 2017, rule 6, paragraph 26).
[104] (CCDCOE I. G., 2017,rule 6, paragraph 26, “The cyber operation has not caused sufficient harm to render the territorial State in violation of this Rule should it not engage in measures to put an end to the activity”)
[105] (CCDCOE I. G., 2017, rule 7, paragraph 8).
[106] IBIDEM.

This perspective suggests that while states are expected to be proactive, the burden of achieving absolute cyber capabilities is unreasonable.

Addressing key questions such as whether due diligence acts as a fundamental principle or a guiding standard in particular contexts, defining its specific duties, determining appropriate responses and actions, and highlighting the necessary measures for nations to diligently operate in cyberspace, is still a central concern[107].

Nonetheless, if states consider integrating capacity-building initiatives and confidence-building measures (CBMS), it is possible to fight the challenges of due diligence enforcement in cyberspace, while ensuring the respect of IL. This strategy makes it possible to manage the transnational nature of cyber threats and enhances international collaboration and trust[108].

CBMs build trust and transparency among parties involved in cyberspace activities. The Organization for Security and Co-operation in Europe (OSCE) implemented a series of Cyber CBMs that are characterized by exchanging information on national cyber strategies and regular discussions among the MS[109], making the risk of cyber incidents lower. These measures are also pivotal in helping prevent misunderstandings and misattributions of cyber incidents, which are most of the time a big part of international friction[110]. Fostering this open environment and communication turns the CBMS into a support to the due diligence principle, by encouraging states to share relevant information and cooperate on cyber mitigations.

Parallel to CBMs, Capacity-building initiatives also play an essential role, particularly by developing the capabilities of less developed nations who struggle the most in fulfilling their due diligence duty.

Developed nations can provide technical support, and training and even share their best practices[111]. This collaboration not only contributes to global cybersecurity but also provides more capable cyber capacities to nations that are not as well equipped

[107] ((UNIDIR), 2021, p. 21).
[108] (York, 2023).
[109] (Europe O. f.-o., 2023, p. 4).
[110] (York, 2023).
[111] (CCDCOE, OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection, s.d.).

technologically, reducing their vulnerabilities and making it easier for them to prevent, detect, and respond to cyber threats, as required by the principles of IL.

c. NON- INTERVENTION

The concept of non-intervention is a crucial foundation in the complicated realm of IL, encapsulating the essence of sovereignty and territorial control. This principle prohibits both individual states and groups of states, from engaging in direct or indirect interference, in the internal or external affairs of another sovereign state, according to the Nicaragua case[112].

Despite its apparent importance, the practical implementation of this concept has frequently been hampered by ambiguity and repeated violations. The requirement for non-intervention in the international system is evident, intending to foster the peaceful coexistence of independent states. However, this principle's clarity and obedience have not always matched its apparent importance.

On the surface, this concept appears to be an appealing approach to dealing with cyber threats. However, following a greater examination, multiple weaknesses become apparent, making it an extremely problematic one. Could the appeal of intervention as a method of gaining worldwide influence be too much to resist in the intensely competitive field of global politics?

The Nicaragua case established a rigorous standard for classifying external interference as an unlawful intervention. For the interference to satisfy these criteria, it must concern topics that are exclusively within the *domaine réservé*, the area in which each state is granted the right to make autonomous judgments, according to its sovereignty[113]. Nevertheless, to classify an action as a violation of this principle, it is not enough that only the *domaine réservé* requirement, is respected.

It is also mandatory to use coercive means that intend to affect sovereign decisions[114]. Potential coercive measures include the direct use of military force[115], economic

[112] (Justice, 1986, p. 88, paragraph 205).
[113] IBIDEM, "A prohibited intervention must accordingly be one bearing on matters in which each State is permitted, by the principle of State sovereignty, to decide freely."
[114] IBIDEM, "Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones."
[115] An example is the USA invasion to Iraq in 2003.

sanctions[116] , propaganda campaigns[117], or any other actions that aim to compel the state to change its policies or actions.

Owing to this dual criterion, numerous cyber operations escape classification as interventions. Consequently, a void is created, allowing for the occurrence of low-intensity cyber operations and attempts to exert influence, without any consequences or accountability.

From this author's perspective, a decisive challenge arises from the lack of precise definitions for the key concepts of "domain réservé", and "coercion", and their associated methods. The presented definitions seem unsuitable when contemplating the features of the cyber environment, as they were originally conceived for application in a physical space.

The Tallinn Manual also emphasizes the significance of addressing the use of inconsistent language to refer to this principle[118]. Frequently, states, the UN, and some judgments from the International Court of Justice (ICJ) employ the term "interference" rather than "intervention", despite the nuanced distinctions in their meanings and the resulting legal consequences[119]. It is necessary to clarify the differences between the aforementioned terminology, to address the current ambiguity and its frequent misapplication. As so, to avoid any more uncertainty, the author believes that it is imperative to define all these concepts, starting with interference and intervention.

Our interpretation adheres to the definitions provided by the Tallinn Manual[120]: interference refers to "acts by States that intrude into affairs reserved to the sovereign prerogative of another State but lack the requisite coerciveness". On the other hand, "acts of interference with a sovereign prerogative of another State that has coercive effects" are the sole acts that qualify as intervention.

The idea of *domaine réservé* refers to areas in which states enjoy freedom from international obligations and regulations[121], particularly concerning their internal affairs.

[116] An example is the EU, UN and USA's sanctions against Iran for its nuclear program.
[117] An example is the systematic international campaign of media, information manipulation, interference and distortion of facts that has been done by Russia, to justify and support its aggression against Ukraine.
[118] (CCDCOE I. G., 2017, p. 313, rule 66, paragraph 3).
[119] IBIDEM.
[120] (CCDCOE I. G., 2017, p. 313, rule 66)
[121] (Ziegler, 2013, paragraph 1).

However, the determination of a state's *domaine réservé* can be difficult as its full contours can only be distinguished after a detailed examination of each state's practice, *opinion juris*, and different international commitments, which requires a difficult, ongoing, and time-consuming assessment, as it evolves with time[122].

However, following this, almost unbearable assessment and identifying if a given field is within a state's jurisdiction—that is if it falls in its *domaine réservé*—becomes a possible exercise. This clarification provides other states with the knowledge that it is not permitted for them, to intervene in such matters.

Usually, the *domain réservé* encompasses matters related to the formulation of political, economic, social, and cultural rules[123]. However, in the current state of the international order, many of these questions have been pulled out of the state's reserved domain[124], making the previously mentioned task of assessing its practices, more difficult and unpredictable.

For instance, as legal procedures enforcing specific free-trade agreements have been established, the government's freedom to make independent economic decisions has decreased[125]. Even in the realm of electoral processes, historically considered a core aspect of each state's *domaine réservé,* some international agreements have been forged[126], further blurring the boundaries of exclusive state authority, and of the concept. If these domains are no longer within the exclusive *domaine réservé*, then even the most extreme forms of interference in the political or economic affairs of another state, may not qualify as prohibited interventions.

Furthermore, not all intrusions into a state's *domaine réservé* are considered violations of the prohibition of intervention, and so, the term "coercion" is also difficult to adapt to the age of technology, being frequently misinterpreted[127]. As previously mentioned, such an intrusion must entail the use of coercive measures to be considered one[128].

[122] (Ziegler, 2013, p. 2, paragraph 2).
[123] (Justice, 1986, p. 88, paragraph 205).
[124] (Ziegler, 2013, p.3, paragraph 3).
[125] (Moulin, 2020, p. 431).
[126] For instance, electoral rights of citizens are protected under Article 25 of the International Covenant on Civil and Political Rights.
[127] Mainly with the concepts like persuasion, propaganda or mere influence. (Moulin, 2020, p. 439) (CCDCOE I. G., 2017, pp. 318-319, paragraph 21).
[128] (CCDCOE I. G., 2017, p.317, paragraph 17).

Adding to the confusion on what "coercion" means and how to use it, the definition in the Nicaragua judgment when mentioning "methods of coercion"[129], raises more questions and creates more ambiguity around the concept, specifically considering the term is not defined in IL[130].

There is also a divergence of opinions on whether intention is a prerequisite for an act to be classified as coercion. In the Nicaragua case, the stance taken was that having the intention to put change or put pressure, is sufficient for that act to be classified as coercion[131].

Two opposing views were emphasized by the experts in the Tallinn Manual, the dominant view being that "the coercive endeavor must be meant to affect the results in or conduct concerning, an issue reserved to a target State"[132]. They did, however, agree that an act does not need to be physical to be considered coercive thus, it is important to keep in mind that a cyber operation does not automatically qualify as a breach of the principle of non-intervention, just because there are no tangible repercussions from it[133]. Therefore, coercion is not a result-based strategy, and whether coercive methods are successful or not, does not affect how they are classified.

Nevertheless, this absence of well-defined core concepts around "coercion" in IL poses a challenge, making it difficult to ascertain definitively whether a violation of the principle of non-intervention has occurred.

Consequently, under Thibault Moulin's perspective, a new understanding of coercion must be developed, particularly regarding its restrictions in the digital sphere[134].

However, rethinking the meaning of coercion is always a sensitive process, and it is important to be cautious about oversimplifying this idea since doing so, might compromise the foundation of interstate relations. Governments are likely to use the intelligence gathered from cyber espionage activities to influence other governments'

[129] (Justice, 1986, p. 88, paragraph 205).
[130] (CCDCOE I. G., 2017, p. 317, paragraph 18).
[131] (Justice, 1986, p. 103, paragraph 241,"(…) if one State, with a view to the coercion of another State, supports and assists armed bands in that State whose purpose is to overthrow the government of that State, that amounts to an intervention by the one State in the internal affairs of the other, whether or not the political objective of the State giving such support and assistance is equally farreaching.")
[132] (CCDCOE I. G., 2017, p. 322, paragrap 29).
[133] (Justice, 1986, p. 123, paragraph 292 (3)).
[134] (Moulin, 2020, p. 443).

negotiating tactics and decision-making to suit their objectives, and states that have been the target of cyberattacks or cyber espionage, are also likely to modify their external and internal policies, either to mitigate the harm that has been done or to prevent similar incidents in the future.

On the other hand, if we equate "coercion" with "attempts at influence" or with "prompting a reaction from another state", any negotiation or process that places a foreign state, in a position requiring a change of stance, could potentially be categorized as prohibited interventions[135]. Given that influence is a common aspect of international relations, there is a risk that a significant portion of interstate interactions might be considered unlawful.
Then, a limit between the lawful influence and the unlawful constraint is needed and should be determined in a case-by-case analysis[136].

The author follows Moulin's approach and defends that in a digital context, coercion can be conceptualized as "a deprivation of control, resulting from the deliberate actions of another state, as evidenced prima facie by the characteristics of the malware employed."[137]

In conclusion, given the importance of non-intervention in IL emphasizing state sovereignty and territorial integrity, it is important to work on achieving a refined framework that can distinguish between lawful influence from unlawful coercion, that also defines core concepts as "coercion" and "intervention", and at the same time maintain the integrity of international relations.

Cyber operations further complicate the application and clarity surrounding this principle, and so, ultimately, the main objective is to balance state sovereignty with the modern emerging threats, which requires an update on the definitions and criteria presented in the traditional warfare realm.

[135] IBIDEM, p.444.
[136] ((Switzerland), 2009, p. 204, paragraph 3.3.1, "Toutefois, la limite entre l'influence, qui est licite, et la contrainte, qui est interdite, ne peut pas être fixée en général, mais doit être établie sur la base d'une appréciation au cas par cas.")
[137] Experts frequently find that the malware used in a cyberattack, is crucial in understanding the purpose of the attack.

IV. THE SYNERGY AND CONSTRAINTS OF INTERNATIONAL HUMANITARIAN LAW IN MILITARY CYBER OPERATIONS

The essential elements of war, such as widespread physical devastation, intense violence, and obliging one party to another's political will, are frequently absent in cyber warfare[138]. However, nowadays the use of cyber capabilities alone is not considered war, and it is a common element of almost all contemporary military confrontations.

The expression “military cyber operations” defines a “sequence of coordinated actions with a defined military purpose in cyberspace, requiring cyber capabilities”[139].

IHL is guided by principles such as necessity, humanity, distinction, and proportionality, which aim to mitigate unnecessary damage and suffering and provide protection to civilians and certain categories of objects and persons. These principles are particularly relevant during the drafting of ROE and in the planning phase of MCO, as it is in this phase that decisions regarding the means, methods, impacts on involved parties, and goals of the operation, are determined.

IHL aims to protect certain persons and objects during armed conflicts, whether international or non-international in character, by restricting the means and methods of warfare used[140]. Established on the 1949 Geneva Conventions and their Additional Protocols (AP), the Hague Conventions, and other treaties governing military action in times of conflict. IHL, also known as "*jus in bello*", governs only the humanitarian elements of conflict and is distinct from "*jus ad bellum*", which governs the problems preceding military intervention and the decision-making process that leads to it[141].

In the national and foreign context, the legality of the use of force, and thus the legitimacy of the military action, play a dominant part. As a result, conflicts must adhere to the legal principles implicit in these situations, and despite the state's differences in the application and interpretation of IL, as well as the obligations to which one commits oneself, these rules derived from international agreements are generally accepted by the majority and are considered the legal basis at the international level.

---

[138] (Rid, 2011).
[139] (CCDCOE, 14th International Conference on Cyber Conflict: keep going, 2022, p. 184).
[140] (Tsagourias & Morrison, What is International Humanitarian Law?, 2023, p. 20).
[141] IBIDEM, p.57.

Because most countries are obligated by the Geneva and Hague Conventions, all states have a responsibility to guarantee that IHL is followed[142], and nations are obliged to train their forces according to established rules and limits[143], as well as be guided by the principles of this and other applicable international provisions[144], such as human rights law[145]. Cyber operations are no exception and must also comply with the principles and rules of IHL.

According to the International Committee of the Red Cross (ICRC), IHL restricts cyber activities during an armed war, as well as the use of specific weapons, means, and methods. However, it should be emphasized that applying IHL to cyber activities, does not justify the use of force, whether kinetic or cyber, under the UN Charter, Article 2(4)[146], and all international disputes should be settled by peaceful means in whatever area[147].

a. PRINCIPLE OF DISTINCTION

The principle of distinction applies to cyberspace, is regarded as the cardinal and unyielding[148], and is one of the foundations of IHL, showing who and what can be targeted, during an armed conflict. This principle governs the level of security given to each target based on their category and as a result, it is decided who and what is a legitimate target, and who can actively engage in hostilities and profit from protected status if captured.

As codified in Articles 48, 51(2), and 52(2) of the AP-I[149], civilians must not be attacked, and the parties engaged in the conflict must always distinguish between the civilian populace and combatants. Protocols II and III also prohibit such attacks, and anyone who does not act in compliance with these rules and deliberately orders an attack against the civilian population, is accountable for a war crime, according to the International Criminal Court's Statute[150].

---

[142] (Djukić & Pons, 2018, p. 57).
[143] IBIDEM, p.60.
[144] (NATO, ATrainP-4: TRAINING IN NATO RULES OF ENGAGEMENT, 2022, pp. B-12).
[145] (Djukić & Pons, 2018, pp. 81-82).
[146] (NATIONS, s.d.).
[147] (NATIONS, article 2(3)"All Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.")
[148] (ICRC, ICJ, Nuclear Weapons Advisory Opinion, 1996, paragraph 78).
[149] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I)).
[150] (PORTUGUES, article 8, number 2 (b).

But who exactly is considered a civilian? According to customary law[151], civilians are described negatively, being those who are not members of the Armed Forces or part of a *levée en masse*[152], as per Article 50 paragraph 1 of AP-I[153]. Such an approach is also implicit in the GC and the Tallinn Manual[154].

However, in the realm of cyber operations, applying the principle of distinction poses unique challenges. The interconnected nature of cyberspace and the dual-use nature of many technologies make it difficult to differentiate between civilian and military targets[155], and many civilian infrastructures such as energy grids or communication networks, also serve critical military functions.

In cyberspace, traditional markers of distinction, such as uniforms or insignias, are often absent. Therefore, alternative methods for identifying legitimate military targets must be developed, considering factors such as the function of a system or network within military operations[156].

Like so, the only targets permissible under IHL while planning and carrying out cyber operations are military objectives, "objects which by their nature, location, purpose or use make an effective contribution to military action and whose partial or total destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage"[157]. Thus, computers or computer systems that contribute effectively to concrete military operations, fulfill these requirements.

However, cyberspace attacks may not be aimed at computer systems used solely in civilian locations, and due to the characteristics of this domain, some changes and gaps must be established. It is meant to safeguard citizens[158] from the effects of hostilities, and, as in traditional battling, the distinction between civilians and soldiers[159], must be

[151] (ICRC, International Humanitarian Law Databases, s.d.).
[152] In case of doubt about the person status, that person must be considered a civilian.
[153] (CCDCOE I. G., 2017, rule 87 and 88).
[154] IBIDEM, rule 93.
[155] IBIDEM, rule 100.
[156] The International Committee of the Red Cross's (ICRC) "Digital Emblem" proposal is one suggested remedy. As a recognizable symbol of neutrality and safety in the digital sphere, the Digital Emblem acts as a virtual equivalent to the real Red Cross emblem. To protect vital services and stop cyberattacks on civilian infrastructure, humanitarian actors and protected entities can use a Digital Emblem to declare their intentions and make use of the protections provided by IHL in cyberspace.
[157] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I), article 52 (1)).
[158] (CCDCOE I. G., 2017, rule 94.).
[159] IBIDEM, rule 93.

maintained, with indiscriminate attacks kept being prohibited[160]. Furthermore, because most developed countries use these cyber operations to provide important services to their citizens, such as water supply, energy, and communications, it is difficult to implement the principle of distinction strictly due to the dual use of certain facilities.

Even though the current landscape evolution of cyber operations presents an ongoing challenge in discerning between the two[161], this dichotomy remains unchanged, however, when confronted with a service that serves dual functions, that same one should be regarded as a military objective[162].

In response to these challenges, policymakers, legal experts, and military strategists must engage in collaborative efforts to refine the application of the principle of distinction in cyberspace. This entails the development of frameworks and guidelines that promote compliance with IHL while effectively addressing the unique complexities of cyber operations.

This author proposes a major focus on enhanced cyber intelligence and surveillance capabilities[163], as that would result in the improvement of identifying and distinguishing between civilian and military targets in cyberspace. Having this enhanced situational awareness will minimize the risk of unintended harm that military forces may cause to civilian infrastructure and non-combatant populations.

Making technological innovation a priority is also a way to make cyber operations more precise in terms of targeting and minimizing the risk of collateral damage[164]. An investment in research and potentiation of new emerging advanced techniques, such as machine learning and artificial intelligence, can be an asset[165] in distinguishing between civilian and military targets, and consequently enhancing the effectiveness of such cyber operations.

---

[160] IBIDEM, rule 111.
[161] (Tsagourias & Morrison, What is International Humanitarian Law?, 2023, p. 58).
[162] (CCDCOE I. G., 2017, rule 10.) However, when faced with circumstances of dual use, such a rigid application of this objective may result in internet infrastructure objectives being considered military objectives and, as a result, lacking protection against any attack, whether physical or cyber. As a result, caution is required in these circumstances, and the other principles of IHL should be applied to determine whether such an assault is worth, taking into consideration potential casualties.
[163] (WARNER, 2017).
[164] (Angelo, AI in Cybersecurity — A CISO's Perspective, 2024).
[165] (Angelo, Witnessing a Revolution in Cybersecurity with AI, 2024).

The proliferation of digital technology has greatly boosted international interconnectedness, making the digital sphere essential for maintaining individual rights, promoting economic growth, and maintaining national security. However, this interconnectivity also poses challenges, as cyber threats do not respect national borders, necessitating a collective response from the international community. Thus, another suggestion to mitigate the lack of clarification surrounding the contours of the person-object dichotomy is to enhance international cooperation and norm development in cyberspace[166].

By engaging in multilateral efforts, nations can work together to establish internationally agreed-upon norms and concepts for cyberspace. Countries can foster their international collaboration in multiple ways as has been seen - one example is the collaboration through forums such as the UN[167] and other regional organizations to develop norms and principles that guide how states should behave in cyberspace[168].

The international community can strive towards a consensus on responsible behavior[169] in cyberspace, by employing multilateral measures such as the ones outlined above, focusing on protecting civilian populations and the critical infrastructure that they depend on.

b. PRINCIPLE OF PROPORCIONALITY

Among the other fundamental principles of IHL, the principle of proportionality stands as a foundation, aiming to balance the imperatives of military necessity with the protection of civilians and civilian infrastructure.

Applying the principle of proportionality is more difficult with the introduction of the concept of cyberspace. Contrary to traditional warfare, cyber operations make it difficult to distinguish between military and civilian environments, making it challenging to estimate the scope of possible damages that can occur.

Rooted in Articles 51(5) and 57(2) (iii) of the AP-I, this principle seeks to limit and mitigate the potential damage caused by military operations. Its essence lies in ensuring

[166] (Stevens, 2017, p. 17).
[167] The UN Group of Governmental Experts (GGE) in the Field of Information and Telecommunications in the Context of International Security, has played a significant role in encouraging nations to engage with each other's, to developing an agreement on standards and actions that strengthen confidence in cyberspace. (LIBRARY, 2015).
[168] (UNODA, 2023, pp. 9--10).
[169] (UNODA, 2023, p. 10).

that the expected collateral damage and civilian casualties do not outweigh the military advantage aimed at the operation. If the expected harm exceeds the anticipated benefit of the military operation, according to the Rome Statute[170], the operation is prohibited[171].

The principle of proportionality exists to protect civilians and civilian objects from being excessively harmed during military operations. While incidental harm, often referred to as "collateral damage" is anticipated and lawful[172], it encompasses situations of accidental deaths, harm to civilians or civilian objects, and even loss of the latter[173].

When applying the concept to cyberspace, a crucial issue will be determining the extent of the word "damage" when considering loss of functionality. Given the gravity of the repercussions of disrupting civilian infrastructure capability, it seems only fair that such damage be factored into the proportionality calculation. However, it remains unclear precisely what kinds of disruptions to functionality fall within the pertinent group of damage[174].

The transfer and adaptability of traditional concepts to the cyber realm made the Experts of the Tallinn Manual[175] agree that "damage to civilian objects" might include deprivation of functionality, under certain conditions[176]. The collateral damage expected by those planning, approving, or executing a cyber-attack needs to include both direct and indirect effects, with the first having included the immediate and first-order effects of the cyber-attack[177].

By contrast, indirect effects include all those with a delayed effect or those that arise due to a chain of events or mechanisms, the so-called second, third, or other order effects[178]. Any collateral damage accounted in the proportionality calculation should include any expected indirect effects[179], by those who participate in any phase of the creation and execution of the cyber-attack.

---

[170] (PORTUGUES, article 8º, number 2, point b, iv).
[171] (CCDCOE I. G., 2017, rule 113, paragraph 4).
[172] (CCDCOE I. G., 2017, rule 113, paragraph 2).
[173] IBIDEM, paragraph 5.
[174] (Diamond, Applying International Humanitarian Law to Cyber Warfare, 2014, p. 79).
[175] (CCDCOE I. G., 2017, rule 113, paragraph 5).
[176] IBIDEM, rule 92.
[177] IBIDEM, paragraph 6.
[178] IBIDEM.
[179] (DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW, 2014, p. 737, "When undertaking a proportionality evaluation, parties to an armed conflict should consider the risk of unintended or cascading effects on civilians and civilian objects in launching a particular cyber-attack, as well as the harm to civilian uses of dual-use infrastructure that may be the target of an attack.")

Determining a threshold for what kind of functional disruptions should be considered when calculating proportionality, is a complicated task. It is important to carefully analyze every detail, starting with the context, the future impact, and the intent of any disruption, so the commander in charge can distinguish between minor and serious disruptions that might pose a threat to civilian lives[180].

However, due to the constant change of the ICTs, cyber threats appear to complicate this assessment. As cyber capabilities grow and gain weight in this realm, there is a greater chance that disruptive cyber operations will seriously damage civilian infrastructure. As a result, proportionality standards and guidelines need to be regularly reviewed.

Anticipating concrete and direct collateral damage, as commonly done in traditional kinetic warfare, presents a challenge in this context. Determining what can be considered a concrete and direct military advantage in cyberspace, requires assessing the validity of cyber operation decisions, during the planning, authorization, or implementation of each attack[181].

Requiring this anticipated result to be concrete and direct forces the decision-makers to make diligent assessments regarding the potential consequences of the correspondent cyber operations, weighing the expected benefits against the unintended risks to civilian populations and objects[182], which leads to the respect of the IHL. Thus, the principle of proportionality stands as fundamental when creating and enforcing ROE, in particular when it comes to assessing collateral damage. When creating the ROE for a mission, every previously mentioned detail needs to be fully considered, to minimize the direct or indirect effects of each operation.

Imagine a cyber operation that aims to disable an enemy state's air defense system, to protect their aircraft during a military operation. The commander in charge of planning the mission must consider that the planned cyber-attack could inadvertently disrupt the same network that is used by civilian air traffic control, most likely leading to air traffic and possible collisions.
In this situation, the principle of proportionality mandates that the Commander assesses whether the military advantage of neutralizing the enemy air defense systems outweighs

[180] (DoD, 2023, p. 1062, paragraph 16.5.1.1).
[181] (Yugoslavia, 2003, paragraph 58).
[182] (Lovitky, 2014).

the potential harm caused to civilian air traffic and collisions. If the expected civilian harm is excessive when compared to the military advantage, then the operations would be deemed disproportionate and consequently, prohibited under IHL.

c. PRINCIPLE OF PRECAUTION

The principle of precaution, often considered less important than the two previous principles when it comes to regulating the conduct of hostilities, has an undeniable practical significance. To effectively respect this principle in the realm of MCO, the solution finds itself in prioritizing the protection of civilians and civilian infrastructure, in cyberspace.

The first-time precaution was mentioned in IL, even though indirectly, in Article 27 of the Hague Convention IV[183]. However, with the crescent need to build robust protection for civilians and civilian objects, this principle has been incorporated into various official documents[184]. The first legally binding regulation can be found in AP-I, which requires that during an armed conflict, both attacking and defending sides, need to take measures to protect civilians and civilian objects[185].

The main objective behind this principle is to minimize civilian harm to the greatest extent possible. To achieve that, the principle of precaution provides twofold protection with one active and one passive requirement[186] : the first one comprises having "constant care" while cyberattacks are being conducted ("precautions in attack")[187], and the second

[183] (Convention (IV) respecting the Laws and Customs of War on Land and its annex, 1907, "In sieges and bombardments all necessary steps must be taken to spare, as far as possible, buildings dedicated to religion, art, science, or charitable purposes, historic monuments, hospitals, and places where the sick and wounded are collected, provided they are not being used at the time for military purposes.)
It is the duty of the besieged to indicate the presence of such buildings or places by distinctive and visible signs, which shall be notified to the enemy beforehand.

[184] Besides article 57 of the AP-I, article 51 of the same regulation also emphasizes civilian protection. Furthermore, various UN resolutions and statements prohibit launching attacks on civilians and the obligation to protect them, as can be observed in the UN Security Council Resolution 2664 (2022), Political Declaration on Explosive Weapons in Populated Areas (2022) and Secretary-General's Reports and Statements (2023). The Tadić Decision also reinforced the guidelines of this principle.

[185] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I), articles 57 and 58).

[186] Failing with complying on taking such precautions can convert an otherwise lawful attack, into a war crime.

[187] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I), article 57(2)).

determines that feasible precautions need to be taken to ensure civilians' protection, from those cyber-attacks[188].

In the cyber context, the "constant care" requirement provided by Article 57 can be found in Rule 114 and would likely require the Commander to maintain an all-time situational awareness[189] during all phases of the MCO, that can affect civilians[190].

According to the manual, to ensure that "constant care" is being respected, targets must be verified[191], potential incidental effects must be limited to the greatest extent possible[192] , and warnings[193] must be given if any cyber-attack may affect the civilian population[194]. The verifying and limiting obligations can be done, for example, by segmenting the opponents' network[195], and by developing a tailored piece of malware, which can disable their system without disrupting the adjacent civilian interconnected one.

However, when conducting a cyber operation, the Commander (and all persons conducting cyber operations) needs to maintain the same attention to the tool and be aware of the possible necessity to adjust the operation in case the effects turn out to be unlawful or have an impact on civilians, contrary to what was initially expected[196]. To achieve this, there is a need for technical expertise, which is one of the challenges to ensure the respect and enforcement of this principle[197].

On the other side, applying the rule of "constant care" in cyberspace will always be complicated, as almost all cyber operations have a big chance of affecting or harming civilian cyber infrastructure[198]. Consequently, after all feasible precautions have been considered by the attacking party,

[188] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I), article 58).
[189] The concept of situational awareness is explained in the Allied Joint Doctrine for Cyberspace Operations by describing it as 'a combination of a near real-time updated RCP [Recognised Cyberspace Picture], analysis and information management'. (NATO, Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations, 2020, p. 26).
[190] (Gül, 2023, p. 11).
[191] (CCDCOE I. G., 2017, Rule 115)
[192] (CCDCOE I. G., 2017, Rules 116, 118 and 120)
[193] (CCDCOE I. G., 2017, Rules 120)
[194] (CCDCOE I. G., 2017, Rules 120)
[195] (Gül, 2023, pp. 38-40).
[196] In this situation, the Commander might need to cancel or suspend the attack, according to Rule 119 of the Tallinn Manual.
[197] (Gül, 2023, pp. 13-14) and (CCDCOE I. G., 2017, Rules 121).
[198] IBIDEM, p.12.

the principle that will prevail is proportionality[199] : if the expected effect on the civilians is not excessive when compared to the anticipated military advantage, the attacker may proceed and carry out the cyber operation as initially planned[200].

The passive requirement of precaution, the feasibility requirement, determines the obligation to remove civilian objects from the scope of military objectives, as observed in Article 58(a) of AP-1, however, this comes with enormous challenges due to the characteristics of cyberspace and the intrinsic interconnectivity of civilian and military infrastructures[201].

Article 58(a) specifically refers to relocating civilians and civilian objects to avoid harm, for example by evacuating them from a town near the military base, which most likely is going to be a target. Alongside, according to Article 58 (c), other necessary precautions must also be taken "to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations"[202]. This can be achieved by implementing cybersecurity measures, incident response plans data mirroring, and other measures which include technical, logistical, or procedural activities, that aim to safeguard civilians and their infrastructure from indirect harm[203].

Despite this, assessing the full spectrum of the feasibility standard is difficult as the concept is already inherently variable and context-dependent. The concept can have different interpretations based on the circumstances of the parties involved, due to differences for many reasons, like resources and technology access. One clear example is the ongoing Gaza conflict, in which Israel warned civilians before the airstrikes by using the "roof knocking" technique. Israel was criticized for not providing sufficient warning and failing to prevent civilian causalities effectively[204].

[199] However, the calculation here may be difficult because of the time factor. Planned operations provide more time to the attacking side to do a better precautions assessment, though time-sensitive ones generally do not permit sufficient time to implement more adequate precautions.
[200] (Gül, 2023, p. 12).
[201] When we are presented with civilian and military infrastructure which are closely connected or have a dual-use structure, the compliance with these obligations becomes almost impossible, turning this requirement various times impractical in the cyber realm.
[202] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I), article 58 (c)).
[203] (Gül, 2023, p. 39).
[204] (INTERNATIONAL, 2024, "The evidence collected by Amnesty International also indicates the Israeli military failed to provide effective, or indeed any, warning – at minimum to anyone living in the locations that were hit – before launching the attacks.")

During the recent escalation in the same conflict, Israeli airstrikes aimed at Hamas infrastructure which also affected hospitals, schools, and some residential buildings. This raises questions about the feasibility of separating military from civilian targets in similar environments[205].

From these two examples, we can conclude that taking "feasible precautions" in the attack can be interpreted as a "relative" concept, bearing a range of factors that diverge from capabilities, resources, and access to technology, among others[206].

As we move to discuss the last principle of military necessity, it is crucial to address how these two principles interact. While the principle of precaution's main objective is protecting civilians, as will be seen the principle of military necessity focuses more on achieving the mission's legitimate objectives. However, maintaining a balance between these two is essential to conduct the hostilities while complying with IHL and ensuring the military operations are conducted concerning human life.

d. PRINCIPLE OF MILITARY NECESSITY

To maintain a balance between war necessities (often connected to the use of force and destruction) and the requirements of humanity (which aim to reduce suffering as much as possible and spare lives), the LOAC incorporates the aforementioned principles and the principle of military necessity[207].

The starting point for evaluating the compliance of belligerent activities within the LOAC is the principle of military necessity[208]. Without it, this evaluation would not be able to proceed to other rules such as distinction and proportionality[209].

The origin of principle of military necessity roots back to the Lieber Code, Article 14, which defines military necessity as "those measures which are indispensable for securing

[205] (WATCH, 2023, "The use of such rockets against civilian areas violates the prohibition on deliberate and indiscriminate attacks. Likewise, a party that launches rockets from densely populated areas, or co-locates military objectives in or near civilian areas – thus making civilians vulnerable to counterattacks – may be failing to take all feasible precautions to protect civilians under its control against the effects of attacks.)

[206] (ICRC, (Protocol II to the 1980 Convention as amended on 3 May 1996, article 3(10)) and (ICRC, Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons, 1980, article 1(5)).

[207] (Burks, 2022, p. 16).

[208] IBIDEM.

[209] Distinction permits militarily necessary attach on legitimate objectives, which are not civilian ones, while proportionality prohibits lawful operations whose incidental loss of civilian life or damage to civilian objects, is excessive when compared to the anticipated military advantage.

the ends of the war"[210]. Article 52 (2) of AP-I[211] limits the range of lawful targets to those having an effective contribution to the military objective, and whose destruction offers a definitive military advantage - "military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage". Similarly, Article 23 (g) of the Fourth Hague Convention[212] also prohibits the prohibition of destruction or seizure of the enemy's property, unless imperatively needed to satisfy the necessities of war[213].

A cyber-attack that targets the adversary's military computer system usually falls within a lawful target considering the potential military necessity[214] and their exclusive military connection[215]. When conducting MCO, targeting a military computer system is justified by this principle, as the outcome of the destruction or disruption of those systems provides a concrete and direct military advantage[216].

Nevertheless, determining whether a target provides a "definitive military advantage", is a complex task considering the unpredictable effects of most cyber operations[217]. This unpredictability makes difficult the assessment of the principle of necessity since the real impact of the cyber-attack, might diverge from the intended one. Thus, the military advantage will only be possibly determined after it has been already carried out.

The intrinsic complexity of computer systems means that by their interconnected nature, a cascading effect[218] and collateral damage should be expected.[219] A cyber-attack targeting a military communications network can inadvertently affect civilian communications systems, due to shared infrastructure.

[210] (ICRC, Instructions for the Government of Armies of the United States in the Field (Lieber Code), 1863)
[211] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I)).
[212] (Convention (IV) respecting the Laws and Customs of War on Land and its annex, 1907).
[213] A violation of the principle of necessity is considered a war crime, under article 8(a)(iv) of the Rome Statute of the ICC.
[214] (Gervais, 2012, p. 526).
[215] Military computer systems are crucial to a nation's defense capabilities, as it included command and control networks, intelligence gathering and operational coordination tools, for example. These tools provide support to military operations and by disrupting or destroying these, there is a direct impact on their capacity to conduct operations, and so, weakening them.
[216] For instance, the Stuxnet attack on Iran's nuclear facility pretended to delay his nuclear capabilities, by providing a military advantage to the attacking state.
[217] (Bokil, 2023, p. 5).
[218] (CCDCOE I. G., 2017, Rules 113, paragraph 6).
[219] (CCDCOE I. G., 2017, Rules 113, paragraph 13).

The cascade effect can amplify the disruption and consequently affect other important civilian sectors, potentially leading to unintended civilian harm. As so, the Commander needs to make sure the used cyber weapons[220] are targeting a specific military target, and that the effects coming from it, are limited[221].

In conclusion, and as we transition from discussing the principles of IHL to exploring ROE in cyberspace, it is critical to understand how these principles should be operationalized in the cyber domain, to achieve lawful military advantages, however, due to the dynamic nature of cyber warfare, there is a need for a continuous adaptation to the legal framework and the standards imposed by them.

V. ADHERING TO INTERNATIONAL (HUMANITARIAN) LAW IN CYBER OPERATIONS: CHALLENGES AND CONSIDERATIONS FOR CYBER-ROE

ROE are well established for land, sea, and air operations however, as the use of information technologies in military operations has evolved, the application and decision of these rules in the cyber world has become every day more challenging.

While there is a clear difficulty in drafting and complying with ROE across all domains, this is particularly enhanced in cyberspace due to its characteristics. Cyberspace gained a lot of prominence in military activities, and so it is also important to demonstrate and adequately that into ROE. This thesis will focus specifically on the challenges related to cyber-ROE.

As mentioned, it is essential to highlight the main differences between drafting ROE for cyberspace and other domains. In a conventional conflict, distinguishing between military and civilian targets is relatively easier due to physical markers such as uniforms or specific installations. However, in MCO, dual-use technologies complicate this distinction, as some civilian infrastructures often serve military functions too. Another important difference is the concept of proportionality in cyberspace. The indirect effects and cascading consequences of a cyberattack are much harder to predict and quantify compared to conventional attacks. These differences highlight the complexities in the formulation of ROE that are effective

[220] (CCDCOE I. G., 2017, Rules 116).
[221] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I), article 35 (2) and 51 (4)) and (CCDCOE I. G., 2017, Rule 105).

across all domains, emphasizing the need for a tailored approach when drafting cyber-ROE.

Cyber-Roe or ROE applicable to cyberspace are characterized as "directives to military forces (including individuals) that define the circumstances, conditions, degree, and manner in which force, or actions which might be construed as provocative, may be applied in or by the use of cyberspace".[222]

These actions include both offensive and defensive operations, such as the "use of a computer worm to disrupt the operation of an enemy command and control center"[223] and "hack back into a system that has been used for an attack against own forces' systems"[224], accordingly.

The cyberattacks in Estonia in 2007, are an example where a series of DDoS attacks targeted governmental, financial, and media websites[225], which showed the need for robust defensive measures and recovery strategies to keep the critical sectors in place. Conducting Joint Operations, requires Commanders to be prepared to confront a broad range of dangers, requiring them to be extremely defensive in and through cyberspace, to accomplish the mission goals.[226]
For the mission to be effective, the risks connected with missions conducted within or through that environment must be reduced, and measures must be created in preparation to determine defensive objectives, build recovery strategies, and guarantee the confidentiality, integrity, and availability of information.[227]

In the ideal scenario, the presence of ROE approved by the political level would fill the legal void, however, this level is unwilling to accept state accountability for operations undertaken by its armed forces in other nations' online territories. Each nation approves its ROE based on its national *caveats*, which is one of the reasons that makes standardizing ROE impossible.[228]

---

[222] (Stinissen, Minárik, Pissanidis, Veenendaal, & Glorioso, 2015, p. 8).
[223] IBIDEM.
[224] IBIDEM.
[225] (Ottis, p. 3).
[226] (Williams B. T., 2014).
[227] (NATO, AJP-3 ALLIED JOINT DOCTRINE FOR THE CONDUCT OF OPERATIONS, 2019, p.1-14 (g)).
[228] (INSTITUTE, 2000).

Aside from that, the existence of ROE with a minimum common denominator among NATO countries, instead of a maximum standard, is important as it allows some ambiguity in the concepts that influence and lead to the creation of those rules. This ambiguity also capacitates the Commander with more flexibility to adapt them to the mission, since each mission has a specific ROE that transforms them into concrete in every scenario.[229]

When drafting ROE for each operational environment, the rules are developed according to the type of mission and its targets[230], and having a general standardized ROE would be counterproductive as the mentioned variables require tailored approaches.[231]

Consequently, and since standardization is not the solution in the view of the author, there is a need for a better understanding and application of the existent and applicable legal frameworks to effectively navigate through these challenges and ensure adherence to IL, as will be further discussed.

a. LEGAL FRAMEWORK AND PRACTICAL IMPLICATIONS FOR CYBERSPACE OPERATIONS AND CYBER-ROE

In both national and international contexts, the legality of the use of force and the legitimacy of the military action play a dominant part. Consequently, conflicts must respect the legal principles implicit in these situations.

As seen before in this dissertation, despite the existent differences in the application and interpretation of IL, as well as the obligations to which state commits themselves, there are a set of rules derived from international agreements that are generally accepted by the majority and are considered the legal basis at the international level.

IHL aims to protect certain persons and objects during armed conflicts by restricting the means and methods of warfare used[232] and because most countries are obligated by the Geneva and Hague Conventions, they have a responsibility to guarantee that IHL is followed[233]. Cyber operations must be guided by the same regulations, training, and

[229] (Amicorum & Gill, 2021, p. 395).
[230] (Williams & Ford, 2020, pp. 109-124).
[231] As an example, the cyber-ROE determined for a mission targeting terrorist networks would differ significantly from ones whose goal is protecting critical infrastructure from state-sponsored cyber threats.
[232] (Tsagourias & Morrison, What is International Humanitarian Law?, 2023).
[233] (Djukić & Pons, 2018).

established rules and limits[234], as well as follow the principles of IHL and other applicable international provisions[235].

However, it is important to highlight that ROE are not themselves IL and should not be confused with legal obligations.[236] ROE and the LOAC are two different sources of operations regulation and although ROE usually contains LOAC obligations, they are not synonyms. ROE usually contains more specific and narrower restrictions than those required by IL[237], however, this does not mean that Commanders are relieved of their underlying legal obligations.

On the opposite, these narrower restrictions are created to ensure compliance with the broader principles of IL. For instance, in a situation where a certain ROE allows a soldier to kill an enemy, that same ROE does not permit the killing of a soldier who has surrendered, as that would be a clear violation of the LOAC. Similarly, if another ROE allows a pilot to destroy a building, the pilot must nonetheless evaluate the proportionality of that action, to ensure the incidental civilian harm is not excessive compared to the obtained military advantage.

For the lowest level of command, ROE and the instructions that flow from them are the most basic way of dictating the use of force, constituting the rules that can potentially influence or determine the escalation of the hostilities in the field of operations.[238] These rules are always composed of three different components - legal, political, and military - and they primarily decide and contribute to the draft of all specific ROE profiles that apply to every operation[239]. Thus, it is from the outcome of these three components that ROE are defined, and troops know how to act or refrain from acting[240].

Because ROE are operational documents, their purpose is to be straightforward, brief, and easy to understand, they do not usually re-state the applicable law for two reasons: their brevity prevents them from restating or including the complete corpus of law, and second, because the relevant law generally necessitates to be analyzed by someone experienced and legally educated.

---

[234] (ICRC, Even wars have rules: Can one decision change your life?, s.d.).
[235] (NATO, ATrainP-4: TRAINING IN NATO RULES OF ENGAGEMENT, 2022, pp. B-12).
[236] (Solis, 2021, p. 490).
[237] IBIDEM, p.495.
[238] IBIDEM.
[239] (NATO, MC 0362/2 FINAL, 2019, p. 2, paragraph 2).
[240] (Cooper, 2020, p. 26).

Restating the law as written serves no purpose for the troops who will implement it in the field[241] and so the solution is to have a follow-up[242], a constant legal adviser on and during the operation itself, to ensure there is a constant interpretation of all the operational ongoing scenarios and its potential consequences.

Despite the existing established regulations, cyberspace still faces enormous challenges in ensuring compliance with IHL through cyber-ROE. The dynamic and speed of cyber operations complicate the enforcement of the existent legal frameworks, which brings us to the next chapter, where we will explore specific obstacles when trying to apply and adapt the principles of IHL to cyber-ROE.

b. IHL PRINCIPLES AND CYBER ROE: CHALLENGES ENSURING COMPLIANCE

By establishing a framework that intends to mitigate the impact of armed conflicts on civilians and civilian objects, the principles of IHL play a very important role in the process of drafting and implementing cyber-ROE. In this last part, the author will delve into the complexities of integrating IHL principles into ROE for cyber operations.

"ROE must be lawful"[243] is one of the ground rules formulated in NATO doctrine. It demonstrates the importance that an organization attaches to the legal compliance[244] of its operations, showing that although the operations are not limited by IL[245], ROE are not more permissive regarding the use of force, in situations that are contrary to the international legal regime[246].

Relating cyber operations to ROE is always complex. It is not easy to understand if cyber operations constitute the use of force[247] or provocative acts and, even though there is extensive use of kinetic language to describe various hostile cyber activities[248], not all cyber activities amount to the use of force in a legal viewpoint. Nevertheless, some of

[241] (Boddens Hosang, 2017, p. 33).
[242] (NATO, ATrainP-4: TRAINING IN NATO RULES OF ENGAGEMENT, 2022, pp. B-80).
[243] IBIDEM.
[244] For deeper analyses of legal considerations for NATO ROE development, see (NATO, ATrainP-4: TRAINING IN NATO RULES OF ENGAGEMENT, 2022, pp. B-51/52).
[245] (NATO, MC 0362/2 FINAL, 2019, p. 3, paragraph 10).
[246] IBIDEM.
[247] The Tallin Manual identifies the factors which determine if a cyber activity amounts to use of force, even though emphasizing those are not formal legal criteria. The Manual also acknowledges that the specific circumstances and context will heavily influence whether an action is considered, or not, use of force.
[248] (Amicorum & Gill, 2021, p. 410, "Cyber warfare" and "Cyber-attack")

those cyber activities amount to the use of force and “armed attack” under Article 51 of the UN Charter, especially when the outcome is connected to physical damage or harm[249].

One significant obstacle both in drafting and ensuring compliance is found when analyzing the principle of distinction. It was already outlined the difficulty in distinguishing between a military and civilian target.
If we translate this to cyber-ROE, the ambiguity hampers the creation of precise and actionable ROE.

The lack of clarity surrounding this principle and its contours leads to misinterpretations and potential violations of IHL, consequently increasing the risk of unlawful targeting unintentionally.

Developing and sharing clearer guidelines[250] within the ROE to be able to categorize the various cyber assets considering their primary use, regularly update them to keep up with the technological advancement, and introducing “classification protocols” to regular training sessions for the attacking forces[251] where they can identify and distinguish between dual-usage targets, are some of the possible solutions to face this problem[252].

However, the difficulties in adapting ROE to cyberspace operations go beyond the principle of distinction. The principle of proportionality also carries a lot of ambiguities and challenges in its application.

Some traditional concepts do not translate well to cyberspace, where the loss of functionality can assume significant impacts. Consequently, determining the extent and meaning of "damage" in cyberspace is particularly difficult[253].
As a result, the ambiguity in assessing “damage”, sabotages the creation of clear and enforceable ROE, leading to possible misjudgments in evaluating the proportionality of each cyber operation.

As previously suggested, also here comprehensive guidelines within the cyber-ROE would be crucial to contribute to the definition of key concepts as “damage” in cyber

[249] IBIDEM.
[250] (ICRC, International humanitarian law and cyber operations during armed conflicts - ICRC short papers, 2023).
[251] (Chouliaras, et al., 2021).
[252] A possible cooperation within international bodies to establish universally accepted concepts and criteria for targeting classification could also be beneficial, however challenging to achieve.
[253] (Diamond, Applying International Humanitarian Law to Cyber Warfare, 2014, p. 79).

operations, encompassing both loss of functionality and physical destruction. These guidelines should be introduced in the same mentioned training sessions for cyber operations teams, to improve their ability in assessing cyber damage and proportionality in their missions.

Including the frequent indirect effects in the proportionality assessment is also important, but complex to achieve. These effects usually arise from a chain of events that were caused by the cyber operation, however failing to account for these can lead to disproportionate operations, especially because most of the time the full impact of a cyber-attack cannot be immediately envisioned. Incorporating detailed protocols that help calculate both direct and indirect effects, by modeling potential cascading effects and long-term impacts[254] (especially on civilian infrastructure), are some of the suggestions of the author.

However, especially in this matter, advanced simulation and monitoring tools need to incorporate new technologies and techniques to facilitate the process.[255] Those tools should also contain continuous monitoring and post-attack analysis to refine the predictions of future indirect effects[256].

In a cyber world, technology plays a vital role and can lead to inadequate assessments when not used appropriately. Therefore, investing in adaptative cyber defense technologies and incorporating them in cyber-ROE, is essential. This way, ROE become more capable of evaluating and mitigating potential collateral damage, being furnished with a mandatory pre-attack impact assessment, and real-time monitoring to minimize harm during and after, each cyber operation.

Even though these technological advancements enhance the precision of cyber operations, the principle of precaution also plays a critical role. Precaution mandates that Commanders maintain a constant awareness of the impact of the operation on civilians and civilian objects, by verifying targets and limiting incidental effects.[257] The mission's legitimacy might be undermined if there is a failure in this duty, leading to excessive civilian harm. The comprehensive guidelines within the ROE should

[254] (Palleti, Adepu, Mishra, & Mathur, 2021).
[255] (HAWSER, p. 3).
[256] Simulation tools like Cyber Analysis Modeling Evaluation for Operations (CAMEO) in (Kavak, et al., 2021).
[257] (CCDCOE I. G., 2017, rules 114-115).

be able to define the extent of the "constant care" requirement and incorporate advanced situational awareness tools[258] to assist the Commanders.

The Commander should also be prepared to adjust the operation in case the effects become unlawful or impact civilians more than expected. This flexibility means that he needs to be able to quickly alter his strategy to mitigate the negative impacts and maintain compliance with IHL while trying to protect civilian life and infrastructure. However, this requires technical expertise to understand the cyber tools and operations they are directing.[259] This expertise enables them to evaluate the operation scenario accurately and implement immediate changes to the cyber-operation when required.

Another important blocking point that further complicates the applicability of precautions to cyber-ROE, is attribution. This hinders both accountability and enforcement of ROE as it is challenging to determine the responsible for a cyberattack[260]. Consequently, it is difficult to hold the correct parties accountable and enforce ROE effectively since it is unclear which party carried out the attack, and Commanders need to understand who is responsible for making informed and proportional responses. Without a clear attribution, they may struggle to decide whether and how to retaliate, deciding either on an insufficient response or escalating the hostilities. Additionally, if the source of the attack is unknown, it becomes harder to ensure that any military response respects the principles of IHL, potentially leading to unlawful actions.

To solve this ongoing issue, it is important to enhance attribution capabilities through advanced forensic tools[261] and international collaboration.[262] To be able to improve the ability to trace the origins of cyberattacks, it is required very sophisticated tools that can analyze digital evidence and track the source of the cyberattack[263]. Additionally, if the States would be able to collaborate and provide data

[258] (Ali, 2016).
[259] (Gül, 2023, p. 14).
[260] (Eric F. Mejia, 2014, p. 118).
[261] These technological tools and techniques are used to analyze the digital evidence derived from the cyberattacks. They examine various data points such as network traffic, malware code and other digital footprints left by the attackers. Examples include reverse engineering of malware, machine learning algorithms for anomaly detection and threat intelligence platforms.
[262] Countries can share threat intelligence and forensic data which provide a better understanding of the threats, and collaborate in various ways, such as capacity building and joint investigations.
[263] (Solutions, 2023).

and insights on similar situations[264], that would also make it easier to identify patterns and thus, the attackers.

Lastly, while the principle of precaution is vital for minimizing harm to civilians and civilian infrastructure, it must be balanced in a way that allows the use of force to achieve military objectives. The principle of military necessity ensures that the conducted operations have a clear and effective purpose, reason why integrating this principle in cyber-ROE is crucial to achieve their concrete and direct military advantage.

However, as in other principles, the ambiguities in defining lawful targets can lead to misidentification and potential violations of IHL, further complicating the drafting of precise and enforceable ROE that guarantees compliance with military necessity. Determining whether a target provides "a definitive military advantage" is a complicated task considering the unpredictable effects for most MCOs[265]. This unpredictability also makes it difficult to respect the principle of necessity as the real impact of the cyberattack might diverge from the initial intended one. Thus, as already mentioned, the military advantage can only be possibly determined after the operation has been initiated.

As suggested, incorporating a practice of modeling potential cascading effects and long-term impacts[266] can also here contribute to respect necessity, as the Commander has a better understanding of the possible consequences of the cyber operation. This will allow him to choose cyber weapons that only target specific military objectives[267]and that limit unintended effects on civilians and civilian infrastructure[268].

Despite this, since there is a constant evolution in the emerging cyber threats, it is needed to continuously update on ROE, as outdated ones do not take into consideration the emerging threats, leading to failures in fighting those and reducing compliance with IHL. Also here, international collaboration assumes a pivotal role in sharing insights and feedback from past operations that can be used to improve and prevent future ones. By

[264] (UNODOC, 2019).
[265] (Bokil, 2023, p. 5).
[266] (Palleti, Adepu, Mishra, & Mathur, 2021).
[267] (CCDCOE I. G., 2017, Rules 116).
[268] (ICRC, Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I), article 35 (2) and 51 (4)) and (CCDCOE I. G., 2017, Rule 105).

sharing information and analyzing real-world case studies of operations, military planners can observe how these threats are evolving and refine their ROE accordingly.

This collaboration would allow each country or targeted organization to gain more information about the attackers, as they often use the same *modus operandi*[269], also avoiding wasting time conducting investigations from scratch. Consequently, the attacked party can respond to the cyberattack more quickly and effectively mitigate its effects based on the other international partner's feedback.

[269] Platforms as: Malware Information Sharing Platform (MISP), are very promising in this regard, however states are still reluctant in sharing this kind of information among each other's.

VI. CONCLUSION

In conclusion, this dissertation has explored the essential relationship between IL, IHL, and the ROE in MCO. The fast evolution of technology and the emergence of cyberspace as a battlefield requires a re-evaluation of traditional legal frameworks to ensure they remain pertinent and effective.

The deductive method employed in this work has shown how the existing legal norms influence and transform the formulation of ROE in cyberspace. By analyzing the definitions and applications provided by NATO and the EU, this dissertation has shown that ROE are not merely operational guidelines but fundamental parts of the strategic planning process, reflecting the legal, political, and military objectives of states.

The key conclusion from this work is that principles of IHL, such as distinction, proportionality, and precaution, are crucial in shaping ROE for cyber operations. These principles ensure that military actions in cyberspace are conducted with a clear objective of minimizing harm to civilians and civilian infrastructure. However, the unique features of cyberspace, such as dual use and the difficulty in attributing cyberattacks, present significant challenges to the application of these IHL regulations.

The principle of distinction becomes complex in a domain where civilian and military infrastructures often overlap. Similarly, assessing proportionality is difficult due to the frequent cascading effects and indirect damage that cyber operations cause.

Despite these obstacles, this dissertation has identified several courses of action to improve the integration of IHL into cyber-ROE. Enhancing cyber intelligence and surveillance capabilities, encouraging international cooperation, and flourishing clear guidelines for the categorization and targeting of cyber assets, are some of the recommendations proposed. Additionally, the use of advanced simulation and monitoring tools can aid the assessment of potential collateral damage and ensure compliance within IHL principles is more efficient and less time-consuming.

The nature of cyberspace necessitates a flexible and versatile perspective on legal frameworks. This study underlines the importance of continuous reassessment and updating of ROE to address the new technological threats and advancements. International collaboration and the creation of cyber-specific addenda to existing treaties are crucial steps to achieve that.

In summary, despite the integration of IHL into ROE for MCO is a difficult task, by adhering and adapting those principles to the unique challenges of cyberspace, states can ensure that their cyber operations are conducted in a manner that sustains humanitarian values and standards.

VII. BIBLIOGRAPHY

JURISPRUDENCE

1. ICJ. (1949). CORFU CHANNEL ((United Kingdom of Great Britain and Northern Ireland v. Albania). Retrieved from INTERNATIONAL COURT OF JUSTICE: https://www.icj-cij.org/sites/default/files/case-related/1/001-19490409-JUD-01-00-EN.pdf
2. ICJ. (1996). ICJ, Nuclear Weapons Advisory Opinion. Retrieved from HOW DOES LAW PROTECT IN WAR: https://casebook.icrc.org/case-study/icj-nuclear-weapons-advisory-opinion
3. Justice, I. C. (27 de JUNE de 1986). (Nicaragua v. United States of America). Retrieved from CASE CONCERNING MILITARY AND PARAMILITARY ACTIVITIES IN AND AGAINST NICARAGUA: https://www.ilsa.org/Jessup/Jessup08/basicmats/icjnicaragua.pdf
4. JUSTICE, I. C. (8 JULY 1996). LEGALITY OF THE THREAT OR USE OF NUCLEAR WEAPONS. Retrieved from https://www.icj-cij.org/public/files/case-related/95/095-19960708-ADV-01-00-EN.pdf
5. JUSTICE, I. C. (s.d.). Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. Albania). Retrieved from ICJ: https://www.icj-cij.org/sites/default/files/case-related/1/001-19490409-JUD-01-01-EN.pdf
6. Yugoslavia, I. T. (2003). Prosecutor v. Stanilav Galic (Trial Judgement and Opinion). Retrieved from REFWORLD: https://www.refworld.org/jurisprudence/caselaw/icty/2003/en/40194

OFFICIAL DOCUMENTS

1. (EEAS), E. E. (23 de APRIL de 2019). EU Concept for Military Command and Control. Retrieved from COUNCIL OF EUROPEAN UNION: https://data.consilium.europa.eu/doc/document/ST-8798-2019-INIT/en/pdf
2. (Switzerland), F. D. (September de 2009). Avis de droit sur les bases légales des opérations dans les réseaux. Retrieved from The Federal Assembly — The Swiss Parliament: https://www.parlament.ch/centers/documents/fr/gutachten-ejpd-computernetz-vbs-2009-03-10-f.pdf
3. (UNIDIR), T. U. (21 de NOVEMBER de 2021). Due diligence in cyberspace: Normative expectations of reciprocal protection of international legal rights.

Retrieved from UNIDIR: https://unidir.org/publication/due-diligence-cyberspace-normative-expectations-reciprocal-protection-international

4. Affairs, M. f. (2020). International law and cyberspace: Finland's national positions. Retrieved from Ministry for Foreign Affairs: https://um.fi/documents/35732/0/Cyber+and+international+law%3B+Finland%27s+views.pdf/41404cbb-d300-a3b9-92e4-a7d675d5d585?t=1602758856859
5. Ali, C. R. (2016). Cyber Situational awareness for the NATO Alliance. Retrieved from NATO Joint Warfare Centre: https://www.jwc.nato.int/images/stories/_news_items_/2016/Cyber_Situational_Awareness.pdf
6. Armées, M. d. (s.d.). DROIT INTERNATIONAL APPLIQUÉ AUX OPÉRATIONS DANS LE CYBERESPACE. Retrieved from Defense Gouvernment: https://www.defense.gouv.fr/sites/default/files/ministere-armees/Droit%20international%20appliqu%C3%A9%20aux%20op%C3%A9rations%20dans%20le%20cyberespace.pdf
7. Assembly, U. N. (JULY de 2021). Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. Retrieved from 2021 GGE: https://front.un-arm.org/wp-content/uploads/2021/08/A_76_135-2104030E-1.pdf
8. Assembly, U. N. (JULY de 2021). Official compendium of voluntary national contributions on the subject of how international law applies to the use of information and communications technologies by States submitted by participating governmental experts in the Group of Governmental Expert. Retrieved from
9. UNITED NATIONS: https://front.un-arm.org/wp-content/uploads/2021/08/A-76-136-EN.pdf
10. Canada, G. o. (s.d.). International Law applicable in cyberspace. Retrieved from https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a5
11. CCDCOE. (2019). National position of France. Retrieved from Cyber Law Toolkit: https://cyberlaw.ccdcoe.org/wiki/National_position_of_France_(2019)#Sovereignty

12. CCDCOE. (2021). National position of Estonia. Retrieved from CyberLaw Toolkit: https://cyberlaw.ccdcoe.org/wiki/National_position_of_Estonia_(2021)#cite_ref-8
13. CCDCOE. (2021). National position of Germany. Retrieved from CyberLaw Toolkit: https://cyberlaw.ccdcoe.org/wiki/National_position_of_Germany_(2021)#Due_diligence
14. CCDCOE. (2022). 14th International Conference on Cyber Conflict: keep going. 14th International Conference on Cyber Conflict: keep going.
15. CCDCOE. (s.d.). Battling Cybercrime Through the New Additional Protocol to the Budapest Convention. Retrieved from https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/
16. CCDCOE. (s.d.). CyberLaw Toolkit. Retrieved from DUE DILIGENCE: https://cyberlaw.ccdcoe.org/wiki/Due_diligence#cite_ref-60
17. CCDCOE. (s.d.). Cyberspace as a 'Domain of Operations' at Warsaw Summit. Retrieved from https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/
18. CCDCOE. (s.d.). OSCE Expands Its List of Confidence-Building Measures For Cyberspace: Common Ground on Critical Infrastructure Protection. Retrieved from CCDCOE: https://ccdcoe.org/incyder-articles/osce-expands-its-list-of-confidence-building-measures-for-cyberspace-common-ground-on-critical-infrastructure-protection/
19. Convention (IV) respecting the Laws and Customs of War on Land and its annex. (1907). Retrieved from REFWORLS: https://www.refworld.org/docid/4374cae64.html
20. DIGEST OF UNITED STATES PRACTICE IN INTERNATIONAL LAW. (2014). Retrieved from https://2009-2017.state.gov/documents/organization/244504.pdf
21. DoD, U. (2023). Department of Defense: law of war manual. Retrieved from https://media.defense.gov/2023/Jul/31/2003271432/-1/-1/0/DOD-LAW-OF-WAR-MANUAL-JUNE-2015-UPDATED-JULY%202023.PDF

22. EU, C. O. (2020). Declaration by the High Representative Josep Borrell, on behalf of the European Union, on malicious cyber activities exploiting the coronavirus pandemic. Retrieved from Consilium: https://www.consilium.europa.eu/en/press/press-releases/2020/04/30/declaration-by-the-high-representative-josep-borrell-on-behalf-of-the-european-union-on-malicious-cyber-activities-exploiting-the-coronavirus-pandemic/
23. EUROPE, C. O. (s.d.). The Budapest Convention (ETS No. 185) and its Protocols. Retrieved from https://www.coe.int/en/web/cybercrime/parties-observers
24. Europe, O. f.-o. (2023). 10 Years of OSCE Cyber/ICT Security Confidence-Building Measure. Retrieved from OSCE: https://www.osce.org/files/f/documents/f/7/555999_1.pdf
25. Excellence, N. S. (JUNE de 2021). RUSSIA'S STRATEGY IN CYBERSPACE. Retrieved from https://stratcomcoe.org/cuploads/pfiles/Nato-Cyber-Report_11-06-2021-4f4ce.pdf
26. ICRC. (s.d.). (Protocol II to the 1980 Convention as amended on 3 May 1996. Retrieved from International Humanitarian Law Databases: https://ihl-databases.icrc.org/assets/treaties/575-IHL-92-EN.pdf
27. ICRC. (1863). Instructions for the Government of Armies of the United States in the Field (Lieber Code). Retrieved from International Humanitarian Law Databases: https://ihl-databases.icrc.org/assets/treaties/110-IHL-L-Code-EN.pdf
28. ICRC. (12 de AUGUST de 1949). IV GENEVA CONVENTION RELATIVE TO THE PROTECTION OF CIVILIAN PERSONS IN TIMES OF WAR. Retrieved from ICRC: https://ihl-databases.icrc.org/assets/treaties/380-GC-IV-EN.pdf
29. ICRC. (1980). Protocol on Prohibitions or Restrictions on the Use of Incendiary Weapons. Retrieved from International Humanitarian Law Databases: https://ihl-databases.icrc.org/en/ihl-treaties/ccw-protocol-iii-1980?activeTab=default
30. ICRC. (2005). Customary International humanitarian law: questions & answers. Retrieved from ICRC: https://www.icrc.org/en/doc/resources/documents/misc/customary-law-q-and-a-150805.htm#a1
31. ICRC. (2011). International Humanitarian Law and the challenges of contemporary armed conflicts Report. Retrieved from ICRC: https://www.icrc.org/en/doc/assets/files/red-cross-crescent-movement/31st-

international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf

32. ICRC. (2019). International Humanitarian Law and Cyber Operations during Armed Conflicts. Retrieved from ICRC: https://www.icrc.org/en/download/file/108983/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf
33. ICRC. (12 de AUGUST de 2021). Rules of war: Why they matter. Retrieved from Rules of war: Why they matter: https://www.icrc.org/en/document/rules-war-why-they-matter
34. ICRC. (2023). International humanitarian law and cyber operations during armed conflicts - ICRC short papers. Retrieved from ICRC: https://www.icrc.org/en/document/short-papers-on-international-humanitarian-law-and-cyber-operations-during-armed-conflicts
35. ICRC. (MARCH de 2023). THE PRINCIPLE OF DISTINCTION. Retrieved from THE PRINCIPLE OF DISTINCTION: https://www.icrc.org/sites/default/files/wysiwyg/war-and-law/03_distinction-0.pdf
36. ICRC. (s.d.). Even wars have rules: Can one decision change your life? Retrieved from Even wars have rules: Can one decision change your life?: https://www.icrc.org/en/rules-of-war
37. ICRC. (s.d.). IHL Databases. Retrieved from IHL Databases: https://ihl-databases.icrc.org/en/customary-ihl/v1/in
38. ICRC. (s.d.). International Humanitarian Law Databases. Retrieved from ICRC DATABASES: Definition of Civilians: https://ihl-databases.icrc.org/en/customary-ihl/v1/rule5
39. ICRC. (s.d.). Protocol Additional to the Geneva Conventions Relating to the Protection of Victims of International Armed Conflicts (Protocol I). Retrieved from ICRC: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977?activeTab=undefined
40. International, a. (february de 2024). Israel/opt: new evidence of unlawful israeli attacks in gaza causing mass civilian casualties amid real risk of genocide . Retrieved from amnesty international: https://www.amnesty.org.au/israel-opt-new-evidence-of-unlawful-israeli-attacks-in-gaza-causing-mass-civilian-casualties-amid-real-risk-of-genocide/

41. Library, U. N. (2015). Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Retrieved from https://digitallibrary.un.org/record/799853
42. NATO. (30 de JUNE de 2003). MC 362/1. Retrieved from https://govtribe.com/file/government-file/rfpactsact1646-mc-362-1-nato-roe-dot-pdf
43. NATO. (2019). AJP-3 ALLIED JOINT DOCTRINE FOR THE CONDUCT OF OPERATIONS. AJP-3 ALLIED JOINT DOCTRINE FOR THE CONDUCT OF OPERATIONS.
44. NATO. (18 de SEPTEMBER de 2019). MC 0362/2 FINAL.
45. NATO. (20 de JANUARY de 2020). Allied Joint Publication-3.20: Allied Joint Doctrine for Cyberspace Operations. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/899678/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf
46. NATO. (2022). ATrainP-4: TRAINING IN NATO RULES OF ENGAGEMENT. Retrieved from NATO STANDARDIZATION OFFICE: https://nso.nato.int/nso/nsdd/main/list-promulg
47. Netherlands, G. o. (2019). Letter to the parliament on the international legal order in cyberspace: Retrieved from Appendix: International law in cyberspace: https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace
48. Office, C. (NOVEMBER de 2011). The UK Cyber Security Strategy- Protecting and promoting the UK in a digital world. Retrieved from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf
49. Trade, N. Z. (DECEMBER de 2020). The Application of International Law to State Activity in Cyberspace. Retrieved from https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

50. UN GGE REPORT. (JULY de 2015). Retrieved from United Nations General Assembly: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/228/35/PDF/N1522835.pdf?OpenElement
51. UNIDIR. (2019). GGE recommendations on international law and norms of responsible State behavior. Retrieved from UNIDIR: https://unidir.org/sites/default/files/2019-10/GGE-Recommendations-International-Law.pdf
52. UNION, C. O. (4 de DECEMBER de 2009). EU Concept for the Use of Force in EU-led Military Operations. EU Concept for the Use of Force in EU-led Military Operations, p. 13. Retrieved from https://data.consilium.europa.eu/doc/document/ST-17168-2009-EXT-1/en/pdf
53. UNION, C. O. (2 de February de 2010). ESDP/PESD. EU Concept for the Use of Force in EU-led Military Operations, p. 13.
54. UK Foreign, C. &. (2021). GOV.UK. Retrieved from GOV.UK: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement#non-intervention-and-sovereignty
55. York, D. t. (2023). EU Statement – UN Open-Ended Working Group on ICT: Confidence-Building Measures. Retrieved from Delegation of the European Union to the United Nations in New York: https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-%E2%80%93-un-open-ended-working-group-ict-confidence-building-measures-0_en?s=63
56. Ziegler, K. (2013). Max Planck Encyclopedia of Public International. (O. P. Law, Ed.) Retrieved from https://moodle2.units.it/pluginfile.php/383613/mod_resource/content/1/Ziegler%2C%20Domaine%20r%C3%A9serv%C3%A9%20%282013%29.pdf

BOOKS/ARTICLES

1. Amicorum, L., & Gill, T. D. (2021). Military Operations and the Notion Of Control Under International Law. Springer.
2. Angelo, D. d. (MARCH de 2024). AI in Cybersecurity — A CISO's Perspective. Retrieved from PALO ALTO NETWORKS: https://www.paloaltonetworks.com/blog/2024/03/ai-in-cybersecurity-a-cisos-perspective/
3. Angelo, D. d. (MARCHO de 2024). Witnessing a Revolution in Cybersecurity with AI. Retrieved from PALO ALTO NETWORKS: https://www.paloaltonetworks.com/blog/2024/03/revolution-in-cybersecurity-with-ai/
4. Anna-Maria Osula, A. K. (2022). EU Common Position on International Law and Cyberspace. Retrieved from Masaryk University Journal of Law and Technology: https://journals.muni.cz/mujlt/article/view/20668
5. Antonio Coco, T. d. (AUGUST de 2021). 'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law. Retrieved from European Journal of International Law: https://academic.oup.com/ejil/article/32/3/771/6356808
6. Arquilla, J. (25 de SEPTEMBER de 2017). The Rise of Strategic Cyberwar? Retrieved from COMMUNICATIONS OF THE ACM: https://cacm.acm.org/blogs/blog-cacm/221308-the-rise-of-strategic-cyberwar/fulltext
7. Boddens Hosang, J. (8 de February de 2017). Rules of engagement: Rules on the use of force as linchpin for the international law of military operations. Retrieved from UNIVERSITY OF AMSTERDAM: UvA-DARE (Digital Academic Repository): https://dare.uva.nl/search?identifier=691ccb62-371e-4e09-94d3-3793f4b3a54d
8. Bokil, R. (2023). Cyber Warfare: Taking War to Cyberspace and its Implications for International Humanitarian Law. Retrieved from International Journal for Multidisciplinary Research: https://www.ijfmr.com/papers/2023/1/1494.pdf
9. Buchan, R. (2016). 'Cyberspace, Non-State Actors and the Obligation to Prevent Transboundary Harm". Retrieved from Journal of Conflict & Security Law, Vol. 21, No. 3, Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence: https://www.jstor.org/stable/26298209?searchText=&searchUri=&ab_segments

=&searchKey=&refreqid=fastly-default%3Aff51b347a1fba4b3f7ad4817b6d75a3f

10. Burks, T. R. (2022). MILITARY NECESSITY: POLICY-CAPABILITY TENSIONS. Retrieved from ÆTHER: A JOURNAL OF STRATEGIC AIRPOWER & SPACEPOWER: https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-3/Burks.pdf
11. Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). Cyber Ranges and TestBeds for Education, Training, and Research. Retrieved from MDPI: https://www.mdpi.com/2076-3417/11/4/1809
12. Cole, C. A., Drew, M. P., McLaughlin, C. R., & Mandsager, P. D. (NOVEMBER de 2009). SANREMO HANDBOOK ON RULES OF ENGAGEMENT. (I. I. Law, Ed.)
13. Cooper, C. G. (2020). NATO Rules of Engagement: On ROE, Self-Defence and the Use of Force during Armed Conflict. Brill.
14. Creemers, R. (FEBRUARY de 2020). China's Conception of Cyber Sovereignty: Rhetoric and Realization. Retrieved from SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3532421
15. Diamond, E. (2014). Applying International Humanitarian Law to Cyber Warfare. Retrieved from JSTOR: https://www.jstor.org/stable/resrep08957.8
16. Djukić, D., & Pons, N. (29 de OCTOBER de 2018). The Companion to International Humanitarian Law. BRILL. Retrieved from Contemporary challenges to IHL – Respect for IHL: overview: https://www.icrc.org/en/document/respect-international-humanitarian-law
17. Eric F. Mejia, C. U. (2014). Act and Actor Attribution in Cyberspace: A Proposed Analytic Framework. Retrieved from JSTOR: https://www.jstor.org/stable/26270607
18. Geers, K. (2020). Alliance Power for CyberSecurity. Retrieved from The Atlantic Council of the United States: https://www.atlanticcouncil.org/wp-content/uploads/2020/08/Alliance-Power-for-Cybersecurity_Geers.pdf
19. Gervais, M. (2012). Cyber Attacks and the Laws of War. Retrieved from Berkeley Journal of International Law: https://lawcat.berkeley.edu/record/1125035?v=pdf

20. Giles, K. (2012). Russia's Public Stance on Cyberspace Issues. Retrieved from CCDCOE: https://ccdcoe.org/uploads/2015/04/CyCon_2012_book_web_sisu.indd_.pdf
21. Greathouse, C. B. (2014). Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? Em J.-F. Kremer, & B. Mtiller (Edits.), Cyberspace and International Relations: Theory, Prospects lind Challenges. Springer.
22. Gül, Y. E. (JULY de 2023). The Military Law and the Law of War Review. The application of the principle of precautions to cyber operations.
23. HAWSER, A. (s.d.). The Rules of Engagement in Cyberspace. Retrieved from ACADEMIA: https://www.academia.edu/7212066/The_Rules_of_Engagement_in_Cyberspace?email_work_card=reading-history
24. Isaac R. Porche III, C. P.-E. (2017). Tactical Cyber: Building a Strategy for Cyber Support to Corps and Below. Retrieved from RAND CORPORATION: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1600/RR1600/RAND_RR1600.pdf
25. Jensen, E. T. (2013). Cyber Attacks: Proportionality and Precautions in Attack. Retrieved from International Law Studies: U.S Naval War Collegue: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1029&context=ils
26. Kavak, H., Padilla, J. J., Vernon-Bido, D., Diallo, S. Y., Gore, R., & Shetty, S. (2021). Simulation for cybersecurity: state of the art and future directions. Retrieved from Journal of Cybersecurity: https://academic.oup.com/cybersecurity/article/7/1/tyab005/6170701
27. Laurent Gisel, T. R. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. Retrieved from International Review of the Red Cross: https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf
28. Lopes, J. A. (2020). Regímes Jurídicos e Direito internacional, Volume I. Porto: Universidade Católica Editora Porto.
29. Lovitky, J. (2014). APPLICATION OF THE PRINCIPLE OF MILITARY ADVANTAGE IN DETERMINING PROPORTIONALITY. Retrieved from

Articles of War : Lieber Institute: https://lieber.westpoint.edu/application-principle-military-advantage-determining-proportionality/

30. Moulin, T. (31 de JULY de 2020). Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward. (J. o. Law, Ed.) Retrieved from OXFORD ACADEMY: https://academic.oup.com/jcsl/article/25/3/423/5879500
31. Nicholas Tsagourias, M. F. (2020). Cyber Attribution: Technical and Legal Approaches and Challenges. Retrieved from European Journal of International Law: https://sites.tufts.edu/cilg/files/2018/09/attributiondraftsm.pdf
32. Ottis, R. (s.d.). Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective. Retrieved from CCDCOE: https://www.ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
33. Palleti, V. R., Adepu, S., Mishra, V. K., & Mathur, A. (2021). Cascading effects of cyber-attacks on interconnected critical infrastructure. Retrieved from Springer: https://cybersecurity.springeropen.com/articles/10.1186/s42400-021-00071-z
34. Roguski, P. (2020). Application of International Law to Cyber Operations: A Comparative Analysis of States' Views. Retrieved from THE HAGUE PROGRAM FOR CYBER NORMS: https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views
35. Sachariew, K. (s.d.). States' entitlement to take action to enforce international humanitarian law. Retrieved from ICRC: https://international-review.icrc.org/sites/default/files/S0020860400073058a.pdf
36. Schmitt, M. N. (2017). Peacetime Cyber Responses and Wartime Cyber Operations Under International. Peacetime Cyber Responses and Wartime Cyber Operations Under International.
37. Schöndorf, R. (DECEMBER de 2020). Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations. Retrieved from Stockton Center for International Law: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2957&context=ils
38. Solis, G. D. (2021). The Law of Armed Conflict: International Humanitarian Law in War. Cambridge University Press.

39. Solutions, A. (2023). Digital Forensics: The Military's Secret to Combating Cyber Threats. Retrieved from ADF Solutions: https://www.adfsolutions.com/adf-blog/digital-forensics-the-militarys-secret-weapon-to-combat-cyber-threats
40. Stevens, T. (2017). International Cooperation in Cyber Defence: A Framework for Policy and Strategy. Retrieved from Chatham House report: https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation
41. Stinissen, L. J., Minárik, T., Pissanidis, M. N., Veenendaal, M., & Glorioso, C. L. (2015). Study of Existing and Possible Rules of Engagement for Cyberspace. (CCDCOE, Ed.) Study of Existing and Possible Rules of Engagement for Cyberspace - CCDCOE, p. 44.
42. Tavares, M. I. (2015). Guerra e Responsabilidade - A intervenção militar no Iraque em 2003. PORTO: UNIVERSIDADE CATÓLICA PORTO EDITORA.
43. Toolkit, C. L. (s.d.). Sovereignty. Retrieved from Cyber Law Toolkit: https://cyberlaw.ccdcoe.org/wiki/Sovereignty
44. Tsagourias, N., & Buchan, R. (2021). Research Handbook on International Law and Cyberspace (2nd edition). Edward Elgar Publishing.
45. Tsagourias, N., & Morrison, A. (JUNE de 2023). What is International Humanitarian Law? Cambridge University Press. Retrieved from ADVISORY SERVICE ON INTERNATIONAL HUMANITARIAN LAW: https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf
46. Tulilahti, E. (2020). APPLICABILITY OF JUS IN BELLO TO CYBER WARFARE. Retrieved from TALLINN UNIVERISTY OF TECHNOLOGY: https://digikogu.taltech.ee/en/Download/b17cb193-f2a1-4619-8a87-0889aeefd56e
47. UNODA. (2023). Advancing Opportunities And Responsibilities for a Peaceful, Safer, and Rights Respecting Cyberspace. Retrieved from UNODA LIBRARY: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/MX_Temple_Microsoft_FINAL_compendium.pdf
48. UNODOC. (2019). International cooperation on cybersecurity matters. Retrieved from UNODOC: https://www.unodc.org/e4j/ar/cybercrime/module-8/key-issues/international-cooperation-on-cybersecurity-matters.html

49. WARNER, M. (2017). Understanding Cyber conflict: Intelligence in Cyber—and Cyber in Intelligence. Retrieved from Carnegie Endowment for International Peace: https://carnegieendowment.org/2017/10/16/intelligence-in-cyber-and-cyber-in-intelligence-pub-73393
50. WATCH, H. R. (2023). Questions and Answers: October 2023 Hostilities between Israel and Palestinian Armed Groups. Retrieved from HUMAN RIGHTS WATCH: https://www.hrw.org/news/2023/10/09/questions-and-answers-october-2023-hostilities-between-israel-and-palestinian-armed#Nine
51. Williams, B. T. (2014). The Joint Force Commander's Guide to Cyberspace Operations. The Joint Force Commander's Guide to Cyberspace Operations.
52. Williams, W. S., & Ford, C. M. (2020). Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare. Oxford University Press.