LEGAL PROTECTION OF CRITICAL INFRASTRUCTURES IN CYBERSPACE

A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF SOCIAL SCIENCES
OF
MIDDLE EAST TECHNICAL UNIVERSITY

BY

AHMET SEMİH PUR

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR
THE DEGREE OF MASTER OF SCIENCE
IN
THE DEPARTMENT OF INTERNATIONAL RELATIONS

MAY 2026

Approval of the thesis:

LEGAL PROTECTION OF CRITICAL INFRASTRUCTURES IN CYBERSPACE

submitted by **AHMET SEMİH PUR** in partial fulfillment of the requirements for the degree of **Master of Science in International Relations, the Graduate School of Social Sciences of Middle East Technical University** by,

Prof. Dr. Sadettin KİRAZCI
Dean
Graduate School of Social Sciences _____

Prof. Dr. Özgehan ŞENYUVA
Head of Department
Department of International Relations _____

Prof. Dr. Necati POLAT
Supervisor
Department of International Relations _____

Examining Committee Members:

Prof. Dr. Pınar BEDİRHANOĞLU (Head of the Examining Committee)
Middle East Technical University
Department of International Relations _____

Prof. Dr. Necati POLAT (Supervisor)
Middle East Technical University
Department of International Relations _____

Assoc. Prof. Dr. Kazım Sedat SİRMEN
Eskişehir Osmangazi University
Faculty of Law _____

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: Ahmet Semih PUR

Signature:

ABSTRACT

LEGAL PROTECTION OF CRITICAL INFRASTRUCTURES IN CYBERSPACE

PUR, Ahmet Semih
M.S., The Department of International Relations
Supervisor: Prof. Dr. Necati POLAT

May 2026, 206 pages

The increasing integration of cyberspace with critical infrastructures, which are essential to the well-being and healthy functioning of society and the State, has rendered them highly vulnerable to cyber threats. This thesis examines the legal protection of critical infrastructures in cyberspace from an international law perspective. It primarily focuses on how existing rules of international law can be interpreted and applied to address cyber operations targeting critical infrastructures. In doing so, this thesis also analyzes their applicability and contested aspects of their practical application.

This thesis first examines State jurisdiction in cyberspace within the framework of relevant international legal rules. It then explores ongoing discussions among States regarding the applicability of international law in cyberspace and development of non-binding cyber norms through international processes. Later, this thesis analyzes the applicability of relevant rules of international law during both peacetime and armed conflict, with a focus on key rules such as sovereignty, non-intervention, due diligence, the prohibition of the use of force and the rules of international humanitarian law.

Based on this legal analysis, this study demonstrates how these international legal rules may contribute to protect critical infrastructures in cyberspace.

This thesis argues that, despite ongoing interpretative differences and practical challenges, international law continues to apply in cyberspace and provides an important legal framework for protecting critical infrastructures against cyber operations.

Keywords: Cyberspace, critical infrastructures, international law, *jus ad bellum*, *jus in bello*

ÖZ

SİBER SAHADA KRİTİK ALTYAPILARIN HUKUKİ KORUNMASI

PUR, Ahmet Semih
Yüksek Lisans, Uluslararası İlişkiler Bölümü
Tez Yöneticisi: Prof. Dr. Necati POLAT

Mayıs 2026, 206 sayfa

Siber sahanın kritik altyapılarla giderek artan şekilde bütünleşmesi, toplumun ve devletin refahı ile sağlıklı işleyişi açısından hayati öneme sahip olan bu altyapıları siber tehditlere karşı oldukça kırılgan hale getirmiştir. Bu tez, kritik altyapıların siber sahada korunmasını uluslararası hukuk perspektifinden incelemektedir. Çalışma, özellikle mevcut uluslararası hukuk kurallarının kritik altyapıları hedef alan siber operasyonlara nasıl yorumlanıp uygulanabileceğine odaklanmaktadır. Bu çerçevede tez, söz konusu kuralların uygulanabilirliğini ve pratikteki uygulamalarına ilişkin tartışmalı yönleri de analiz etmektedir.

Tez, ilk olarak siber sahada devlet yetkisini ilgili uluslararası hukuk kuralları çerçevesinde incelemektedir. Ardından, devletler arasında siber uzayda uluslararası hukukun uygulanabilirliğine ilişkin süregelen tartışmaları ve uluslararası süreçler aracılığıyla bağlayıcı olmayan siber normların geliştirilmesini ele almaktadır. Daha sonra çalışma, barış zamanı ve silahlı çatışma dönemlerinde ilgili uluslararası hukuk kurallarının uygulanabilirliğini; özellikle egemenlik, içişlerine karışmama, gerekli özeni gösterme, kuvvet kullanma yasağı ve uluslararası insancıl hukuk kuralları gibi temel ilkeler ışığında analiz etmektedir. Bu hukuki analiz temelinde tez, söz konusu

uluslararası hukuk kurallarının siber sahada kritik altyapıların korunmasına nasıl katkı sağlayabileceğini ortaya koymaktadır.

Bu tez, devam eden yorum farklılıkları ve uygulamadaki zorluklara rağmen, uluslararası hukukun siber sahada uygulanmaya devam ettiğini ve kritik altyapıların siber operasyonlara karşı korunması açısından önemli bir hukuki çerçeve sunduğunu ileri sürmektedir.

Anahtar Kelimeler: Siber saha, kritik altyapılar, uluslararası hukuk, *jus ad bellum, jus in bello*

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my supervisor Prof. Dr. Necati Polat for his guidance during this process. I would like to also thank rest of my thesis committee; Prof. Dr. Pınar Bedirhanoğlu and Assoc. Prof. Dr. Kazım Sedat Sirmen, for their insightful comments, encouragement, criticism and suggestions.

I am deeply grateful to my family: my mother, Hatice, who has brought me to where I am today; my brothers, Emir Vefa and Volkan, who has always stood by my side; my dearest Merve, who has given me the strength to keep moving forward.

My heartfelt thanks also go to my lifelong friends, who have been my side since the very beginning. I am fortunate to have so many of them that I cannot name each individually, and I am grateful for their support throughout this journey.

Lastly, I would like to thank my superiors and colleagues in the Grand National Assembly of Türkiye for being part of this journey and for their support. I would especially like to thank Dr. Handan Karakaş Demir for the many things she has taught me and for being a source of inspiration for the years to come.

TABLE OF CONTENTS

PLAGIARISM iii

ABSTRACT iv

ÖZ vi

ACKNOWLEDGMENTS viii

TABLE OF CONTENTS ix

LIST OF ABBREVIATIONS xiii

CHAPTERS 1

1. INTRODUCTION 1

2. INTERNATIONAL LAW AND CYBERSPACE 6

2.1. State Jurisdiction in International Law 7

2.1.1 Principle of Territoriality 10

2.1.2 Principle of Nationality 12

2.1.3 Protective Principle 13

2.1.4 Principle of Universality 15

2.2. Applicability of International Law in Cyberspace 16

2.3. State Jurisdiction in Cyberspace 30

3. PEACETIME PROTECTION OF CRITICAL INFRASTRUCTURES 37

3.1. Concept of Critical Infrastructure 37

3.2. Sovereignty 41

3.2.1. Sovereignty in Cyberspace 45

3.2.2. Sovereignty and Critical Infrastructures 50

3.3. Non-Intervention 52

3.3.1. Concept of *Domaine Réservé* 54

3.3.2. Element of Coercion 55
3.3.3. Non-Intervention in Cyberspace 59
3.3.4. Non-Intervention and Critical Infrastructures 62
3.4. Due Diligence 65
3.4.1. Due Diligence in Cyberspace 69
3.4.2. Due Diligence and Critical Infrastructures 72
3.5. Prohibition of Threat/Use of Force 73
3.5.1. Prohibition of Threat of Force 76
3.5.2. The Right of Self-Defense 80
3.5.2.1. Individual Self-Defense 82
3.5.2.1.1. Armed Attack Threshold 82
3.5.2.1.2. The Elements of Necessity, Proportionality and Immediacy 84
3.5.2.1.3. Notification of the UN Security Council 87
3.5.2.2. Collective Self-Defense 87
3.5.3. Prohibition of Threat/Use of Force in Cyberspace 88
3.5.3.1. Cyber Operations That Cause Physical Damage to Objects or Injury/Death to Persons 92
3.5.3.2. Non-Destructive or Non-Injurious Cyber Operations 93
3.5.4. Prohibition of Threat of Force in Cyberspace 95
3.5.5. The Right of Self-Defense in Cyberspace 96
3.5.6. Prohibition of Threat/Use of Force and Critical Infrastructures 101
4. PROTECTION OF CRITICAL INFRASTRUCTURES IN ARMED CONFLICT 106
4.1. Applicability of International Humanitarian Law: Cyber Armed Conflicts 108
4.1.1. International Armed Conflicts 111
4.1.2. Non-International Armed Conflicts 114

4.1.3. Notion of Attack in International Humanitarian Law 117
4.1.4. Applicability of International Humanitarian Law in Cyberspace 118
4.1.4.1. Notion of Attack in Cyberspace 121
4.2. Distinction 127
4.2.1. Prohibition of Targeting Civilians 128
4.2.2. Prohibition of Targeting Civilian Objects 130
4.2.3. Prohibition to Conduct Indiscriminate Attacks 133
4.2.4. Special Protection Granted by IHL 135
4.2.4.1. Medical Units 135
4.2.4.2. Objects Indispensable to the Survival of the Civilian Population 137
4.2.4.3. Works and Installations Containing Dangerous Forces 138
4.2.5. Distinction in Cyberspace 140
4.2.5.1. Question of Dual-Use Objects 142
4.2.5.2. Question of Data 145
4.2.6. Distinction and Critical Infrastructures 148
4.3. Proportionality 149
4.3.1. Proportionality in Cyberspace 151
4.3.2. Proportionality and Critical Infrastructures 153
4.4. Precautions 154
4.4.1. Active Precautions 155
4.4.2. Passive Precautions 158
4.4.3. Precautions in Cyberspace 160
4.4.4. Precautions and Critical Infrastructures 164
5. CONCLUSION 167
BIBLIOGRAPHY 174
APPENDICES 187

A. TABLE OF AUTHORITIES.....187

B. TURKISH SUMMARY / TÜRKÇE ÖZET.....195

C. THESIS PERMISSION FORM / TEZ İZİN FORMU.....206

LIST OF ABBREVIATIONS

AP I	Additional Protocol I to the 1949 Geneva Conventions
AP II	Additional Protocol II to the 1949 Geneva Conventions
ASEAN	Association of Southeast Asian Nations
AU	African Union
CI	Critical Infrastructure
EU	European Union
G7	Group of Seven
G20	Group of Twenty
GC	1949 Geneva Conventions
GC I	First Geneva Convention
GGE	Group of Governmental Experts
GPS	Global Positioning System
IAC	International Armed Conflict
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICT	Information and Communications Technology
ICTY	International Criminal Tribunal for the Former Yugoslavia
IHL	International Humanitarian Law
ILC	International Law Commission
ITLOS	International Tribunal for the Law of the Sea
LOAC	Law of Armed Conflict
MFA	Ministry of Foreign Affairs
NIAC	Non-International Armed Conflict
OEWG	Open-Ended Working Group
PCIJ	Permanent Court of International Justice
UK	United Kingdom
UN	United Nations
UNGA	United Nations General Assembly

UNSC	United Nations Security Council
US	United States
VCLT	1969 Vienna Convention on the Law of Treaties

CHAPTER 1

INTRODUCTION

Since its emergence in the second half of the 20th century, cyberspace has transformed from an initially limited information-sharing network into a global “fifth domain” of human conduct, affecting nearly every aspect of life. It has become increasingly integrated into social, economic, and political spheres, significantly impacting how individuals, societies, States, and companies behave. This growing integration trend is likely to continue with the emergence of new technologies such as artificial intelligence, the Internet of Things, blockchain, cloud computing, quantum computing, and advanced communication technologies, further incorporating cyberspace into the daily functioning of modern societies. As a result, the importance of cyberspace for individuals, societies, and States will inevitably increase.

Alongside its increasing significance in human and societal life, cyberspace has also become more prominent in international relations. States not only use the communication opportunities provided by cyberspace to hold conferences and negotiations but also increasingly employ cyberspace as a tool of foreign policy, developing cyber strategies and acquiring cyber capabilities. As a tool of foreign policy, States conduct various cyber operations, such as disinformation campaigns, espionage, and attacks against critical infrastructures, to achieve their goals. In this context, cyberspace has become both a platform for diplomatic engagement and a domain of strategic competition between States.

Critical infrastructures are vital for daily life, the healthy functioning of society, the economy, and national security, because they provide essential services for modern living, such as energy generation, water supply, transportation, financial services, and health care. Disruption of critical infrastructures could cause significant harm to individuals, societies, and States. Similar to other aspects of human life, critical infrastructures are increasingly connected to cyberspace, computer systems, and cyber networks. While this growing integration offers benefits such as improved efficiency and resilience, it also makes critical infrastructures more vulnerable targets in cyberspace. A malicious cyber operation can disrupt critical infrastructure and cause serious harm from kilometers away without any physical force. Additionally, such an operation could have repercussions on other critical infrastructures due to the interconnectedness of cyberspace and networks. Given the importance of critical infrastructures for societies and States, the characteristics of cyberspace, and increased vulnerabilities, critical infrastructures have become a lucrative target for both States and non-State actors. The absence of a comprehensive international legal regime and ambiguity about how rules apply in cyberspace also complicate the issue. As a result, critical infrastructures increasingly constitute a target of cyber operations.

In response to increasing threats, protecting critical infrastructures in cyberspace has become a central topic on the States' agendas both nationally and internationally. States implement various measures such as developing legal frameworks, establishing institutional mechanisms, enhancing cyber capabilities, and pursuing international cooperation initiatives to improve the security of critical infrastructures in cyberspace. Discussions on how international legal rules apply, and the development of non-binding, voluntary norms for responsible State conduct in cyberspace between States, and sometimes with different stakeholders, stand as the most remarkable initiatives at the international level.

The increasing significance of cyberspace has led to notable implications for international law, the body of rules that governs conduct and relations between States.

The unique characteristics that distinguish cyberspace from the physical domains of human conduct, namely land, air, and sea, such as its interconnectedness, borderlessness, anonymity, and multiplicity of actors, have given rise to debates among States and within literature over how, and to what extent, international legal rules originally designed for these conventional domains can be applied to cyberspace, which is a non-physical and rapidly evolving domain.

Clarifying the scope and application of international legal rules in cyberspace is crucial for effectively protecting critical infrastructures, as it would enhance certainty, stability, and security by establishing a legal foundation for both State conduct and cooperation. Such measures would not only define the boundaries of what States can and cannot do in cyberspace but also foster cooperation among States, especially in tackling transnational cyber threats. In this context, this study aims to examine how international law safeguards critical infrastructures in cyberspace during both peacetime and armed conflicts. In the absence of a special legal regime governing cyberspace, the international legal rules relevant to the protection of critical infrastructures must be derived from the existing framework of international law and its primary sources. In this regard, the central question addressed in this study is how existing rules of international law can be interpreted and applied to protect critical infrastructures against cyber operations. This study is built upon the fundamental premise that cyberspace does not exist in a legal vacuum; rather, it constitutes a domain fully governed by the existing framework of international law.

Accordingly, the thesis first identifies the relevant international legal rules and explains their content. Second, it analyzes the positions of States on the applicability of these rules in cyberspace. Third, it examines their practical application, with particular attention to controversial aspects. Finally, it considers how these rules may be employed to protect critical infrastructures in cyberspace. While doing so, this thesis employs the term “cyber operations” to refer to malicious cyber conduct against critical infrastructures, covering a broad range of actions and also differentiating

between malicious cyber conduct and “cyber attacks” as defined under international humanitarian law. In its analysis, this thesis uses primary sources of international law, including international treaties, customary international law, general principles of international law, and its subsidiary means, including judicial decisions, and teachings of publicists such as books, articles, handbooks, reports, and commentaries.

The second chapter of this thesis focuses on State jurisdiction in cyberspace by analyzing relevant rules on State jurisdiction in international law. It then discusses debates among States, particularly within the United Nations (UN), regarding the applicability of international law in cyberspace. Finally, the chapter addresses cyber norm processes, which aim to develop soft law for responsible State conduct, involving different stakeholders.

The third chapter examines how critical infrastructures can be protected by international law during peacetime, focusing on relevant rules. It explains the content of these international legal principles, such as sovereignty, non-intervention, due diligence, and the prohibition of threat or use of force, followed by their application in cyberspace, including controversial aspects. After this analysis, the chapter examines the potential role these rules can play in protecting critical infrastructures in cyberspace. It also discusses whether cyber operations against critical infrastructures can trigger a State’s right of self-defense.

The fourth chapter discusses how international humanitarian law, the body of law applicable during armed conflicts, offers protection to critical infrastructures. In this context, the chapter first explains the conditions that trigger the applicability of international humanitarian law. Then, it addresses the concept of “attack” under international humanitarian law and how cyber operations can qualify as attacks, given that the rules of international humanitarian law apply to operations that qualify as attacks. Lastly, the chapter examines the content of relevant rules of international

humanitarian law, including the principles of distinction, proportionality, and precaution. It discusses their applicability in cyberspace and how they can protect critical infrastructures during armed conflict.

This thesis seeks to clarify the role that international law can play in protecting critical infrastructures in cyberspace. By examining the applicability and interpretation of relevant rules, this study aims to demonstrate how the existing international legal framework may contribute to regulating cyber operations and addressing cyber threats against critical infrastructures.

CHAPTER 2

INTERNATIONAL LAW AND CYBERSPACE

International order and law are based on States' sovereignty and sovereign equality. International law regulates conduct between sovereign States. In this regard, sovereignty "represents the basic constitutional doctrine of the law of nations."[1] It comes with a bundle of rights, one of which is the exercise of jurisdiction by the States. State jurisdiction means "the authority of a State to regulate conduct, persons or property within the limits of international law,"[2] and it also includes the capacity to enforce these rules upon persons.[3] Accordingly, State jurisdiction is one of the defining features of Statehood because it entails the power to regulate ordinary life and the conduct of ordinary people by legislative, executive, and judicial means within a State's territory,[4] and of course, "one of the most obvious forms of the exercise of sovereign power."[5] Its place in international law is undoubted as it addresses one of the core requirements of the international system, delimiting and legitimizing the regulatory authority of equal sovereigns.[6]

---

[1] James Crawford, *Brownlie's Principles of Public International Law*, 9th ed. (Oxford University Press, 2019), 431.

[2] Daniel Costelloe, "Conceptions of State Jurisdiction in the Jurisprudence of the International Court of Justice and the Permanent Court of International Justice," in *The Oxford Handbook of Jurisdiction in International Law*, ed. Stephen Allen, Daniel Costelloe, and Malgosia Fitzmaurice (Oxford University Press, 2019), 460.

[3] Christopher Staker, "Jurisdiction," in *International Law,* ed. Malcom Evans, 5th ed. (Oxford University Press, 2018), 289.

[4] Crawford, *Brownlie's Principles*, 440.

[5] *Legal Status of Eastern Greenland (Denmark v. Norway)*, Judgment, 1933 P.C.I.J. (ser. A/B) No. 53, at 48 (April 5).

[6] Alex Mills, "Rethinking Jurisdiction in International Law," *British Yearbook of International Law* 84, no.1 (2014): 187-188, https://doi.org/10.1093/bybil/bru003.

Jurisdiction is important for cyberspace given the fact that it is a corollary to State sovereignty, entitling them to regulate cyberspace and cyber conduct and to draw boundaries between equally sovereign States within cyberspace. Accordingly, this chapter first outlines the international legal framework on jurisdiction. It then examines how international law applies in cyberspace and, finally, analyzes the application of jurisdictional rules in that domain.

2.1. State Jurisdiction in International Law

Jurisdiction is "the power of the state under international law to regulate or otherwise impact upon people, property and circumstances" and is one of the main features of State sovereignty, as includes the exercise of authority which may alter, create or terminate legal relationships and obligations.[7] The rules and principles governing State jurisdiction derive from the broader framework of sources of international law, particularly customary law and in certain context treaty law.[8]

Regarding State jurisdiction, the Permanent Court of International Justice (PCIJ) states that "jurisdiction which, in principle, belongs solely to the State, is limited by rules of international law."[9] Accordingly, States are entitled to exercise their jurisdiction as long as they abide by the limits imposed by international law. This fact is also noted by the PCIJ as "all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty."[10]

The content of State jurisdiction is dynamic as observed by the PCIJ: "[T]he question whether a certain matter is or is not solely within the jurisdiction of a State is an essentially relative question; it depends on the development of international

[7] Malcolm N. Shaw, *International Law*, 8th ed. (Cambridge University Press, 2017), 500.

[8] Cedric Ryngaert, "Jurisdiction in International Law: United States and European Perspectives" (PhD diss., Katholieke Universiteit Leuven, 2007), 39 https://lirias.kuleuven.be/retrive/67311.

[9] *Nationality Decrees Issued in Tunis and Morocco of Nov. 8th, 1921*, Advisory Opinion, 1923 P.C.I.J. (ser. B) No. 4, at 23-24 (February 7).

[10] *S.S. Lotus (France v. Turkey),* Judgment, 1927 P.C.I.J. (ser. A) No.10, at 18 (September 7).

relations."[11] Since State jurisdiction depends heavily on international law, it can be fully understood with regard to the other features of international law.[12]

In international law, there are three types of State jurisdiction: the first is prescriptive jurisdiction, which refers to a State's power to legislate and make decisions;[13] the second is enforcement jurisdiction, which is a State's ability to take executive or judicial action to enforce its laws within or outside of its territory.[14] The third is adjudicative jurisdiction, which operationalizes both prescriptive and enforcement jurisdiction into practice and concerns the judicial branch of a State.[15] While the limits of prescriptive jurisdiction are less clear and will be discussed below, the limits of enforcement jurisdiction are more precise and strictly territorial.

States can exercise enforcement jurisdiction freely within their territory, but they cannot do so outside of their territory unless they obtain a sovereign State's consent or a custom or international treaty allow such enforcement.[16] Therefore, a State cannot apply legal measures to enforce its laws extraterritorially.[17]

Regarding prescriptive jurisdiction, two strands of thought can be identified for its scope. The first is the permissive approach, exemplified by the PCIJ's famous *Lotus* Case, which allows States to exercise jurisdiction as long as no international legal rule suggests otherwise.[18] Noting that international law does not impose a general prohibition on prescriptive jurisdiction, the PCIJ states that

---

[11] P.C.I.J., *Nationality Decrees*, 24

[12] Costelloe, "Conceptions of Jurisdiction," 460.

[13] Crawford, *Brownlie's Principles*, 440.

[14]Uta Kohl, "Jurisdiction in Network Society," in *Research Handbook on International Law and Cyberspace,* ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar Publishing, 2021), 75.

[15] Costelloe, "Conceptions of Jurisdiction," 457.

[16] Crawford, *Brownlie's Principles*, 462.

[17] Ryngaert, "Jurisdiction in International Law," 35.

[18] Ryngaert, "Jurisdiction in International Law," 32.

> [f]ar from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion which is only limited in certain cases by prohibitive rules; as regards other cases, every State remains free to adopt the principles which it regards as best and most suitable.[19]

Accordingly, under this approach, States are free to exercise extraterritorial prescriptive jurisdiction over persons, property, and acts as long as such actions are not prohibited by international law.[20] Jurisdiction is also plenary, as it is an aspect of sovereignty and thus only subject to restrictions voluntarily accepted by the sovereign State itself.[21] *Lotus* decision is regarded as "represent[ing] the high-water mark of *laissez-faire* in international relations, and an era that has been significantly overtaken by other tendencies"[22] and heavily criticized by international lawyers. However, it is still relied upon by States that assert jurisdiction.[23]

The second approach is the restrictive approach, which reflects customary international law, entitles States to exercise jurisdiction as long as they can base their claim on jurisdictional principles permitted by international law.[24] These principles of jurisdiction include territoriality and nationality, and although controversial, also the protective and universal jurisdiction principles.[25] This means that a State cannot exercise jurisdiction when it has no legitimate interest or is not affected by the activity in question, regardless of whether other sovereign States protest.[26] This approach is practiced by most States and endorsed by the majority of legal doctrine.[27]

---

[19] P.C.I.J., *SS Lotus*, 18-19.

[20] Ryngaert, "Jurisdiction in International Law," 36.

[21] Mills, "Rethinking Jurisdiction,"190.

[22] *Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium),* Judgment, 2002 I.C.J. Rep. 3, 79.

[23] Ryngaert, "Jurisdiction in International Law," 33.

[24] Staker, "Jurisdiction," 295.

[25] Mills, "Rethinking Jurisdiction,"196.

[26] Ryngaert, "Jurisdiction in International Law," 43.

[27] Ryngaert, "Jurisdiction in International Law," 33.

It is also worth mentioning that due to the numerous jurisdiction principles, concurrent jurisdiction between States is likely, and international law does not prohibit such situations.[28] Although international law does not regulate issues of concurrent jurisdiction, it contains an obligation for States "to exercise moderation and restraint as to the extent of the jurisdiction assumed by its courts in cases having a foreign element and to avoid undue encroachment on a jurisdiction more properly appertaining to"[29] another State. This reasonable exercising is also mentioned in the Third Restatement, which foresees that "a State may not exercise jurisdiction ... with respect to a person or activity having connections with another State when the exercise of such jurisdiction is unreasonable."[30] This reasonable exercise depends on various factors such as direct or substantial effect upon the territory, character of activity or interest of other States.[31] In addition, international comity, which refers to "courts of one State or jurisdiction giving effect to laws and judicial decisions of another State or jurisdiction, not as a matter of obligation but out of deference and mutual respect"[32] can also be utilized to curb jurisdiction conflicts between States.

After discussing the jurisdiction in general, the principles of jurisdiction in international law namely, the principle of territoriality, the principle of nationality, the protective principle, and universal jurisdiction will be discussed below.

2.1.1 Principle of Territoriality

The principle of territoriality is a key aspect of sovereignty: States hold sovereignty over specific areas of land, inland waters, territorial waters, its seabed, subsoil, airspace and exercise their authority within them. This principle also grants States the exclusive right to legislate and regulate public order within their territories, and as

[28] Mills, "Rethinking Jurisdiction,"199.

[29] *Barcelona Traction, Light and Power Company Limited (Belgium v. Spain),* Judgment, 1970 I.C.J. Rep. 3, 106.

[30] American Law Institute, *Restatement of the Law, the Foreign Relations Law of the United States*, (American Law Institute Publishers, 1987), § 403.

[31] Kohl, "Jurisdiction in Network Society," 88.

[32] Ryngaert, "Jurisdiction in International Law," 137.

noted, "the development of international law, have established this principle of the exclusive competence of the State in regard to its own territory."[33] Accordingly, territoriality serves as the primary rule governing all types of jurisdiction, including prescriptive jurisdiction; thus, subject to limitations imposed by international law, a State has the right to legislate on all matters within its territory and address external acts that affect it.[34] The primacy of territorial jurisdiction naturally stems from the principles of sovereign equality and non-intervention.[35]

States assert two types of territorial jurisdiction: the first is objective territorial jurisdiction, where a State exercises jurisdiction and applies its laws to events completed within its territory, irrespective of whether they began outside it; the second is subjective territorial jurisdiction, where a State exercises jurisdiction over an event that commenced within its territory but was completed elsewhere.[36] In addition to territorial jurisdiction, States may also extend their jurisdiction extraterritorially, provided they establish a specific basis accepted by international law.[37] Extraterritorial jurisdiction serves as a supplement to the territorial principle, which is the basis of the international jurisdictional order.[38] It is also important to note that States are obligated to demonstrate that they possess the necessary basis for asserting extraterritorial jurisdiction.[39]

Another concept related to the principle of territoriality is the effects doctrine, which permits a State to exercise jurisdiction if the effects of the act in question occur within

[33] *Island of Palmas Case (Netherlands v. USA),* Award, Apr. 4, 1928, 2 R.I.A.A. 829, 838.

[34] Mills, "Rethinking Jurisdiction,"196.

[35] Ryngaert, "Jurisdiction in International Law," 40.

[36] Staker, "Jurisdiction," 296-297.

[37] Crawford, *Brownlie's Principles*, 440.

[38] Mills, "Rethinking Jurisdiction,"197.

[39] Staker, "Jurisdiction," 295.

the State's territory, even if the act neither commenced nor concluded there.[40] The PCIJ recognized this doctrine in the *Lotus* case, where it asserted that a State may exercise jurisdiction "if one of the constituent elements of the offence, and more especially its *effects*, have taken place"[41] within that territory.

Accordingly, under the effects doctrine, a State can assert jurisdiction over an act that does not fully satisfy the criteria for the principle of territoriality or the protective principle.[42] Although the limitations of the effects doctrine in international law remain ill-defined, there is a growing acceptance among States of exercising jurisdiction based on this doctrine, provided certain conditions are met, with the United States (US) and the European Union (EU) being the most notable practitioners.[43] These conditions include a clear and internationally recognized interest, that the effects in question should be sufficiently direct and either intended or foreseeable, and that jurisdiction is exercised reasonably, with due regard for the interests of other States.[44]

2.1.2 Principle of Nationality

Although territorial jurisdiction is the primary basis for exercising jurisdiction, States may nevertheless exercise jurisdiction extraterritorially, provided they establish a specific basis recognized by international law. The principle of nationality serves as one basis for extraterritorial jurisdiction.

Nationality is defined as "a legal bond having as its basis a social fact of attachment, a genuine connection of existence, interests, and sentiments, together with the

[40] Julia Hörnle and Elif Mendos Kuskonmaz, "Criminal Jurisdiction—Concurrent Jurisdiction, Sovereignty, and the Urgent Requirement for Coordination," In *Internet Jurisdiction Law and Practice*, ed. Julia Hörnle (Oxford University Press, 2021), 84.

[41] P.C.I.J., *SS Lotus*, 23.

[42] Crawford, *Brownlie's Principles*, 447.

[43] Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017), 58.

[44] Schmitt, *Tallinn Manual,* 59.

existence of reciprocal rights and duties."[45] Thus, it is the bond between an individual and a State that grants reciprocal rights and duties. According to international law, States are free to determine the conditions under which they grant citizenship to individuals, legal entities, aircraft, and ships. However, this freedom is not absolute, as States must comply with international law.[46] States can extend their laws to their nationals, making the principle of nationality an accepted basis for jurisdiction in international law, where the bond between the subject (individual) and sovereign (State) serves as the connecting factor to the State's prescriptive power.[47]

The primary application of the nationality principle is the active personality principle, which views the State as a collective of persons under the same authority, irrespective of location, and allows a State to exercise jurisdiction over its nationals regardless of their location.[48] Although it is noted that the individual over whom the State seeks to exercise jurisdiction should be a national of the State at the time of the event, some States exercise jurisdiction over individuals who become nationals after the event in question.[49]

2.1.3 Protective Principle

Another basis accepted by international law regarding extraterritorial jurisdiction is the protective principle, under which States are entitled to exercise jurisdiction over acts that are detrimental to their vital interests related to external and internal security, as well as other key interests.[50] According to this principle, States can exercise jurisdiction when their vital interests are jeopardized, even if the act committed by the

[45] *Nottebohm Case (Liechtenstein v. Guatemala),* Second Phase, Judgment, 1955 I.C.J Rep. 4, 23.

[46] Staker, "Jurisdiction," 300.

[47] Mills, "Rethinking Jurisdiction," 198.

[48] Ryngaert, "Jurisdiction in International Law," 99-100.

[49] Ryngaert, "Jurisdiction in International Law," 101-103.

[50] Crawford, *Brownlie's Principles*, 446.

non-nationals outside of territory of the State.[51] Protective principle is a well-established concept, and many States have legislation based on the principle.[52] In addition, protective principle is also utilized in treaties providing for multiple jurisdictional grounds with regard to specific offences, such as 1979 Hostages Convention.[53] Only acts detrimental to vital State interests are included within the scope of protective principle, such as attempts upon the life or physical safety of key State officials; acts that are directed at forcibly overthrowing a State's government or seriously interfering with key State functions or national security, such as terrorism; and acts that are aimed at seriously compromising a State's financial solvency and stability, such as counterfeiting its currency or seriously compromising its banking system.[54]

This principle is linked to the State's political independence and sovereign equality; for it to operate, vital State interests must be threatened directly or indirectly, without requiring actual harm to occur.[55] The protective principle is closely related to the principles of territoriality and nationality, but it differs from them in significant ways: while territoriality and nationality are both inherent in modern Statehood, the protective principle is based on State interests and does not require these connections.[56] On the other hand, protective principle is different than the effects doctrine: While the protective principle is only limited to certain acts and does not require an effect to be happen upon the State's territory, effects doctrine is not limited to certain acts and requires an effect to happen.[57]

---

[51] Staker, "Jurisdiction," 301.

[52] Ryngaert, "Jurisdiction in International Law," 121.

[53] Shaw, *International Law*, 499.

[54] Schmitt, *Tallinn Manual,* 64.

[55] Ryngaert, "Jurisdiction in International Law," 120.

[56] Kenneth S. Gallant, *International Criminal Jurisdiction: Whose Law Must We Obey?* (Oxford University Press, 2022), 413.

[57] Schmitt, *Tallinn Manual,* 64.

2.1.4 Principle of Universality

The principle of universality as a principle of jurisdiction constitutes an exception to the general prohibition that a State cannot exercise jurisdiction unless it provides a basis accepted by international law. It entitles States to exercise jurisdiction over a crime solely based on its nature, "without regard to where the crime was committed, the nationality of the alleged or convicted perpetrator, the nationality of the victim, or any other connection to the State exercising such jurisdiction."[58] Accordingly, the principle of universality is linked to the nature of the crime, rather than any a connection between the State and the act in question. The fundamental logic of the principle of universality is that States have a legitimate interest in repressing certain crimes.[59] Today, many States include provision conferring universal jurisdiction in their criminal legislation in cases when State is bound by international law to prosecute a particular offense.[60]

While historically established for crimes like piracy and slave trade, principle of universality in modern era has largely transitioned into a treaty-based framework as the core crime against international law, which are now the main crimes subject to universal jurisdiction in modern times, were not subject to international criminalization but they became so by treaties such as 1948 Genocide Convention, 1949 Geneva Conventions and 1984 UN Torture Convention.[61] In this regard, the exercise of jurisdiction on the basis of principle of universality mostly operates through treaty obligations rather than as an autonomous jurisdictional principle. The scope of crimes subject to universal jurisdiction is controversial, dynamic, and open to modification.[62] It is important to note that States can introduce quasi-universal

[58] Ryngaert, "Jurisdiction in International Law," 540.

[59] Staker, "Jurisdiction," 302.

[60] Ryngaert, "Jurisdiction in International Law," 129.

[61] Ryngaert, "Jurisdiction in International Law," 548-549.

[62] Ryngaert, "Jurisdiction in International Law," 541.

jurisdiction through treaty regimes, which require States to exercise jurisdiction over specific individuals within their territory, regardless of any link.[63]

Regarding application, when a State wants to exercise jurisdiction based on the principle of universality, it must do so with a definition of the crime in question in line with international law.[64] Finally, under the principle of *aut dedere, aut judicare*, which requires States to either to prosecute or, failing that, to extradite a perpetrator to a place where he/she can be prosecuted, States may exercise universal jurisdiction on individuals present within their territory. However, the application of the universal principle *in absentia* remains controversial, as legal doctrine is reluctant to accept it, and State practice is lacking.[65]

Today, many States include provision conferring universal jurisdiction in their criminal legislation in cases when State is bound by international law to prosecute a particular offense.[66]

2.2. Applicability of International Law in Cyberspace

In recent years, States and international organizations have widely recognized that existing international law applies to States' cyber conduct as it does in physical domains, unless there is State practice and *opinio juris* to suggest otherwise.[67] However, given the debates within the UN on the applicability of international law to cyberspace, there are still disagreements on the exact scope and boundaries of the international legal framework governing cyber conduct.[68]

---

[63] Crawford, *Brownlie's Principles*, 454.

[64] Gallant, *International Criminal Jurisdiction*, 463.

[65] Ryngaert, "Jurisdiction in International Law," 556-557.

[66] Ryngaert, "Jurisdiction in International Law," 129.

[67] Harriet Moynihan, "The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace," *Journal of Cyber Policy* 6, no. 3 (2021): 395, https://doi.org/10.1080/23738871.2020.1832550.

[68] Kubo Mačák, "Unblurring the Lines: Military Cyber Operations and International Law," *Journal of Cyber Policy* 6, no 3 (2021): 413, https://doi.org/10.1080/23738871.2021.2014919.

The legal framework governing State conduct in cyberspace is anchored in the traditional sources of international law as defined in Article 38(1) of the Statute of International Court of Justice (ICJ), which includes international conventions, international custom, and general principles of law, while judicial decisions and scholarly writings function as subsidiary means for determination of legal rules.[69] In the absence of a comprehensive global cyber regime, the international legal rules that govern States' cyber conduct, which can be relied on to protect critical infrastructures, must be derived from the primary sources of international law, namely international treaties such as the Charter of United Nations and the Geneva Conventions of 1949, international custom, evidenced by State practice and *opinio juris*, and general principles of law. On the other hand, judicial decisions and scholarly writings can be utilized to determine the rules rather than serve as independent sources. Given their importance, it is useful to take a closer look at these primary sources and subsidiary means.

The first primary source of international law mentioned in Article 38 is the international conventions and treaties, which are defined in the 1969 Vienna Convention on the Law of Treaties (VCLT) as "an international agreement concluded between States in written form and governed by international law, whether embodied in a single instrument or in two or more related instruments and whatever its particular designation."[70] Promoting written treaties, the Vienna Convention at once recognizes the existence and validity of unwritten treaties.[71] Accordingly, treaties are written and unwritten agreements made by State parties in which they bind themselves to act in a particular way or establish a particular relationship, regardless of the designation of the agreement as a convention, pact, charter, statute, etc.[72] Treaties vary; they can be

[69] *Statute of the International Court of Justice*, June 26, 1945, 33 U.N.T.S. 993, Art. 38(1).

[70] *Vienna Convention on the Law of Treaties*, May 23, 1969, 1155 U.N.T.S. 331, Art. 2(1)(a).

[71] VCLT, Art. 3.

[72] Shaw, *International Law*, 69.

bilateral treaties that regulate narrow issues, or they can be multilateral treaties that establish a regime governing an entire field.[73]

In principle, only the parties to a treaty are bound by its terms, unless the treaty in question reflects customary international law or a non-party State accepts an obligation or benefit derived from the treaty based on the mutual consent of the parties and non-party State itself.[74] In addition, treaties may create objective regimes that produce legal effects with regard to non-party third States, thereby constituting an exception to the relative effect of treaties.[75] Such treaties establish international settlements, territories, boundaries and extraterritorial regimes and generate general legal effects.[76] The 1936 Montreux Convention Regarding the Regime of the Straits can be cited as an example of a treaty creating an objective regime.

The fact that obligations emanating from a treaty are binding upon the parties is based on the customary international law principle of *pacta sunt servanda*, which is expressed in VCLT.[77] The obligations imposed by a treaty to the parties continue to bind them unless and until the treaty is validly terminated, either in accordance with its provisions or by mutual consent of the parties.[78]

The second primary source of international law mentioned in Article 38 is the international custom, which is a general practice that is accepted as law by States. Traditionally, there are two elements of binding custom: the first is State practice, which refers to sufficient and consistent conduct by States in accordance with the alleged custom, and the second is the *opinion juris sive necessitates* (*opinio juris*),

[73] Anthea Roberts and Sandesh Sivakumaran, "The Sources of International Law," in *International Law*, 5th ed., ed. Malcolm D. Evans (Oxford: Oxford University Press, 2018), 91.

[74] Hugh Thirlway, *The Sources of International Law*, 2nd ed. (Oxford University Press, 2019), 43.

[75] Carlos Fernandez De Casadevante Romani, "Objective Regime," in *The Max Planck Encyclopedia of Public International Law*, ed. Rüdiger Wolfrum (Oxford: Oxford University Press, 2012), vol. VII, 912.

[76] De Casadevante Romani, "Objective Regime," 912.

[77] *VCLT*, Art. 26.

[78] Thirlway, *The Sources of International Law*, 49.

which requires the sufficient practice to be accompanied by a sense of legal right or obligation.[79] To form a binding international custom, both elements must be present cumulatively.

The first element of a binding international custom is State practice. State practice refers to acts conducted by a State in its capacity as a State by its organs, such as the judiciary, the legislature, the executive, the military and State officials.[80] State practice includes, but not limited to, diplomatic correspondence, legislation, case law, executive decisions and practices, official manuals on legal questions, opinions of government legal advisors, and statements by State officials.[81]

State practice has different elements, namely consistency, generality and duration, which must be evaluated relatively depending on the specific circumstances of each case.[82] As regards consistency, State practice must be exercised in a constant and uniform manner and must have some degree of uniformity; however, it does not need to be exercised in a perfect manner.[83] As regards generality, it is important to look at the reaction of other States concerned; affirmation, acquiescence or protest may impact whether the rule constitutes a customary rule, affirmation helping the creation of a customary rule clearly and quickly, whereas acquiescence may be sufficient depending on the circumstances.[84] As regards duration, there is no particular duration for the practice, and long-standing practice is not necessarily required; rather, the necessary duration depends on the circumstances.[85] On the other hand, settled State practice does

[79] Thirlway, *The Sources of International Law*, 65.

[80] Roberts and Sivakumaran, "The Sources of International Law," 93.

[81] Crawford, *Brownlie's Principles*, 21-22.

[82] Roberts and Sivakumaran, "The Sources of International Law," 93.

[83] Shaw, *International Law*, 56.

[84] Roberts and Sivakumaran, "The Sources of International Law," 93.

[85] Crawford, *Brownlie's Principles*, 22.

not need to be universal and practiced by every State, rather it must be widespread, representative and consistent.[86]

The second element of a binding international custom is *opinio juris*, which refers to the belief that State practice is exercised with a sense of legal right or obligation.[87] *Opinio juris* is the element that separates legally required or permitted practice from the acts of comity or courtesy.[88] *Opinio Juris* can be expressed in a variety of ways such as public statements made on behalf of States, official publications, governmental legal opinions, diplomatic correspondence, decisions of national courts, treaty provisions, and conduct in connection with resolutions adopted by international organization or at intergovernmental conference.[89] In addition, UN General Assembly resolutions can also provide evidence for the existence of *opinio juris*.[90] Just as State practice, the *opinio juris* also depends on both the State asserting the right or obligation and the reactions of other States.[91]

Contrary to treaties, international custom binds all States without exception from the moment it is established as a custom. While it is necessary to establish that a State is bound by a treaty in a dispute on a rule of treaty law, it is sufficient to prove the existence of an international custom if the disputed rule forms part of customary law.[92] There are two exceptions to this general rule: the status of the persistent objector and local custom.[93] Accordingly, if a State opposes the existence of a custom during its formation, it may opt out of the rule, provided that opposition is expressed clearly,

---

[86] Thirlway, *The Sources of International Law*, 78.

[87] Thirlway, *The Sources of International Law*, 85.

[88] Roberts and Sivakumaran, "The Sources of International Law," 96.

[89] Tullio Treves, "Customary International Law," in *The Max Planck Encyclopedia of Public International Law*, ed. Rüdiger Wolfrum (Oxford University Press, 2012), vol. II,943.

[90] Thirlway, *The Sources of International Law*, 92.

[91] Shaw, *International Law*, 64.

[92] Thirlway, *The Sources of International Law*, 63.

[93] Crawford, *Brownlie's Principles*, 26-27.

held persistently and made known to other States.[94] It should be underlined that the persistent objector status can only attained if the State in question objects to the custom from its formation; once the rule is established, it is not possible to gain the status by objecting to the rule.[95]

The second exception is local custom, which may be formed within a particular region or even between two States and binds only the States concerned.[96] For a such custom to emerge, all States need to positively accept the rule in question and the standard of proof required is higher than that required for general custom.[97]

With regard to the interaction with the treaty and customary law, an obligation stated in a treaty may also be included in customary law in three ways: first, a treaty may be made to embody, record or codify obligations already included in customary law; second, it is possible that a treaty can play a role in crystallizing a rule that was widely followed by States before the treaty is made; and lastly, a treaty provision may contribute to the emergence of a new rule of customary international law.[98] If treaty and customary law collide, this does not automatically result in an irreconcilable contradiction, as several norms relating to the same subject matter should be interpreted in a manner that produces a compatible set of obligations to the extent possible.[99]

The last primary source of international law mentioned in Article 38 is the general principles of law. General principles of law were introduced by the Advisory Committee of Jurists, who prepared the draft of PCIJ Statute, to cover the gap that

[94] Thirlway, *The Sources of International Law*, 100.

[95] Roberts and Sivakumaran, "The Sources of International Law," 97.

[96] Crawford, *Brownlie's Principles*, 27.

[97] Shaw, *International Law*, 68-69.

[98] Thirlway, *The Sources of International Law*, 148-149.

[99] Thirlway, *The Sources of International Law*, 152.

would emerge in international law and prevent the situation of *non liquet*.[100] General principles of law play an important role in the implementation of rules of international law that come from custom and treaties; as such, they are not substantive rules creating new legal obligations. Rather, they operate as principles governing the functioning and application of the legal system, thus relating to its *modus operandi*.[101] For instance, the principle of good faith does not determine the substantive content of a State's obligations; rather it guides the performation or interpretation of these obligations. Similarly, principle of *res judicata* is recognized by international courts in regulating procedural matters and ensuring finality in adjudication. Accordingly, general principles of law as a primary source make it possible to formulate legal rules capable of filling the gaps and weaknesses where customary and treaty law are insufficient; they constitute a broader normative framework for the interpretation and application of customary and treaty law, and they may also generate rules of independent legal force.[102] In this sense, general principles of international law contribute to the interpretation, coherence, and procedural operation of international law.

General principles of law can be derived by comparison of different municipal law systems or may also include general principles applicable directly to relations between States.[103] Compared to customary law and treaty law, it is accepted that general principles of law have a limited scope of application, which is reflected in PCIJ and ICJ decisions.[104]

Apart from the primary sources, Article 38 also mentions subsidiary means, which are judicial decisions and the teachings of publicists. The reason why judicial decisions and teachings of publicists are classified as subsidiary means is that they state the rule

[100] Shaw, *International Law*, 73.

[101] International Law Commission, *Report of the International Law Commission: Seventy-fourth Session (24 April–2 June and 3 July–4 August 2023)* (United Nations, 2023), 29-30. https://docs.un.org/en/a/78/10.

[102] Thirlway, *The Sources of International Law*, 111-112.

[103] Crawford, *Brownlie's Principles*, 32.

[104] Shaw, *International Law*, 73.

because it was derived from the primary sources of international law, rather than creating the rule by themselves.[105] Accordingly, judicial decisions as a subsidiary means include decisions given by international tribunals, including the ICJ and other tribunals, and also decisions given by municipal courts.[106] Decisions of municipal courts might provide evidence of State practice regarding the matter and offer an analysis of the international legal rules involved.[107] Judicial decisions are important for the practice and development of international law, given that they apply and interpret the law, and international law develops through interpretation considerably.[108]

On the other hand, teachings of publicists played an important role in the development of international law historically, but their importance has decreased today, as the emphasis has shifted towards the contribution made judicial decisions.[109] Nevertheless, teachings of publicists continue to remain relevant, as States and international courts continue to cite and quote such teachings in their claims and decisions.[110] They also play a significant role in organizing and clarifying the structure of international law, as well as in elaborating the nature, historical development, and practical application of legal rules.[111]

Apart from the fact that subsidiary means have a subordinate function when compared to primary sources, and that general principles of law have a more complementing role with regard to customary and treaty law, Article 38 does not express a hierarchy or priority between rules emanated from the different primary sources.[112] However,

[105] Roberts and Sivakumaran, "The Sources of International Law," 99.

[106] Thirlway, *The Sources of International Law*, 140.

[107] Crawford, *Brownlie's Principles*, 38.

[108] Roberts and Sivakumaran, "The Sources of International Law," 108.

[109] Roberts and Sivakumaran, "The Sources of International Law," 133.

[110] Roberts and Sivakumaran, "The Sources of International Law," 99.

[111] Shaw, *International Law*, 84.

[112] Shaw, *International Law*, 92.

peremptory norms (*jus cogens)* of the international law should be mentioned, given that it is stated in the VCLT that "A treaty is void if, at the time of its conclusion, it conflicts with a peremptory norm of general international law."[113] Peremptory norms are defined by the VCLT as "a norm accepted and recognized by the international community of States as a whole as a norm from which no derogation is permitted."[114] It is also stated in the VCLT that a treaty is void if it conflicts with a newly emerged peremptory norm.[115] Accordingly, although a hierarchy of norms between different sources of international law does not exist explicitly in Article 38, the concept of peremptory norms implies a hierarchy as it prevails over contrary treaty and customary rules, and these rules cannot contradict the peremptory norms.[116] Examples of such peremptory rules are provided by International Law Commission and the include unlawful use of force, genocide, piracy, and slave trading.[117]

Apart from these sources and rules emanating from them, today there exist a category called "soft law," which is a system of international commitments or obligations that are not binding when compared to those imposed by international law but nevertheless constitute something more than mere political gestures, so there is an expectation of compliance even if there is no legal requirement to do so.[118] Accordingly, soft law is not binding as binding international legal rule emanating from the sources of international law, but it nevertheless has an influence on the international politics. Examples of such soft law include the resolutions of international organizations, programmes of action, texts of treaties which are not yet in force or are not binding for a particular actor, interpretative declarations to international conventions, non- binding agreements and codes of conduct, recommendations, and reports adopted by international agencies or within international conferences, as well as similar

[113] *VCLT*, Art. 53.

[114] *VCLT*, Art. 53.

[115] *VCLT*, Art. 64.

[116] Thirlway, *The Sources of International Law*, 177.

[117] Shaw, *International Law*, 94.

[118] Thirlway, *The Sources of International Law*, 188.

instruments and arrangements used in international relations to express commitments which are more than just policy statements but less than law in its strict sense.[119]

States create soft law instruments for various reasons: Firstly, given that soft law is not binding, it enables States to reach agreements easier and take on commitments they would not want to take in a binding treaty, giving them a freedom of action; secondly, soft law is more easier to amend, supplement, or repeal when compared to treaties, which enables States to respond more effectively to uncertainties arising from technical developments; thirdly, given that soft law instruments are not treaties, they are not subject to domestic treaty ratification processes; which makes it easier for States to adhere to them; finally, soft law instruments may constitute a more immediate evidence of international consensus when compared to a treaty.[120] In this regard, soft law has a complementary and strengthening function within the international legal order, as it helps to fill the gap between the need for norms in the realities of international relations and limited possibilities of international law's rudimentary problem-solving capacity.[121] In addition, soft law instruments may constitute a first step toward the making of a binding treaty, may be utilized for interpretation of treaties and provide evidence of the crystallization of customary rules.[122]

There have been various efforts to develop non-binding and voluntary cyber norms aimed at defining responsible State conduct in cyberspace. Norms can be defined as "collective expectations for the proper behavior of actors with a given identity."[123] These norms establish a higher, more desirable standard of responsible behavior, exceeding the minimum requirements set by international law.[124] Today, the

---

[119] Daniel Thürer, "Soft Law," in *The Max Planck Encyclopedia of Public International Law*, ed. Rüdiger Wolfrum (Oxford University Press, 2012), vol. IX, 270.

[120] Alan Boyle, "Soft Law in International Law-Making," in *International Law*, 5th ed., ed. Malcolm D. Evans (Oxford University Press, 2018), 123.

[121] Thürer, "Soft Law," 276.

[122] Boyle, "Soft Law in International Law-Making," 125-130.

[123] Martha Finnemore ve Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 438.

[124] Mačák, "Unblurring the Lines," 415.

development of cyber norms has become a policy tool employed by both States and private stakeholders to promote stability and security in cyberspace, given their flexible nature.[125] The norm development processes involve various stakeholders from both the private and public sectors; they can be aimed at more universal goals, done by a limited range of actors, and/or target a specific area.[126]

While cyber norms are dynamic, subject to reinterpretation by the actors and evolving as circumstances change over time, it is also worth noting that different norm processes can run simultaneously with overlapping or similar actors. Norms produced through such processes may operate concurrently in different contexts without clear hierarchy among them.[127] Norms generated through these different processes serve as "soft law" for cybersecurity in the absence of an international treaty governing cybersecurity issues.[128]

As mentioned above, various cyber norm processes initiated by different actors exist simultaneously today. Examples include multilateral efforts under the UN, Group of Twenty (G20), and Shanghai Cooperation Organization led by States; private sector-led initiatives such as the Global Commission on the Stability of Cyberspace, Charter of Trust (Siemens), and Cybersecurity Tech Accord (Microsoft); and multistakeholder processes like the Paris Call, Christchurch Call, and NETmundial Initiative.[129]

The UN General Assembly (UNGA) has actively discussed principles, elements, and good practices concerning Member States' behavior in the context of cybersecurity.[130]

---

[125] Finnemore and Hollis, "Constructing Norms," 426.

[126] Finnnemore and Hollis, "Constructing Norms," 426.

[127] Finnnemore and Hollis, "Constructing Norms," 428-429.

[128] François Delerue, *Cyber Operations and International Law* (Cambridge University Press, 2020), 24.

[129] Christian Ruhl et al., "Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads," Working Paper, (Carneige Endowment for International Peace, 2020), 3. https://carnegieendowment.org/research/2020/02/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-a-crossroads?lang=en

[130] Christian Henderson, "The United Nations and the Regulation of Cyber-Security," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar Publishing, 2021), 589.

Since 1998, six Groups of Governmental Experts (GGE) and two Open-Ended Working Groups (OEWG) within the UN have been established to examine "how international law applies to the use of information and communications technologies by States."[131]

The third GGE, which issued its report in 2013, was the first important breakthrough. The report was a significant success because it affirmed that existing international law applies in cyberspace and that additional norms can be developed over time. The report also highlighted that "State sovereignty and the international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities."[132]

After the UNGA adopted the third GGE report, it established a fourth GGE to explore the discussed issues further. Additionally, UNGA requested the fourth GGE to examine how international law applies in this context. The fourth GGE commenced its work and issued a consensus report in 2015. The 2015 report reaffirms the conclusions of the 2013 report, particularly that the UN Charter "applies in its entirety,"[133] and emphasizes the "inherent right of States to take measures consistent with international law and as recognized in the Charter."[134] It also referred to the principles of humanity, necessity, proportionality, and distinction, which are core principles of international humanitarian law, along with the principles of sovereignty, sovereign equality, peaceful dispute resolution, and non-intervention.[135]

---

[131] United Nations General Assembly, *Developments in the Field of Information and Telecommunications in the Context of International Security*, A/RES/73/27 (Dec. 5, 2018), https://docs.un.org/en/A/res/73/27

[132] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (United Nations General Assembly, 2013), 8, https://digitallibrary.un.org/record/753055?v=pdf

[133] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (United Nations General Assembly 2015), 12, https://digitallibrary.un.org/record/799853?v=pdf

[134] UN GGE, *2015 Report*, 12.

[135] UN GGE, *2015 Report*, 12-13.

The report's most significant advancement was the proposal of 15 non-binding norms for responsible State behavior and confidence-building measures in cyberspace[136] Upon adoption, UNGA urged member States "to be guided in their use of information and communications technologies by the 2015 report."[137] In addition to the United Nations, the EU, the Group of Seven (G7), G20, and the Association of Southeast Asian Nations (ASEAN) have endorsed the list of norms, either referring to them or incorporating them in their declarations.[138]

After the report, the UNGA established a new fifth GGE. Unlike the previous GGEs, the fifth GGE concluded its work without a consensus report, marking a significant setback. Diverging views on international humanitarian law, the right of self-defense, and countermeasures led to this failure. While the US wanted the report to include more explicit language, some countries, such as Russia, China, and Cuba, opposed this.[139]

After the failure of the Fifth GGE, the UNGA established two distinct groups to study cybersecurity and international law in 2018. The first was the OEWG, which was open to all member States, and the second was a new GGE comprised of 25 members. Russia and several other countries backed a proposal to create an OEWG. However, Russia's proposal was not well received by Western nations, who were concerned that the OEWG might become a battleground between two conflicting visions for the future of cyberspace: democratic and autocratic.[140]

---

[136] UN GGE, *2015 Report*, 7-9.

[137] UN GGE, *2015 Report*, 3.

[138] Marja Lehto, "The Rise of Cyber Norms," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar Publishing, 2021), 34.

[139] Ann Väljataga, "Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly," NATO Cooperative Cyber Defence Centre of Excellence (CDDCOE), accessed 25 November 2024, https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/.

[140] Heli Tiirmaa-Klaar, "The Evolution of the UN Group of Governmental Experts on Cyber Issues: From a Marginal Group to a Major International Security Norm-Setting Body," Paper (The Hague Centre for Strategic Studies, 2021), 7, https://hcss.nl/wp-content/uploads/2021/12/Klaar.pdf

Both processes issued their final reports in 2021. The GGE's 2021 report reaffirmed the 2015 Report's positions on international law and explicitly stated that rules of international humanitarian law apply to cyber operations conducted during an armed conflict.[141] However, the report left several issues unresolved, such as sovereignty, countermeasures, and due diligence.

The OEWG's 2021 Report reaffirmed the work of previous GGEs. It stated that international law applies to cyberspace and that non-binding norms of responsible State behavior help prevent conflict.[142] However, despite affirming international law, the 2021 OEWG report did not explicitly reference international humanitarian law. It mentioned that further common understandings of how international law applies to State use of ICTs must be developed.[143]

Apart from the UN, the process of how international law applies to cyberspace continues in different international organizations, most notably within NATO, which produced the influential *Tallinn Manual on the International Law Applicable to Cyber Warfare.* Consisting of 154 rules, the Manual seeks to comprehensively illustrate the general legal principles governing cyberspace, cyber conduct, and cyber operations and their interaction with various specialized international legal regimes by adapting the existing international legal framework to new circumstances through interpretation and analogies.[144] Although it is an academic work intended to guide questions regarding the application of international law in cyberspace, it has a significant influence on discussions surrounding international law and cyberspace. This impact is

---

[141] United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (United Nations General Assembly, 2021), 18, https://digitallibrary.un.org/record/3934214?v=pdf

[142] United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), *Final Substantive Report* (United Nations General Assembly, 2021), 4, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[143] UN OEWG, *2021 Report*, 5.

[144] Dan Efrony and Yuval Shany, "A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice," *American Journal of International Law* 112, no. 4 (2018): 583-584, https://doi.org/10.1017/ajil.2018.86.

evident in scholarly commentary, such as the observation that "with regard to certain pivotal legal doctrines … the Manual's contribution facilitated interpretations of the law that had previously been virtually inconceivable."[145]

2.3. State Jurisdiction in Cyberspace

After broadly outlining the framework of State jurisdiction in international law and discussing how international law applies in cyberspace, this section will address how international legal rules regarding State jurisdiction apply in cyberspace.

On the one hand, it has been established that international law mandates States to exercise jurisdiction over events in when they have a nexus with the matter in question, within the limits imposed by international law. This nexus can be established through the jurisdictional principles recognized under international law, namely the principles of territoriality, nationality, protective, and universality. States cannot exercise jurisdiction unless they base their claims on one of these principles. On the other hand, it is acknowledged by States and international organizations that existing international law applies to cyberspace and States' cyber conduct in the same manner as it does in the physical realm. The natural outcome of these findings is that international legal rules regulating State jurisdiction are applicable in cyberspace. Accordingly, States are entitled to exercise jurisdiction (prescriptive, judicial, and enforcement) over cyber activities within the constraints imposed by international law. Therefore, States must base their cyber jurisdiction claims on the principles of territoriality, nationality, protective, and universality.

The fact that States are entitled to exercise jurisdiction is affirmed in the GGE processes, where States acknowledged that "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory,"[146] and

[145] Henning Lahmann, "State Behaviour in Cyberspace: Normative Development and Points of Contention," *Zeitschrift Für Außen- Und Sicherheitspolitik* 16, no. 1 (2023): 34, https://doi.org/10.1007/s12399-023-00939-7.

[146] UN GGE, *2015 Report*, para 27.

also observed that States "exercise jurisdiction over the ICT infrastructure within their territory by, inter alia, setting policy and law and establishing the necessary mechanisms to protect ICT infrastructure on their territory from ICT-related threats."[147]

States' opinions on the matter mostly align with and support the conclusions of the GGE. For example, the common position of the African Union (AU) holds that "States are entitled to exercise jurisdiction, including legislative, adjudicative, and enforcement authority, over the components of cyberspace that are located on their territory."[148] The common position of the European Union also recognizes that "States exercise territorial jurisdiction over Information and Communications Technology (ICT) infrastructure located in their territory, and persons engaged in cyber activities, within their territory."[149]

Apart from these common positions, national positions on the matter also reach the same conclusion, as the US explicitly "acknowledge[s] the continuing relevance of territorial jurisdiction, even to cyber activities, and the exercise of jurisdiction by the territorial State … must also be consistent with applicable international law."[150] Additionally, China notes that "States should exercise jurisdiction over the ICT infrastructure, resources, data as well as ICT-related activities within their territories … States have the right to make ICT-related public policies, laws, and regulations."[151]

---

[147] UN GGE, *2021 Report*, para 71 (b).

[148] African Union Peace and Security Council, *Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace* (African Union, 2024), 2, https://papsrepository.africanunion.org/server/api/core/bitstreams/65bdfced-80d9-445b-b57f-31037616ccda/content

[149] Council of the European Union, *Declaration on a Common Understanding of International Law in Cyberspace* (European Union, 2024), 4, https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pdf.

[150] United Nations General 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 Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266 (A/76/136)* (United Nations, 2021), 139, https://digitallibrary.un.org/record/3933543?v=pdf

As can be seen from the GGE process and national positions on the matter, *opinio juris* on State jurisdiction in cyberspace favors the view that States are entitled to exercise jurisdiction in cyberspace, just as they are entitled to do in the physical world, within limits imposed by international law.

Given this affirmation and national positions on the matter, it can be said that States are entitled to exercise jurisdiction over cyber infrastructure within their territory and over cyber conduct related to that infrastructure.[152] On the other hand, States must base their jurisdiction claims over cyber activities conducted abroad, cyber infrastructure located abroad, or cyber conduct having effects within a State's territory on the jurisdictional principles accepted by international law.[153]

Firstly, Under the established framework of international law, States are entitled to exercise prescriptive, adjudicative and enforcement jurisdiction of over persons and objects located on its territory. Accordingly, States are entitled to exercise jurisdiction based on the principle of territoriality in cyberspace with regards to natural and legal persons present within the State's territory, who engage in cyber activities and cyber infrastructure and data located in the State's territory, cyber activities started or completed on its territory and cyber activities that originate, conclude or take place in its territory but have effects within.[154]

Secondly, states can exercise jurisdiction on the cyber activities of the natural or legal persons possessing the nationality of the State, irrespective of their geographic location.[155]

---

[151] Ministry of Foreign Affairs of the People's Republic of China, *China's Positions on International Rules-making in Cyberspace* (Ministry of Foreign Affairs of the People's Republic of China, 2021), 2, https://www.fmprc.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_11405183.html

[152] Kriangsak Kittichaisaree, *Public International Law of Cyberspace* (Springer International Publishing, 2017), 23.

[153] Schmitt, *Tallinn Manual,* 52.

[154] Schmitt, *Tallinn Manual,* 55-57.

[155] Schmitt, *Tallinn Manual,* 62.

Thirdly, States can exercise jurisdiction based on the protective principle if State's vital interests are threatened by cyber activities regardless of the perpetrator's location or nationality.[156]

Lastly, a State can exercise jurisdiction in cyberspace on the basis of principle of universality within the modern treaty-based frameworks if the cyberspace is utilized to commit crimes subject to principle of universality such as genocide, war crimes and torture, one example might be the committing a network intrusion to acquire the names of individuals belonging to certain race in a State census for preparation of a genocide.[157]

Regarding judicial jurisdiction, its scope is nearly identical to prescriptive jurisdiction: subject to immunities provided by international law, a State can exercise judicial jurisdiction over persons, objects, or conduct within the scope of its prescriptive jurisdiction.[158] At the same time, enforcement jurisdiction remains strictly territorial, just as in the physical realm: States are only entitled to exercise enforcement jurisdiction over cyber infrastructure, conduct, and persons affiliated with cyber activities within their territory, as well as ships and aircraft registered in that State unless they are granted necessary competence to exercise extraterritorial enforcement jurisdiction with the consent of another State, an international treaty, or custom.[159] If States exercise enforcement jurisdiction extraterritorially without the necessary competence, this action risks violating other States' sovereignty and independence.[160]

State practice further supports these arguments. In addition to the explicit endorsement of findings from the GGE processes by the UN General Assembly, States both legislate

[156] Schmitt, *Tallinn Manual,* 64.

[157] Schmitt, *Tallinn Manual,* 66.

[158] Schmitt, *Tallinn Manual,* 53.

[159] Schmitt, *Tallinn Manual,* 66-67.

[160] Benedikt Pirker, "Territorial Sovereignty and Integrity and The Challenges of Cyberspace," in *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, ed. Katherina Ziolkowski (NATO Cooperative Cyber Defence Centre of Excellence, 2013), 196.

and regulate cyberspace through their legislative authority and exercise cyber jurisdiction based on jurisdictional principles accepted by international law. For instance, the Council of Europe's Convention on Cybercrime (the Budapest Convention) allows States to exercise jurisdiction over cybercrime according to principles of territoriality and nationality.[161] Moreover, States increasingly regulate the Internet through their legislative powers, and today the majority of States have cyber legislation regulating various aspects Cyberspace.[162] Notable examples in this subject include Germany's Network Enforcement Law (2017),[163] the US Cybersecurity Information Sharing Act (2015),[164] the EU's General Data Protection Regulation (2016),[165] Russia's Sovereign Internet Law (2019),[166] China's Cybersecurity Law (2017),[167] and United Kingdom's (UK) Data Protection Act (2018).[168] Jurisdictional principles are also evident in the judgments of national courts. For example, in the case of LICRA *& UEJF v Yahoo! Inc & Yahoo France* (2000), the French court applied the protective principle to establish its jurisdiction.[169]

---

[161] Council of Europe, *Convention on Cybercrime (ETS No. 185)*, Budapest, 23 November 2001, Article 22. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[162] United Nations Conference on Trade and Development (UNCTAD), "Global Cyberlaw Tracker," accessed 12 April 2025, https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.

[163] Kohl, "Jurisdiction in Network Society," 79.

[164] "Federal Cybersecurity Information Sharing Act Signed into Law," Data Protection Report, 04 January 2016, https://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law/.

[165] European Union. *Regulation (EU) 2016/670 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation),* OJ L 119, 4 May 2016, 1-88.

[166] British Broadcasting Corporation (BBC), "Russia Internet: Law Introducing New Controls Comes into Force," 01 November 2019, https://www.bbc.com/news/world-europe-50259597.

[167] Rogier Creemers, Graham Webster, and Paul Triolo, "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)," DigiChina, accessed 12 April 2025, https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

[168] *Data Protection Act 2018*. King's Printer of Acts of Parliament., https://www.legislation.gov.uk/ukpga/2018/12/contents.

[169] Pirker, "Territorial Sovereignty and Integrity," 198.

Finally, it should be noted that the potential for concurrent jurisdiction in cyberspace is significant due to its cross-border nature and various jurisdictional principles.[170] In such circumstances, jurisdiction must be exercised in a reasonable manner that balances the affected State's regulatory authority with the sovereignty and interests of other States, as well as those of their citizens.

So far, it has been demonstrated that cyberspace is not a lawless zone, and that States can exercise their jurisdiction in cyberspace based on the jurisdiction principles in international law; and that international law applies in cyberspace, which is a fact that is no longer doubted by any State or international organization. In the absence of a special regime for cyberspace, international legal rules emanating from the different primary sources of international law, namely treaty, custom and general principles of law, apply in cyberspace, and any legal protection must emerge from the interpretation and application of existing rules.

The application of treaty law in cyberspace is subject to the rules of interpretation rules in the VCLT, which states that "A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose."[171] Accordingly, although instruments such as the UN Charter or the 1949 Geneva Conventions emerged well before the existence of cyberspace, their content can be applied to the realities of this new domain. On the other hand, the consensus reached by States within the GGE and OEWG processes as well as the increasing number of national positions published by States on the matter, can be regarded as evidence of crystallizing customary rules in cyberspace.

As regards subsidiary means, there is no judicial decision on cyberspace given by international courts, but they nevertheless be helpful, given that international legal rules, which emerged long before the cyberspace, continue to govern it. On the other hand, scholarly literature is utilized to determine the applicable law in cyberspace,

[170] Hörnle and Kuskonmaz, *Criminal Jurisdiction*, 82.

[171] *VCLT*, Art. 31.

particularly the prominent Tallin Manual. Rather than being the law itself, these subsidiary means are utilized to determine the rules emanating from the primary sources. Accordingly, the following chapters will analyze the protection of critical infrastructures in cyberspace through the framework provided by these sources.

CHAPTER 3

PEACETIME PROTECTION OF CRITICAL INFRASTRUCTURES

After discussing how international legal rules regarding jurisdiction apply in cyberspace and reviewing the current state of the discussions on the relationship between international law and cyberspace, this chapter focuses on the peacetime protection of critical infrastructures (CIs) in cyberspace. First, it defines the concept of CI and then examine how international law can be utilized to protect CIs in peacetime through the principles of sovereignty, non-intervention, due diligence, and the prohibition of the threat or use of force.

3.1. Concept of Critical Infrastructure

The concept of critical infrastructure "refers to infrastructures, assets or systems that a State considers to be essential for the maintenance of vital societal functions or pose potential serious risk to the population."[172] These infrastructures are deemed critical because their disruption or destruction could affect a State's national security and the socioeconomic well-being of its population. Due to their importance for national security and the well-being of the population, States view CIs as strategic assets that are becoming increasingly vital, which in turn heightens the risk of conflicts between States.[173] The notion of CI generally includes energy generation, transmission and distribution; air and maritime transport; banking and financial services; e-commerce;

[172] Delerue, *Cyber Operations,* 298.

[173] Jason Joley, "Recommendation 13 (f)," in *Voluntary Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology- A Commentary* (United Nations, 2017), 170.

water supply; food distribution; and public health.[174] This list is not exhaustive, as noted in relevant UN resolutions, each State has the right to define what constitutes CI.[175]

Designation of CI is not only a right but also an obligation as the UN Security Council (UNSC) "recognizes that each State determines what constitutes its critical infrastructure and how to effectively protect it."[176] CI includes both virtual and physical components and is often interconnected and interdependent. CIs also heavily rely on computer systems and networks, making them vulnerable to cyberattacks, and emerging technologies such as Machine Learning, Artificial Intelligence, and quantum computing increase threats to CIs.[177] This vulnerability has been evident in previous incidents, such as the Stuxnet attack (2010), the attack on the Ukrainian power grid (2015), and the US Colonial Pipeline incident (2021). In addition to these major attacks, States frequently conduct both direct and indirect low-level cyber operations targeting critical infrastructures, often employing proxies and criminals.[178]

It should be noted that there is no universally agreed upon or legally binding definition of the notion of CI. International law and other international instruments do not provide a legally binding definition; thus, States retain discretion to designate critical infrastructure.[179] Accordingly, States have the right to define the concept of CI and designate what constitutes CI according to their national interests and priorities.[180] In this regard, several States, such as the US, the UK, France, and Australia, and the EU,

---

[174] UN General Assembly, *Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures (A/RES/58/199)* (United Nations General Assembly, 2004). https://docs.un.org/en/A/RES/58/199

[175] UN General Assembly, *Culture of Cybersecurity*

[176] UN Security Council, *Resolution 2341* (S/*RES/2341)* (UN Security Council, 2017). https://docs.un.org/en/S/RES/2341(2017)

[177] Kristan Stoddart, *Cyberwarfare: Threats to Critical Infrastructure* (Palgrave Macmillan Cham, 2022), 23.

[178] Stoddart, *Threats to Critical Infrastructure,* 13-14.

[179] United Nations Office of Counter Terrorism (UNOCT), *The Protection of Critical Infrastructures Against Terrorist Attacks: Compendium of Good Practices* (United Nations, 2018), 38.

[180] Stoddart, *Threats to Critical Infrastructure,* 20.

as a non-State entity, have their own definition of CI and lists of sectors they consider critical. For instance, the EU defines CI as

> an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions.[181]

The EU also identifies 11 sectors as critical: energy; transport; banking; financial and market infrastructure; health; drinking water; wastewater; digital infrastructure; public administration; space; and food sectors.[182]

Most of the different definitions and lists designated by States include the sectors of governmental and public services; security; food; water; transportation; energy; health; finance; and banking.[183] While international law does not provide any criteria to designating CI either, function-based and effects-based approaches can be identified from the wide array of country definitions.[184] The function-based approach links criticality to the performance of essential societal functions, while the effects-based approach connects criticality to the effects of disruption or destruction.[185]

In addition to the designation of CIs, the UNSC also obliges States to effectively protect their own CIs. To this end, States apply various protection models that fit their unique characteristics, such as the threats faced, the size of the economy, political culture, institutional structure, or constitutional regime, since no single protection

---

[181] Council of the European Union, *Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection*, (European Union, 2008), Article 2.

[182] Council of the European Union, *Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC* (European Union, 2022), Annex I.

[183] Delerue, *Cyber Operations,* 299.

[184] UNOCT, *Compendium*, 39.

[185] UNOCT, *Compendium*, 39.

model exists two models can be identified.[186] The first model is the voluntary approach, which relies on self-regulation and voluntary compliance; public and private actors are invited to contribute to protection policy, and legislative and regulatory schemes are complementary.[187] The second model is a mandatory approach based on binding legal frameworks enforced by sanctions.[188] Rather than using the two models in their pure forms, States often employ hybrid models that incorporate elements from both.[189]

Addressing CI security in cyberspace has been on the agenda of States and international organizations since the development of ICTs in the 1990s. In light of the growing risks of potential adverse effects from malicious cyber operations against CIs, States, international organizations, and private entities have begun discussions on developing norms for CI protection.[190] The most notable outcome of these discussions was the UN GGE's 2015 Report, which offered several norms for responsible State behavior in cyberspace, including three norms regarding CIs. 2015 Report's norm (f) states that "[a] State should not conduct or knowingly support ICT activity… that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure."[191] Norm (g) urges that "States should take appropriate measures to protect their own CI from ICT threat"[192] and norm (h) provides that "States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory."[193]

---

[186] UNOCT, *Compendium,* 50.

[187] UNOCT, *Compendium,* 51.

[188] UNOCT, *Compendium,* 51.

[189] UNOCT, *Compendium,* 51.

[190] Michael Berk, "Recommendations 13 (g) and (h)," In *Voluntary Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology - A Commentary* (United Nations, 2017), 197.

[191] UN GGE, *2015 Report*, 8.

[192] UN GGE, *2015 Report*, 8.

[193] UN GGE, *2015 Report*, 8.

Concerning their contents, Norm (f), based on the law of State responsibility, prohibits States from knowingly or unknowingly engaging in cyber activity that would impact CI contrary to their existing obligations in international law.[194] On the other hand, norm (g) calls for States to adopt a comprehensive national framework that encompasses various aspects of CI protection, including political, conceptual, and institutional dimensions, to ensure appropriate protection of national critical infrastructure.[195] Lastly, Norm (h) promotes State cooperation in the face of malicious cyber operations against CIs and the prevention of emanating from such operations originating within their jurisdiction.[196] In addition to these norms, there are three more norms closely related to CI protection: norm (i), which concerns the integrity of supply chains; norm (j), which encourages States to report ICT vulnerabilities responsibly; and finally, norm (k), which protects the emergency response teams of other States.[197]

It can be argued that agreement on these norms demonstrates some level of understanding between States on critical infrastructures that should not be targeted. For instance, it is argued that States begin to accept norm (g) as a customary norm due to the growing number of cyber operations targeting CIs and increasing dependence on ICTs, which entails the adoption of national regulatory frameworks and implementing security measures for CI protection.[198]

3.2. Sovereignty

Sovereignty is the fundamental principle of international relations and law. In the *Nicaragua* case, the ICJ stated that international law rests upon it,[199] and the UN Charter remarks that "the organization is based on the principle of the sovereign

[194] Joley, "Recommendation 13 (f)," 189.

[195] Berk, "Recommendations 13 (g) and (h)," 209.

[196] Berk, "Recommendations 13 (g) and (h)," 219.

[197] Berk, Recommendations 13 (g) and (h)," 193.

[198] Berk, Recommendations 13 (g) and (h)," 203.

[199] *Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. USA),* Judgment, 1986 ICJ Rep. 14, para. 263.

equality of all its members."[200] 1928 arbitral award of the *Island of Palmas* clearly defined the principle as: "Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[201]

Historically, the sovereignty has served as a foundation for both domestic and international order since antiquity, and the concept itself has constantly evolved over time in three main dimensions: the subject of sovereignty, the nature of sovereignty, and the source of sovereignty.[202] The conception of sovereignty has shifted over time depending on historical and political contexts.

The modern conception of sovereignty officially dates back to the Peace of Westphalia in 1648, which formalized the territorial delimitation of State authority and the principle of non-intervention.[203] In modern times, the conception of sovereignty has evolved in tandem with the development of international law.[204] Although the concept internationalized in both its external and internal dimensions, this evolution does not signify the end of sovereignty but rather an adjustment to its modern form shaped by the developments of the 20th century.[205]

As a result of this evolution, the modern conception of sovereignty has witnessed the recognition of international organizations as subjects of international law, globalization, increasing interdependence between States, the extension of international law to fields previously considered domestic matters, the recognition of the rights of peoples and individuals before some international courts, and the notion

---

[200] *Charter of the United Nations and Statue of the International Court of Justice*, signed June 26, 1945, 1 U.N.T.S. XVI, Art. 2(1).

[201] *Island of Palmas,* 838.

[202] Samantha Besson, "Sovereignty," in *The Max Planck Encyclopedia of Public International Law*, ed. Rüdiger Wolfrum, 1st ed., vol. 9 (Oxford University Press, 2012), 368.

[203] Besson, "Sovereignty," 368.

[204] Besson, "Sovereignty," 371.

[205] Besson, "Sovereignty," 372.

that States are obliged to encourage and protect the common values of the international community.[206]

Regarding the relationship between sovereignty and international law, it can be noted that standing between politics and law, sovereignty acts as both a foundation and a general principle of international law. At the same time international law comes to life by the consent of its subjects, namely sovereign States, yet it also defines, limits, and protects sovereign power in a community of equal sovereign States.[207]

Sovereignty in international law entails a bundle of rights: a State's right to territorial sovereignty, the right to independence of State powers, and principle of sovereign equality in the international order.[208]

In brief, territorial sovereignty encompasses a State's right over its land territory, airspace, and maritime zones, which together constitute the physical and social foundation of a State along with its government and population.[209] As a crucial aspect of sovereignty, territorial sovereignty empowers States to exercise their authority exclusively within their territories, independent of other States.[210] Consequently, territorial sovereignty refers to a State's right to exercise jurisdiction in its prescriptive, enforcement, and adjudicative forms, to regulate entry and exit to its territory,[211] and, lastly, its right to integrity and inviolability.[212]

---

[206] Katharina Ziolkowski, "General Principles of International Law as Applicable in Cyberspace," in *Peacetime Regime for State Activities in Cyberspace International Law, International Relations and Diplomacy,* ed. Katharina Ziolkowski (NATO Cooperative Cyber Defence Centre of Excellence), 156.

[207] Besson, "Sovereignty," 378-379.

[208] Moynihan, "Role of International Law," 398.

[209] Crawford, *Brownlie's Principles*, 191.

[210] Pirker, "Territorial Sovereignty and Integrity," 191.

[211] Wolff Heintschel von Heinegg, "Territorial Sovereignty and Neutrality in Cyberspace," *International Law Studies* 89, no. 1 (2013): 124.

[212] *Island of Palmas,* 839.

On the other hand, the right to independence of State powers entitles States to freely exercise their powers within the limits permitted by international law, which includes a State's right to political independence, the right to freely choose its political, economic, cultural, and social systems, and its right to exercise jurisdiction.[213]

Lastly, principle of sovereign equality means that all States have equal rights and duties as equal members of the international order, regardless of economic, social, or political differences or power imbalances within the international system, under which all States are equal before international law.[214] The principle strengthens the understanding that every State enjoys the same rights and is bound by the same obligations under the equal status granted by international law, and that sovereignty must be applied objectively.[215]

The rights granted by sovereignty are the basis for all the claims of violation. In addition to rights, the principle of sovereignty imposes obligations on States, such as refraining from threats or the use of force and not intervening in matters that fall within a State's domestic jurisdiction,[216] as well as adhering to the principle of due diligence and good neighborliness.[217] These obligations help to protect the sovereignty and territorial integrity of the other States.[218]

It should be noted that, contrary to flowing from sovereignty, these rights and duties constitute the concept of sovereignty itself, which is regarded as the "collective or

[213] Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention* (The Royal Institute of International Affairs, 2019), 12. https://www.chathamhouse.org/2019/12/application-international-law-State-cyberattacks

[214] Bruno Simma et al., eds., *The Charter of the United Nations: A Commentary*, 3rd ed. (Oxford University Press, 2012), 157-158.

[215] Moynihan, *Sovereignty and Non-Intervention,* 13.

[216] Simma, *UN Charter Commentary*, 158.

[217] Ziolkowski, "International Law as Applicable in Cyberspace," 165-171.

[218] Heintschel von Heinegg, "Territorial Sovereignty and Neutrality," 134.

umbrella term denoting the rights which, at a given time, a State is accorded by international law, and the duties imposed upon it by the same law."[219]

The sovereignty of a State may be violated when one State exercises its authority in another State's territory without the territorial State's consent, concerning an area where the territorial State holds the exclusive right to exercise its powers independently.[220] In this regard, PCIJ in its *Lotus* judgement underlined that "'first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State."[221]

In addition to territorial basis, sovereignty can also be violated by the interference or usurpation of inherently governmental functions.[222] Inherently governmental function can be defined as "a function that States alone have the authority to perform."[223] Functions such as tax collection, law enforcement, judiciary, policy making, and conducting elections can be given as examples of inherently governmental functions. Interference or usurpation of these functions without a State's consent would amount to a violation of sovereignty, regardless of the fact that sovereignty is violated on a territorial basis.

3.2.1. Sovereignty in Cyberspace

The international community reached a consensus that the sovereignty applies in cyberspace, with the 2013 and 2015 Reports explicitly referring to this principle. It is agreed that "State sovereignty and international norms and principles that flow from

[219] Simma, *UN Charter Commentary*, 155.

[220] Moynihan, "Role of International Law," 399.

[221] P.C.I.J., *SS Lotus*, 18.

[222] Michael N.Schmitt, "Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention*" International Law Studies* 96, no. 1 (2020): 556. https://digital-commons.usnwc.edu/ils/vol96/iss1/18/

[223] Schmitt, "Sovereignty and Intervention," 557.

sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory."[224]

The consensus reached in GGE processes is further supported by the State's opinion and practice on the matter. For instance, China states that "[t]he principle of sovereignty applies in cyberspace … State sovereignty in cyberspace is a legally binding principle under international law."[225] The US position emphasizes that "State sovereignty and the international principles that flow from sovereignty apply to States' ICT-related activities."[226] Russia also maintains that "the international community has reached consensus on the applicability of the universally accepted principles and norms of international law … These include, in particular, the principles of sovereign equality of States."[227] Lastly, France explicitly states that "[t]he principle of sovereignty applies to cyberspace. France exercises its sovereignty over the information systems located on its territory."[228]

It should also be noted that States exercise jurisdiction over and regulate cyberspace and continue to do so. Accordingly, the principle of sovereignty in cyberspace grants States the authority to control cyber infrastructure within their land territory, internal waters, territorial sea, and airspace, as well as regulate cyber activities. This principle encompasses physical (physical network components), logical (connection between networks), and social (persons and groups that conduct cyber activities) dimensions of cyberspace.[229]

---

[224] UN GGE, *2013 Report*, 8.

[225] MFA China, *China's Position*, 2.

[226] UNGA, *Official Compendium*, 139.

[227] UNGA, *Official Compendium*, 79.

[228] Ministry of Armed Forces of the French Republic, *International Law Applied to Operations in Cyberspace* (Ministry of Armed Forces, 2019), 3, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

[229] Schmitt, *Tallinn Manual,* 12.

Although there is a consensus that the sovereignty applies in cyberspace, how it can be violated is a subject of divergence. There are two approaches among States on this issue: One of the approaches, which can be named the "sovereignty as principle" argues that sovereignty itself is not a rule of international law that can be violated but rather it is a principle.[230] According to this approach, sovereignty does not operate as a stand-alone legal rule and cyber-attacks against States become unlawful If these attacks constitute intervention or use of force.[231] This perspective is supported by the UK, which states that "[t]he general concept of sovereignty by itself does not provide a sufficient or clear basis for extrapolating a specific rule of sovereignty or additional prohibition for cyber conduct going beyond that of non-intervention."[232]

Second approach is the "sovereignty as a rule" approach, which sees sovereignty as a stand-alone rule of international law whose violation has legal consequences. Under this approach, the principle of sovereignty operates on its own, and cyber operations against States can violations of sovereignty under certain circumstances.[233] This approach has been adopted by several countries, such as the Netherlands, France, Austria, Czechia, Finland, Iran, New Zealand, and Germany.[234] For instance, Germany states that

> State sovereignty constitutes a legal norm in its own right and may apply directly as a general norm also in cases in which more specific rules applicable to State behaviour, such as the prohibition of intervention or the use of force, are not applicable.[235]

---

[230] Moynihan, *Sovereignty and Non-Intervention,* 8.

[231] Samuli Haataja, "Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law," *International Journal of Law and Information Technology* 30, no. 4 (2022): 438, https://doi.org/10.1093/ijlit/eaad006.

[232] Suella Braverman, "International Law in Future Frontiers," speech, Chatham House, 19 May 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers

[233] Haataja, "Operations Against Critical Infrastructure," 436.

[234] Haataja, "Operations Against Critical Infrastructure," 436.

[235] Federal Government of Germany, *On the Application of International Law in Cyberspace* (Federal Government of Germany, 2021), 3, https://www.auswaertiges-amt.de/resource/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

This study argues that interpreting sovereignty as a binding legal rule offers a stronger protection for CIs. If sovereignty is viewed only as a general principle as some States advocate, many cyber operations that seriously harm or disrupt CIs without reaching intervention or use of force threshold would escape legal accountability. By considering sovereignty as an independent legal rule, international law can prohibit cyber operations that harm or disrupt CIs even if such operations do not cause physical destruction.

The Tallinn Manual also endorses "sovereignty as a rule" approach as Rule 4, stating that "[a] State must not conduct cyber operations that violate the sovereignty of another State."[236] According to Manual, Cyber operations that prevent or disregard another State's exercise of its sovereign prerogatives constitute a violation of such sovereignty and are prohibited by international law.[237]

However, there is a rift within the second approach regarding whether all cyber-attacks constitute a violation of sovereignty. Some advocate that any cyber intrusion violates sovereignty, while others assert that there is a certain minimal threshold for violation.[238] For instance, while France maintains that any cyber operation targeting "French digital systems or any effects produced on French territory by digital means by a State organ … constitutes a breach of sovereignty,"[239] New Zealand argues that "territorial sovereignty prohibits every unauthorised intrusion into a foreign ICT system or prohibits all cyber activity which has effects on the territory of another State."[240]

---

[236] Schmitt, *Tallinn Manual,* 17.

[237] Schmitt, *Tallinn Manual,* 17.

[238] Moynihan, "Role of International Law," 400.

[239] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 3.

[240] Ministry of Foreign Affairs and Trade of New Zealand, *The Application of International Law to State Activity in Cyberspace* (Ministry of Foreign Affairs and Trade of New Zealand, 2020), para. 14, https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

There is also disagreement among States about the degree of effects needed for a cyber act to constitute a violation of sovereignty. For instance, Finland observes without elaborating that "[w]hether an unauthorized cyber intrusion violates the target State's sovereignty depends on its nature and consequences and is subject to a case-by-case assessment."[241] On the other hand, Germany holds that a minimal threshold exists for violation of sovereignty and cyber operations that cause "physical effects and harm in the territory of another State" and also "[i]f functional impairments result in substantive secondary or indirect physical effects in the territory of the target State" then "a violation of territorial sovereignty will appear highly probable."[242]

As observed from these differing views, a consensus has yet to emerge on whether a mere intrusion is sufficient to constitute a violation of sovereignty, or if a *de minimis* criterion may apply in such situations, and if such a criterion exists, what degree of required damage qualifies as a violation of sovereignty.

On the other hand, Tallinn Manual asserts that a minimal threshold exists, concluding that cyber intrusions will only constitute a violation of sovereignty when a certain level of harmful effects is inflicted on the territory of the victim State.[243] According to Manual, these harmful effects include "physical damage or injury" and "remote causation of loss of functionality of cyber infrastructure located in another State."[244] Manual also states that State cyber operations constituting interference with, or usurpation of, inherently governmental functions of another State violates principle of sovereignty, regardless of whether "physical damage, injury, or loss of functionality has resulted."[245]

---

[241] Ministry of Foreign Affairs of Finland, *International Law and Cyberspace* (Ministry of Foreign Affairs of Finland, 2020), 3, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

[242] Federal Government of Germany, *Application of International Law in Cyberspace*, 4.

[243] Moynihan, "Role of International Law," 400.

[244] Schmitt, *Tallinn Manual,* 20.

[245] Schmitt, *Tallinn Manual,* 22.

3.2.2. Sovereignty and Critical Infrastructures

Although cyberspace is a virtual and non-tangible domain, it relies on physical infrastructure such as cables, servers, and computer networks. These infrastructures are located within a State's territory and are subject to State sovereignty, which constitutes the geographical scope of principle of sovereignty in cyberspace.[246] States explicitly hold the view that infrastructures located in the territory of a State are subject to its sovereignty. One example can be seen in the common position of the EU, which observes that "States exercise territorial jurisdiction over Information and Communications Technology (ICT) infrastructure located in their territory."[247] Tallin Manual Rule 2 states that "[a] State enjoys sovereign authority with regard to the cyber infrastructure, persons, and cyber activities located within its territory, subject to its international legal obligations."[248]

The globally interconnected nature of these infrastructures does not remove States' sovereign rights over them.[249] A State uses its sovereign rights to the exclusion of other States, and it is entitled to take any measure it sees necessary or appropriate with regard to cyber infrastructure.[250] It does not matter that infrastructure in question is public owned or private owned.[251]

Accordingly, cyber operations targeting both the cyber and critical infrastructures located within a State's territory might constitute a violation of sovereignty if the cyber operation causes physical damage, injury, or loss of functionality in a manner that requires the replacement of physical components of the infrastructure or hampers the functionality of the equipment or other physical components on which the targeted

[246] Heintschel von Heinegg, "Territorial Sovereignty and Neutrality," 128.

[247] Council of the European Union, *International Law in Cyberspace*, 4.

[248] Schmitt, *Tallinn Manual,* 12.

[249] Michael N. Schmitt and Sean Watts, "Beyond State-Centrism: International Law and Non-State Actors in Cyberspace," *Journal of Conflict and Security Law* 21, no 3 (2016): 597, https://doi.org/10.1093/jcsl/krw019.

[250] Schmitt, *Tallinn Manual,* 13.

[251] Schmitt, *Tallinn Manual,* 14.

infrastructure relies for its operation.[252] Although there is some level of understanding regarding physical damage, injury, or loss of functionality, no consensus exists on whether cyber operations not causing such effects would constitute a violation of sovereignty.[253] This rule also applies to infrastructures located on aircrafts, vessels or other platforms subject to State's sovereign immunity.[254]

On the other hand, cyber operations against CIs might cause interference or usurpation of inherently governmental functions given that CIs are vital for the healthy functioning of the State, economy and population. In such situations, the cyber operation in question constitutes a violation of sovereignty regardless of physical damage, injury or loss of functionality. For instance, a cyber operation that alters or removes necessary data to conduct elections would constitute a violation of sovereignty, as it interferes with an inherently governmental function that a State is entitled to exercise exclusively. In addition, while cyber operations against a State's infrastructures might interfere with the victim State's exercise of its independent State powers, they have also have a territorial dimension, as such operations occur within the territory of the victim State.[255]

The last point worth mentioning on cyber violation of sovereignty is that sovereignty can only be violated by States or non-State actors whose actions can be attributed to a State. Non-State actors alone cannot violate sovereignty.[256] As long as their actions cannot be attributed to a State, non-State actors that commit violations of sovereignty are subject to the domestic law of the victim State.[257]

---

[252] Schmitt, *Tallinn Manual,* 20-21.

[253] Schmitt, *Tallinn Manual,* 21.

[254] Heintschel von Heinegg, "Territorial Sovereignty and Neutrality," 129.

[255] Moynihan, *Sovereignty and Non-Intervention,* 19.

[256] Schmitt, *Tallinn Manual,* 17.

[257] Schmitt, *Tallinn Manual,* 17.

3.3. Non-Intervention

Another rule that malicious cyber operations against CIs can violate is non-intervention. Non-intervention is a fundamental customary rule of international law, derived from the notion of sovereignty.[258] It enables States to exercise their exclusive sovereign rights without interference from others, while also reinforcing sovereign equality among them. In other words, non-intervention

> protects the liberty of action that States have within international law, and not regardless of it, and prohibits a State from coercing another into doing something it does not have an obligation to do, or into not doing something it has the right to do.[259]

In its *Nicaragua* judgment, the ICJ stated that "[t]he principle of non-intervention involves the right of every sovereign State to conduct its affairs without outside interference … the Court considers that it is part and parcel of customary international law."[260] Non-intervention is also affirmed by several UN General Assembly resolutions including 1970 UNGA Friendly Relations Declaration:

> No State may use or encourage the use of economic, political or any other type of measures to coerce another State in order to obtain from it the subordination of the exercise of its sovereign rights.[261]

The non-intervention is also included in several international treaties, such as the Montevideo Convention and the Helsinki Final Act,[262] African Union's Constitutive

---

[258] ICJ, *Nicaragua,* para. 202.

[259] Marco Roscini, *International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles* (Oxford University Press, 2024), 162.

[260] ICJ, *Nicaragua*, para. 202.

[261] United Nations General Assembly, *Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Aaccordance with the Charter of the United Nations (A/RES/2625)* (United Nations General Assembly, 1970). https://digitallibrary.un.org/record/202170?v=pdf

[262] Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention," *Baltic Yearbook of International Law* 14, no. 1 (2015): 141, https://doi.org/10.1163/22115897-90000125.

Act, and Charter of the Shanghai Cooperation Organisation.[263] Given the fact that non-intervention is a corollary of the principle of sovereignty, only States are eligible to benefit from it. As stated by the European Court of Justice:

> customary international law principle, also called the principle of non-intervention, concerns the right of any sovereign State to conduct its affairs without external interference and constitutes a corollary of the principle of sovereign equality of States.[264]

As with the sovereignty, non-intervention operates exclusively with respect to States.[265] It does not apply to private actors, provided their actions are not attributable to a State. On the other hand, the main difference between sovereignty and non-intervention is the requirement of the coercive element.[266]

Although non-intervention is firmly established in international law, its content and application remain controversial because of its complicated interaction with other rules of international law and divergent State practice, particularly regarding whether economic coercion constitutes prohibited intervention.[267] Emphasizing that States have "an inalienable right to choose its political, economic, social and cultural systems, without interference in any form by another State,"[268] the UNGA 1970 Friendly Relations Declaration underlines that "armed intervention and all other forms of interference or attempted threats against the personality of the State or against its political, economic, and cultural elements, are in violation of international law."[269]

---

[263] Roscini, *Principle of Non-Intervention,* 107-108.

[264] *Liberation Tigers of Tamil Eelam (LTTE) v. Council of the European Union,* Case T-208/11, Judgment of 16 October 2014, EU: T:2014:885, para 69.

[265] Watts, "Low-Intensity Cyber Operations," 142.

[266] Moynihan, "Role of International Law," 403.

[267] Philip Kunig, "Intervention, Prohibition Of," in *The Max Planck Encyclopedia of Public International Law*, ed. Rüdiger Wolfrum, 1st ed., vol. 6 (Oxford University Press, 2012), 289-293.

[268] UNGA, "Friendly Relations Declaration," Principle 3.

[269] UNGA, "Friendly Relations Declaration," Principle 3.

On the other hand, the ICJ elaborated on the non-intervention in detail in its Nicaragua judgment. The Court noted that

> [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. … Intervention is wrongful when it uses methods of coercion in regard to such choices, which must remain free ones.[270]

Consequently, a prohibited intervention has two components: First, the intervention must relate to a subject that the victim State is entitled to decide freely, specifically within its *domaine réservé.* Second, the intervention must contain an element of coercion. These elements will be discussed below.

3.3.1. Concept of *Domaine Réservé*

The concept of *domaine réservé,* which enjoys protection from outside interference, describes a State's internal affairs within its domestic jurisdiction, and includes matters "not, in principle, regulated by international law."[271] Thus, *domaine réservé* consists of issues that international law does not regulate or leaves solely to the prerogative of States.[272]

The exact scope of *domaine réservé* is indistinct,[273] has always been fluid, and will likely remain so in the future.[274] This is because an issue that was once regarded as part of *domaine réservé* can be regulated by international law over time. This is expressed by the PCIJ, which observed that "the question whether a certain matter is or is not solely within the jurisdiction of a State is an essentially relative question; it depends on the development of international relations."[275] The reduction of *domaine*

---

[270] ICJ, *Nicaragua*, para. 205.

[271] P.C.I.J., *Nationality Decrees*, 24.

[272] Schmitt, *Tallinn Manual,* 314.

[273] Schmitt, *Tallinn Manual,* 314.

[274] Watts, "Low-Intensity Cyber Operations," 154.

[275] P.C.I.J., *Nationality Decrees*, 24

réservé can occur in various ways, such as growing interdependence among States, the development and enforcement of international law, and increasing international integration.[276]

Today, there are very few areas that remain entirely outside of the scope of international law, and the lines between domestic and international spheres are increasingly blurred.[277] Nevertheless, examples of what is included in the *domaine réservé* can be given. For instance, according to the ICJ, "choice of a political, economic, social and cultural system, and the formulation of foreign policy" are included in the State's *domaine réservé*.[278]

To be a prohibited intervention, the act must be designed to undermine State authority in the *domaine réservé*.[279]

3.3.2. Element of Coercion

The second element of prohibited intervention is coercion, which is not explicitly defined in international law. Based on the Declaration of Friendly Relations and the *Nicaragua* judgment, coercion can be described as

> an act by one State that seeks to deprive the target State of its free will over its sovereign functions, in order to compel an outcome or conduct with respect to the target State's exercise of its sovereign functions.[280]

Coercion manifests itself in two forms: it can aim to compel another State to do or not to do something, or it can aim to hijack a specific matter and impose conditions.[281]

---

[276] Kaatja S. Ziegler, "Domaine Réservé," in *The Max Planck Encyclopedia of Public International Law*, ed. Rüdiger Wolfrum, 1st ed., vol. 3 (Oxford University Press, 2012), 209.

[277] Ziegler, "Domaine Réservé," 207.

[278] ICJ, *Nicaragua*, para. 202.

[279] Schmitt, *Tallinn Manual,* 315.

[280] Moynihan, "Role of International Law," 403.

[281] Roscini, *Principle of Non-Intervention,* 152.

Thus, coercion goes beyond mere pressure or persuasion, as it entails the subjugation of a State's will matters within its *domaine réservé*. Coercive acts can be either direct or indirect; as noted by the ICJ, "the principle forbids all States or groups of States to intervene directly or indirectly in the internal or external affairs of other States."[282] The range of acts that can constitute prohibited intervention is diverse and can take different forms, including armed, political, and economic coercion; they may involve physical force or may fall short of constituting the use of force.[283] The ICJ held that the element of coercion is evident in cases of armed coercion, including the use of force and support of armed insurgents, as it observed that

> the element of coercion . . . is particularly obvious in the case of an intervention which uses force . . . in the direct form of military action or in the indirect form of support for subversive or terrorist armed activities within another State.[284]

The Court held that a violation of the principle of non-intervention would also constitute a violation of the prohibition on the use of force "if they directly or indirectly involve the use of force,"[285] and "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."[286]

While the prohibition of the use of force will be discussed in detail below, regarding support to armed groups, it should be noted that only supporting armed groups with the aim of overthrowing a government constitutes a prohibited form of intervention.[287] This support includes training, the supply of weapons, financial support, intelligence, and logistical support.[288]

---

[282] ICJ, *Nicaragua,* para. 205.

[283] Kunig, "Intervention, Prohibition Of," 293.

[284] ICJ, *Nicaragua,* para. 205.

[285] *Case Concerning Armed Activities on the Territory of the Congo (Democratic Republic of the Congo* v. *Uganda),* Judgment, 2005 I.C.J. Rep. 168, para. 164

[286] ICJ, *Nicaragua*, para. 241.

[287] Roscini, *Principle of Non-Intervention,* 187.

[288] ICJ, *Nicaragua*, para. 242.

Although it is clear that armed coercion falls under the prohibitive scope of the principle of non-intervention, given that it is explicitly included in the Friendly Relations Declarations and confirmed by the ICJ, the issue is controversial with regard to other forms of coercion such as economic and political coercion.

During the Cold War, Western countries supported the narrow interpretation of the principle of non-intervention, which excludes political and economic forms, while the socialist bloc and third world countries supported a broad interpretation that included political and economic forms of coercion.[289]

To constitute a prohibited intervention, these economic measures must be taken to coerce another State to do or not do something in a matter within its *domaine réservé*. While many States expressed condemnation of economic measures, many States continue to employ such measures as tools of foreign policy.[290]

The ICJ also observed that "a State is not bound to continue particular trade relations longer than it sees fit to do so, in the absence of a treaty commitment or other specific legal obligation"[291] and judged that the US economic cut-off and subsequent trade embargo against Nicaragua did not violate the principle of non-intervention.[292]

Nevertheless, UNGA's designation of US sanctions against Cuba as a violation of international law since 1992, with the overwhelming majority and other resolutions criticizing unilateral coercive economic measures, demonstrates that economic measures may amount to economic coercion.[293]

---

[289] Roscini, *Principle of Non-Intervention,* 171.

[290] Vaughan Lowe and Antonios Tzanakopoulos, "Economic Warfare," in *The Max Planck Encyclopedia of Public International Law*, ed. Rüdiger Wolfrum, 1st ed., vol. 3 (Oxford University Press, 2012), 338.

[291] ICJ, *Nicaragua*, para. 276.

[292] ICJ, *Nicaragua*, para. 244-245.

[293] Harold Bertot Triana, "A Customary Rule against Unilateral Economic Sanctions of the Nature of the Helms-Burton Act? Regarding Another (Potential) Vote in the United Nations General Assembly against the 'Bloqueo,'" *EJIL: Talk!*, 21 October 2024, https://www.ejiltalk.org/a-customary-rule-against-unilateral-economic-sanctions-of-the-nature-of-the-helms-burton-act-regarding-another-potential-vote-in-the-united-nations-general-assembly-against-the-bloqueo/.

Political coercion can occur through diplomatic threats, premature recognition of belligerency or government,[294] as well as the disruption of electoral processes.[295] It might also involve disinformation,[296] and support for peaceful opposition groups,[297] although this aspect of remains debated. While these actions are not illegal, they may constitute coercion if the criteria are met.

In short, while UNGA Resolutions 2131, 2625, and the Helsinki Final Act contain articles that support a broad interpretation of coercion, State practice and *opinio juris* remain controversial.[298] Nevertheless, they indicate that the possibility of economic and political coercion is not ruled out, and political and economic acts may constitute coercion if the threshold is met.

However, this threshold remains disputed, and no clear line can be drawn. The important aspect is whether the act in question involves a degree of coercion sufficient to amount to intervention.[299] It should also be noted that the motives and intentions of the coercing State carry little importance. The ICJ, in both its *Nicaragua* and *Armed Activities* judgments, did not review the motives of the intervening States. While the Court held that "the obligations arising under the principles of non-use of force and non-intervention were violated by Uganda even if the objectives of Uganda were not to overthrow President Kabila"[300] in the *Armed Activities* judgment, it did not consider that it is "necessary to seek to establish whether the intention of the United States … the United States intended … to coerce the Government of Nicaragua in respect of matters in which each State is permitted."[301] What matters is the coercive act by a

[294] Roscini, *Principle of Non-Intervention,* 184.

[295] Moynihan, *Sovereignty and Non-Intervention,* 40.

[296] Kunig, "Intervention, Prohibition Of," 293.

[297] Roscini, *Principle of Non-Intervention,* 186.

[298] Roscini, *Principle of Non-Intervention,* 174.

[299] Watts, "Low-Intensity Cyber Operations," 149.

[300] ICJ, *Armed Activities*, para. 163.

[301] ICJ, *Nicaragua*, para. 241.

perpetrating State that seeks to deprive a victim State of its free will to gain benefits regardless of coercive act achieved the intended outcome.[302]

3.3.3. Non-Intervention in Cyberspace

Non-intervention applies to cyberspace, as it is a rule of customary international law. This fact is affirmed in the UN GGE processes: "In their use of ICTs, States must observe, among other principles of international law, State sovereignty ... and non-intervention in the internal affairs of other States."[303] The applicability of non-intervention in cyberspace has found widespread support among States, and this issue is not disputed in the cyber age.[304] For instance, the United Kingdom states that "the rule on non-intervention provides a clearly established basis in international law for assessing the legality of State conduct in cyberspace during peacetime."[305] China observes that "[n]o State shall intervene in other States' rights to survival, security and development in cyberspace."[306] Non-intervention's formulation in the language of the UNGA Resolutions 2131 and 2625 and the Helsinki Final Act also enables the principle to be applied in cyberspace by evolutionary interpretation.[307]

On the other hand, Rule 66 of the Tallinn Manual states that "[a] State may not intervene, including by cyber means, in the internal or external affairs of another State."[308] The concept of *domaine réserv*é operates in cyberspace analogously to the

[302] Watts, "Low-Intensity Cyber Operations," 159.

[303] UN GGE, *2015 Report*, 12.

[304] Thibault Moulin, "Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward," *Journal of Conflict and Security Law* 25, no.3 (2020): 427-428, https://doi.org/10.1093/jcsl/kraa011.

[305] Braverman, "International Law in Future Frontiers."

[306] Ministry of Foreign Affairs of People's Republic of China, *China's Views on the Application of the Principle of Sovereignty in Cyberspace* (Ministry of Foreign Affairs of People's Republic of China, 2021), 2, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

[307] Roscini, *Principle of Non-Intervention,* 378.

[308] Schmitt, *Tallinn Manual,* 312.

physical world; it encompasses all matters that States are entitled to freely decide upon that are not regulated by international law.[309]

In the cyber context, the concept of *domaine réserv*é is sometimes equated with "inherently governmental functions," as seen in the national positions of Canada,[310] New Zealand,[311] and Finland.[312] Although both concepts overlap to some degree, they are not identical, given that the concept of *domaine réserv*é is broader than that of inherently governmental functions.[313]

Regarding the concept of coercion, a coercive act should aim to influence the conduct of a State in an area within its *domaine réserv*é, and it should be distinguished from criticism, public diplomacy, propaganda, or mere persuasion.[314] Therefore, coercive cyber operations that aim to compel another State to act or refrain from acting on a matter within its *domaine réservé* for the purpose of gaining a benefit will violate the principle of non-intervention.[315] It is irrelevant whether the cyber operation achieved its intended goal.

As regards which cyber operations can violate non-intervention when they contain necessary elements, *domaine réservé* and coercion, these operations vary. Cyber operations that cause or are designed to cause material damage or injury to persons or physical objects would constitute a violation of non-intervention, even though such

[309] Roscini, *Principle of Non-Intervention,* 381.

[310] Government of Canada, *International Law Applicable in Cyberspace* (Government of Canada, 2022), para. 22, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a4

[311] Ministry of Foreign Affairs and Trade of New Zealand, *Application of International Law in Cyberspace*, para. 9.

[312] Ministry of Foreign Affairs of Finland, *International Law and Cyberspace*, 3.

[313] Schmitt, "Autonomous Cyber Capabilities," 560.

[314] Schmitt, *Tallinn Manual,* 318.

[315] Moynihan, *Sovereignty and Non-Intervention,* 31.

operations fall below the threshold of prohibition of the use of force, which is supported by different national positions.[316] For instance, Germany states that

> [m]alicious cyber activities will only in some cases amount to direct or indirect use of force. However, measures below this threshold may also qualify as coercive. Generally, Germany is of the opinion that cyber measures may constitute a prohibited intervention under international law if they are comparable in scale and effect to coercion in non-cyber contexts.[317]

Although it remains debated whether cyber operations that cause or are designed to cause loss of functionality of infrastructure constitute a violation of the prohibition of the use of force, there is a consensus that such operations may breach non-intervention.[318] Apart from these, other cyber operations include altering election results, disrupting government operations, doxing operations, disinformation campaigns, and propaganda campaigns.[319] In addition, cyber operations conducted to support subversive, terrorist or armed opposition groups might breach the principle of non-intervention as expressed by China "[n]o State shall support or allow separatist forces to undermine other States' territorial integrity, national security and social stability through use of ICTs."[320]

Cyberspace provides new opportunities for States to intervene in other States' internal and external activities. These new opportunities brought by cyberspace seriously challenge two elements of the non-intervention.[321] The increasing role of non-State actors in cyberspace blurs the line between State and non-State, thus increasing the ambiguity about what is included in *domaine réserv*é. The concept's failure to include

---

[316] Roscini, *Principle of Non-Intervention,* 386.

[317] Federal Government of Germany, *Application of International Law in Cyberspace*, 5.

[318] Roscini, *Principle of Non-Intervention,* 387-388.

[319] William Ossoff, "Hacking the Domaine Réservé ′: The Rule of Non-Intervention and Political Interference in Cyberspace," *Harvard International Law Journal* 62, no. 1 (2021): 317.

[320] Ministry of Foreign Affairs of People's Republic of China, *Principle of Sovereignty in Cyberspace*, 2.

[321] Ido Kilovaty, "The International Law of Cyber Intervention," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar Publishing, 2021), 98.

cyber operations that only target private actors creates a favorable opportunity for State interference.[322] This is demonstrated by Russian interference in the 2016 US elections, in which Russian intelligence hacked emails from the Democratic National Committee and Hillary Clinton's campaign and later leaked these emails on the internet.[323] Cyberspace, with its developing capabilities, also enables States to interfere with other States without attacking any *domaine réservé* targets, most notable example being deepfake technology which can be used in disinformation campaigns during election processes.[324]

Secondly, States can interfere with important issues using cyber techniques that do not involve coercion. It is also argued that the classical understanding of coercion sets the threshold so high that most cyber operations would not qualify as coercion.[325] Different approaches to adapting the coercive element to the reality of cyberspace are proposed, namely expanding the notion of coercion, which seeks to broaden the acts that would be included within the definition of coercion; adopting a human rights law-based approach, which would extend the principle's protective scope not only to governments but also to peoples based on the right to self-determination; and lastly, utilizing McDougal and Feliciano's consequentiality approach, which emphasizes effects over tools and methods, arguing that elements such as the importance and number of affected values, the extent of the impact, and the number of people whose values are affected should be considered.[326]

3.3.4. Non-Intervention and Critical Infrastructures

After discussing non-intervention in international law and its implications for cyberspace, we can analyze how this rule can be applied to the protection of critical

[322] Moulin, "Principle of Non-Intervention," 432.

[323] German Marshall Fund of the United States, "Fact Sheet: What We Know about Russia's Interference Operations, accessed 07 May 2025, https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations.

[324] Kilovaty, "Cyber Intervention," 104.

[325] Moulin, "Principle of Non-Intervention," 441.

[326] Kilovaty, "Cyber Intervention," 105-107.

infrastructures. In this regard, it can be said that a State might violate the non-intervention directly or indirectly by conducting cyber operations against another State's critical infrastructure if the State perpetrating the attacks does so to coerce the victim State by depriving it of its free will regarding a subject within its *domaine réservé*.

Non-intervention operates exclusively between States, just as sovereignty; therefore, it can only be violated by States or non-State actors whose actions can be attributed to a State under international law. This conclusion is supported by the numerous national positions of States regarding international law in cyberspace, including Estonia's view on the issue, which states that

> cyber operations that aim to force another nation to act in an involuntary manner or to refrain from acting in a certain manner and target the other nation's *domaine réservé*. (e.g. national democratic processes such as elections, or military, security or critical infrastructure systems) could constitute such an intervention.[327]

Such cyber operations against a CI may constitute an international wrongful act that triggers State responsibility under international law by violating the non-intervention principle.

More examples can also be found in various national positions: For instance, the UK expresses that "[c]overt cyber operations by a foreign State which coercively restrict or prevent the provision of essential medical services or essential energy supplies would breach the rule on non-intervention."[328] Japan observes that "[a]n act of causing physical damage or loss of functionality by means of cyber operations against critical infrastructure, including medical institutions, may constitute an unlawful intervention."[329] New Zealand exemplifies that "cyber activity deliberately causing

[327] UNGA, *Official Compendium*, 25.

[328] Braverman, "International Law in Future Frontiers."

[329] Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations* (Ministry of Foreign Affairs of Japan 2021), 3, https://www.mofa.go.jp/files/100200935.pdf

significant damage to, or loss of functionality in, a State's critical infrastructure, including – for example – its healthcare system, financial system, or its electricity or telecommunications network"[330] would violate non-intervention. Australia states that cyber operations conducted to "manipulate the electoral system to alter the results of an election in another State, intervention in the fundamental operation of Parliament, or in the stability of States' financial systems"[331] may breach non-intervention. The argument that a cyber operation against electoral infrastructures would breach the non-intervention finds support in the national positions of various countries, such as Brazil,[332] Canada,[333] and Israel.[334]

Other examples of cyber operations that may constitute a violation of non-intervention include "any action in cyberspace that would prevent the filing of tax returns online"[335] or "cyber activities directed at interfering with the operation of the systems of public agencies or institutions in another State."[336]

It can be said from these different national positions and UN GGE processes that, although the necessary threshold for coercion remains controversial and further State practice and *opinio juris* are needed in this regard, there is a consensus among States that cyber operations targeting CIs may breach non-intervention, given that they contain necessary elements. In the view of this study, cyber operations targeting

[330] Ministry of Foreign Affairs and Trade of New Zealand, *Application of International Law in Cyberspace*, para. 10.

[331] UNGA, *Official Compendium*, 5.

[332] UNGA, *Official Compendium*, 19.

[333] Government of Canada, *International Law Applicable in Cyberspace*, para. 24.

[334] Roy Schöndorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," *International Law Studies* 97, no. 1 (2021): 403, https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2957&context=ils

[335] Ministry of Foreign Affairs of Republic of Poland, *The Republic of Poland's Position on the Application of International Law in Cyberspace* (Ministry of Foreign Affairs of Republic of Poland, 2022), 4, https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace

[336] Ministry of Foreign Affairs of Colombia, *Colombia's National Position on the Application of International Law in Cyberspace* (Ministry of Foreign Affairs of Colombia, 2025), 9 https://static.wikitide.net/cyberlawwiki/0/0a/Colombia_-_NP_Cyber_PDF_Ingles.pdf

essential services such as healthcare, financial systems, or energy grids can be considered inherently coercive when they deprive a State of its freewill on the subjects within its *domaine réservé*. In addition, the analysis demonstrates that non-intervention serves as a complementary to sovereignty, protecting State functions even when physical destruction is absent. While a global consensus on the threshold for element of coercion is still emerging, this study further argues that an increasing number of national positions view the targeting of CIs to influence a State's sovereign choices is a prohibited form of intervention. In cyberspace, compromising a State's essential functions must be recognized as being just as coercive as traditional military or economic pressure.

Finally, it should be noted that whether a cyber act targeting CIs violates the principle of non-intervention depends on the circumstances; therefore, a case-by-case analysis is needed.

3.4. Due Diligence

Due diligence can be described as "a duty or standard of care that should be applied to a State's actions on its territory or activities subject to its jurisdiction or control, which harm the rights and interests of other States."[337] It is a standard of conduct that States should follow while performing certain acts or fulfilling their obligations.[338]

Due diligence emanates from sovereignty,[339] and acknowledged in various bodies of international law, such as international humanitarian law, international human rights law, international environmental law, and the law of the sea.[340] It lies between the primary rules of conduct and the secondary rules of State responsibility. While it is

[337] International Law Commission, *Report of the International Law Commission Seventy-Fifth Session (29 April-31 May and 1 July-2 August 2024)* (United Nations General Assembly, 2024), 147. https://legal.un.org/ilc/reports/2024/

[338] Delerue, *Cyber Operations,* 355.

[339] *Island of Palmas,* 839.

[340] Antonio Coco and Talita De Souza Dias, "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law," *European Journal of International Law* 32, no 3 (2021): 776, https://doi.org/10.1093/ejil/chab056.

one of the elements of State responsibility, its content is also defined by the different sets of international primary legal rules.[341]

Historically, due diligence has been triggered with regard to private actors whose actions cannot be attributed to a State, where the State's legal responsibility arises from its exclusive power.[342] In this regard, due diligence involves a three-way relationship among the duty bearer (State), the source of harm (State, non-State actor, or natural event), and the beneficiary (other States).[343]

The ICJ referred to due diligence in different cases. For instance, in its *Corfu Channel* judgment, the ICJ stated that "it is every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[344] Accordingly, States have an obligation to prevent acts within their territory that are contrary to the rights of other States. States are only bound to take measures within their power or reasonably available[345] when the State has the knowledge or objectively should have been aware of the malicious act.[346] If this is not possible, States have an obligation to warn other States about the known or foreseeable harms.[347]

Generally, due diligence entails a State's duty to implement all necessary actions to prevent or reduce the risk of substantial transboundary harm, foster international cooperation on due diligence measures, enforce necessary due diligence standards using diverse tools, and inspect, control and authorize the activities that pose potential

[341] Timo Koivurorova, "Due Diligence," in *The Max Planck Encyclopedia of Public International Law*, ed. Rüdiger Wolfrum, 1st ed., vol. 3 (Oxford University Press, 2012), 236.

[342] Koivurova, "Due Diligence," 236.

[343] Coco and Dias, "Cyber Due Diligence," 777.

[344] *The Corfu Chanel Case (United Kingdom v. Albania),* Judgment, 1949 ICJ Rep. 4, para. 22.

[345] Irène Couzigou, "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations," *International Review of Law, Computers & Technology* 32, no. 1 (2018): 47, https://doi.org/10.1080/13600869.2018.1417763.

[346] Couzigou, "Securing Cyber Space," 42.

[347] Scott Shackelford, Scott Russell, and Andreas Kuehn, "Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors," *Chicago Journal of International Law* 17, no 1 (2015): 9, https://doi.org/10.2139/ssrn.2652446.

risks of significant transboundary damage in advance.[348] The due diligence principle also applies to any other area where the State has exclusive control.[349]

The legal status of due diligence is a matter of controversy. Different views exist, with some seeing due diligence as a principle of general international law, a principle of customary international law, or a standard/concept of law.[350] Although due diligence emerged as a rule of customary law in the context of environmental law, as expressed by the International Law Commission (ILC), States have a duty to "take all appropriate measures to prevent significant transboundary harm or at any event to minimize the risk thereof,"[351] and as observed by the ICJ, States are obliged to "ensure that activities within their jurisdiction and control respect the environment of other States."[352]

Apart from environmental law, whether due diligence imposes a general obligation on States is controversial. The ICJ, in its various judgments, first identifies a particular international obligation of the State and then applies due diligence as a standard that a State must undertake to comply with the specific rule.[353] For instance, in its *Bosnian Genocide* judgment, the Court observed that

> the Genocide Convention is not the only international instrument providing for an obligation on the States parties to it to take certain steps to prevent the acts it seeks to prohibit. Many other instruments include a similar obligation … The content of the duty to prevent varies from one instrument to another, according to the wording of the relevant provisions, and depending on the nature of the acts to be prevented. The decision of the Court does not, in this case, purport to establish a general jurisprudence applicable to all cases where a treaty

[348] Joanna Kulesza, *Due Diligence in International Law* (Brill Nijhoff, 2016), 270.

[349] Couzigou, "Securing Cyber Space," 41.

[350] Koivurova, "Due Diligence," 237.

[351] International Law Commission, *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities with Commentaries* (United Nations General Assembly, 2001), Commentary of Article 3 para. 3.

[352] *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion, 1996 ICJ Rep. 226, para. 242.

[353] Jack Kenny, "Cyber Operations and The Status of Due Diligence Obligations In International Law," *International and Comparative Law Quarterly* 73, no. 1 (2024):141, https://doi.org/10.1017/S0020589323000489.

> instrument, or other binding legal norm, includes an obligation for States to prevent certain acts.[354]

As can be seen, the ICJ regards due diligence not as a stand-alone obligation but as an ancillary obligation attached to a primary international obligation.[355] It should also be noted that States did not refer to the principle as a stand-alone obligation in different cases before the ICJ; they referred to it in relation to specific primary obligations arising from treaty or customary law.[356]

The exact boundaries of due diligence are hard to identify, as observed by the International Tribunal for the Law of the Sea (ITLOS)

> due diligence is a variable concept may change over time as measures considered sufficiently diligent at a certain moment may become not diligent enough in light, for instance, of new scientific or technological knowledge. It may also change in relation to the risks involved in the activity.[357]

Thus, whether a State successfully undertook its due diligence obligation is contextual; therefore, a case-by-case evaluation is needed. Although the evaluation should be done case-by-case, some evaluation criteria have emerged to determine whether a State undertook due diligence.[358] These criteria include the effectiveness of State control over its territory, the balancing of interests that the State needed to safeguard, predictability of damage, and an assessment of the State's initiatives to gather vital information regarding the risks.[359]

On the other hand, the ICJ embraced a more moderate standard of proof for due diligence. In the *Corfu Channel* case, the Court observed that "[t]he proof may be

---

[354] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro),* Judgment, 2007 ICJ Rep. 43, para. 429.

[355] Kenny, "Status of Due Diligence," 146.

[356] Kenny, "Status of Due Diligence," 145.

[357] *Responsibilities and Obligations of States with Respect to Activities in The Area*, Advisory Opinion, ITLOS Reports 2011, p. 10, para. 117.

[358] Koivurova, "Due Diligence," 237.

[359] Kulezsa, *Due Diligence*, 264.

drawn from interferences of fact, provided that they leave no room for reasonable doubt."[360] The State engages its responsibility where it is proven that it failed to take measures that were reasonably available, and that such action might have prevented serious harm.[361]

3.4.1. Due Diligence in Cyberspace

In the cyber context, due diligence was referred to in the UN GGE's 2013, 2015 and 2021 reports, urging that "States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs."[362] Although the applicability of due diligence in cyberspace is acknowledged by States in UN GGE processes, controversies exist regarding whether this principle constitutes a general obligation on States.

Supporters of both views may be found among States. For instance, Japan observes that "States have a due diligence obligation regarding cyber operations under international law,"[363] while the Netherlands contends that "the principle as an obligation in its own right, the violation of which may constitute an internationally wrongful act."[364]

On the other hand, Israel states that "we have not seen widespread State practice … and … practice grounded in some overarching *opinio juris*, which would be indispensable for a customary rule of due diligence, or something similar to that."[365] Additionally, New Zealand holds the view that "a cyber-specific "due diligence"

[360] ICJ, *Corfu Chanel,* 18.

[361] Couzigou, "Securing Cyber Space," 49.

[362] UN GGE, *2015 Report*, 8.

[363] Ministry of Foreign Affairs of Japan, *Basic Position of the Government of Japan*, 5.

[364] UNGA, *Official Compendium*, 59.

[365] Schöndorf, "Israel's Perspective, 404.

obligation has crystallised in international law."[366] Even though the majority of national positions from States that have expressed their opinions on due diligence in cyberspace favor a general binding due diligence obligation—contrary to ICJ jurisprudence—there are also opposing States, and consensus on the issue has yet to be reached.[367]

However, this controversy regarding the status of due diligence in cyberspace does not absolve States from their protective duties stemming from the primary rules of international law.[368] The different State positions mentioned above do not dispute the existence of due diligence obligations in cyberspace, but rather the extent and manner in which this obligation can be performed by States.[369]

Rule 6 of the Tallinn Manual is also dedicated to due diligence in cyberspace:

> A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its governmental control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States.[370]

The two elements mentioned in the rule are cumulative.[371] Accordingly, when a State knows or should have known that a malicious cyber operation likely to occur would cause serious adverse consequences for the rights of another State and is perpetrated from its territory or cyber infrastructure under its exclusive control, it must prevent the

[366] Ministry of Foreign Affairs and Trade of New Zealand, *Application of International Law in Cyberspace*, para. 17.

[367] Harriet Moynihan, "Unpacking Due Diligence in Cyberspace," *Journal of Cyber Policy* 8, no. 1 (2023): 10, https://doi.org/10.1080/23738871.2023.2250358.

[368] Coco and Dias, "Cyber Due Diligence," 783.

[369] Karine Bannelier, "Due Diligence as a Cardinal Principle in the Fight Against Malicious Cyber Activities," in *Global Cybersecurity and International Law,* ed. Antonoi Segura-Serrano (Routledge, 2024), 49.

[370] Schmitt, *Tallinn Manual,* 30.

[371] Schmitt, *Tallinn Manual,* 34.

act.[372] If the act is ongoing, the State has an obligation to stop it. If a State cannot prevent or stop a malicious cyber act, it must inform other States about the threat. Therefore, due diligence obligation applies when the act is either ongoing or imminent.[373] This rule also applies to transit States only if the transit State has knowledge of the malicious act.[374] Knowledge in this regard does not mean absolute knowledge of the events; instead, it requires a State to possess minimum capacity enabling it State to acquire such knowledge.[375]

This obligation encompasses not only cyber acts that directly violate the rights of third States but also the rights of their nationals, both within and abroad.[376] It should be noted that the State only has this obligation when the cyber act in question is unlawful.[377] States should also be vigilant about significant transboundary harm or the risk thereof.[378] It should also be noted that International Human Rights Law[379] and International Humanitarian Law[380] impose protective obligations that requiring States to exercise due diligence. Contrary to the principles of sovereignty and non-intervention that operate exclusively between States, the application of due diligence also extends to non-State actors.[381]

Given that due diligence requirements are contextual, the due diligence obligations of more technologically advanced States are greater than those of less advanced States, since these advanced nations have superior technical and financial resources, enabling

[372] Schmitt, *Tallinn Manual,* 30.

[373] Coco and Dias, "Cyber Due Diligence," 787.

[374] Schmitt, *Tallinn Manual,* 33.

[375] Coco and Dias, "Cyber Due Diligence," 789.

[376] Coco and Dias, "Cyber Due Diligence," 784.

[377] Schmitt, *Tallinn Manual,* 34.

[378] Coco and Dias, "Cyber Due Diligence," 790.

[379] Coco and Dias, "Cyber Due Diligence," 795.

[380] Coco and Dias, "Cyber Due Diligence," 801.

[381] Schmitt, *Tallinn Manual,* 35.

them to exercise better control over their territorial cyber infrastructure.[382] States can also take different measures in different situations. Measures taken by States should be assessed in light of reasonableness and feasibility.[383]

3.4.2. Due Diligence and Critical Infrastructures

Due diligence can be utilized in CI protection, particularly since the concept also includes non-State actors who regularly engage in cyber operations targeting CIs. Despite technical progress in recent years, attribution, still proves problematic in cyberspace. Due diligence can mitigate attribution related problems, as the victim State can invoke the territorial State's responsibility for failing to fulfill its due diligence obligation, even without attribution.[384] Although this would not require attribution to a State, the necessary technical evidence to show that a cyber act emanates or transits through the territory of the State is essential; the State had, or should have had the knowledge of the incident and reasonable means to stop it.[385] The GGE 2015 Report explicitly refers to this principle:

> States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.[386]

The report also emphasizes that States "should seek to ensure that their territory is not used by non-State actors to commit" international wrongful acts.[387]

Accordingly, if a State fails to take available measures to stop or prevent a cyber act likely to cause serious damage to another State's CI, it will breach its due diligence

[382] Couzigou, "Securing Cyber Space," 47.

[383] Delerue, *Cyber Operations,* 374.

[384] Delerue, *Cyber Operations,* 375.

[385] Bannelier, "Due Diligence," 62.

[386] UN GGE, *2015 Report*, 8.

[387] UN GGE, *2015 Report*, 13.

obligation.[388] Such damage to CIs does not require physical damage to objects or injury to persons, given that disruption of CIs alone would create serious adverse effects for the third State.[389]

Due diligence acts as an important legal stabilizer in cyberspace given that attribution remains problematic. Because directly attributing cyber operations to a State is challenging, the due diligence shifts the focus to territorial State's failure to prevent or respond to harmful activities originating within its jurisdiction. In this regard, States are obliged to prevent that their cyber infrastructure from being utilized to cause significant harm to foreign CIs. Furthermore, Due diligence facilitates greater cooperation and the exchange of information between States, mutual assistance, the prosecution of cyber terrorists or criminals, and the implementation of other cooperative measures aimed at combating cyber operations against CI.[390]

Lastly, due diligence, by virtue of protective obligations arising from international human rights law and international humanitarian law, would also enhance the enjoyment of human rights and compliance with international humanitarian law, which in turn increases CI protection, given that CIs are also essential for the healthy functioning of civilian life.

3.5. Prohibition of Threat/Use of Force

The prohibition of the use of force derives from both treaty law, notably Article 2/4 of the UN Charter:

> All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the Purposes of the United Nations.[391]

---

[388] Tomohiro Mikanagi, "Application of the Due Diligence Principle to Cyber Operations," *International Law Studies* 97, no.1 (2021): 1035.

[389] Schmitt, *Tallinn Manual,* 38.

[390] Kulezsa, *Due Diligence*, 299.

[391] UN Charter, Article 2(4).

and customary international law. The ICJ affirms the prohibition's customary law and *jus cogens* status[392] and has labeled the prohibition as "a cornerstone of the United Nations Charter."[393] Accordingly, States are forbidden to use force or threaten others in their international relations.

In this regard, the prohibition operates exclusively between States or non-State actors whose acts are attributable to a State.[394] The prohibition applies between States regardless of whether they recognize each other or whether a State is a member of the UN.[395] It can also be argued that although the UN Charter does not bind international organizations, those that can conduct military operations, such as NATO, might still be bound by the prohibition, given that the prohibition is part of customary law.[396] Two exceptions to this prohibition exist: exercising the right of self-defense enshrined in Article 51 of UN Charter and authorization by the UN Security Council in accordance with the Chapter VII of the UN Charter.

Although the Charter forbids States from using force, it does not include a definition. The notion of force is broader than "war," and it is accepted that measures short of war that were allowed under the Covenant of the League of Nations are now prohibited under the UN Charter.[397] However, the main controversy surrounding the concept of force is whether it is limited only to military force or also includes other forms of force, such as economic, political, or ideological.[398]

---

[392] ICJ, *Nicaragua*, para. 190.

[393] ICJ, *Armed Activities*, para. 148.

[394] Michael N. Schmitt and Anusha S. Pakkam, "Cyberspace and the Jus Ad Bellum: The State of Play," *International Law Studies* 103, no. 1 (2024): 198.

[395] Simma, *UN Charter Commentary*, 213.

[396] Simma, *UN Charter Commentary*, 213.

[397] Olivier Corten, *The Law Against War: The Prohibition On The Use Of Force In Contemporary International Law*, 2nd ed. (Bloomsbury Publishing, 2021), 51.

[398] Corten, *The Law Against War*, 50.

During the Cold War, Western States supported a narrow interpretation that limits the concept of force to military force, while Socialist States and Third World countries embraced a broader understanding that also includes economic coercion.[399] Today, the narrower interpretation, which limits force to military means, has prevailed. Not only did States rejected the Brazilian proposal to include political, diplomatic, and economic coercion within the scope of the Article 2(4) during the preparatory work of the UN Charter,[400] The Friendly Relations Declaration- which the ICJ expressed in its case law that the Declaration's clauses on the prohibition of the use of force reflect customary international law[401] only dealt with military force.[402] For instance, it is stated in the Declaration that "[t]he territory of a State shall not be the object of military occupation resulting from the use of force in contravention of the provisions of the Charter."[403] On the other hand, the Declaration explicitly referred to economic or political coercion under the principle of non-intervention.[404] Thus, it must be pointed out that the concept of force is limited solely to military force, and not all forms of coercion fall under the prohibition of the use of force. Nevertheless, actions apart from the military force might constitute a violation of the principle of non-intervention, which was discussed above.

Although the prohibition is limited to military force, it should be understood broadly, which would include any kind of military force, regardless of whether the act is conducted against the territorial integrity or political independence of a State.[405] Accordingly, it includes not only direct military force but also indirect military force, which can be described as the involvement "of one State in the use of force by another

---

[399] Christine Gray, "The Use of Force and International Legal Order," in *International Law,* ed. Malcom Evans, 5th ed. (Oxford University Press, 2018), 604.

[400] James A. Green, "The Regulation of Cyber Warfare Under Jus Ad Bellum," in *Cyber Warfare: A Multidisciplinary Analysis*, ed. James A.Green, (Routledge, Taylor & Francis Group, 2016), 101.

[401] ICJ, *Nicaragua*, para. 212.

[402] Simma, *UN Charter Commentary*, 208.

[403] UNGA, *Friendly Relations Declaration,* Principle 1.

[404] UNGA, *Friendly Relations Declaration,* Principle 3.

[405] Schmitt, *Tallinn Manual,* 329.

State … as well as a State's participation in the use of force by unofficial bands organized in a military manner, … against another State."[406] This fact is also expressed in the Friendly Relations Declaration as "[e]very State has the duty to refrain from organizing or encouraging the organization of irregular forces or armed bands, including mercenaries, for incursion into the territory of another State."[407] It is also expressed that

> [e]very State has the duty to refrain from organizing, instigating, assisting or participating in acts of civil strife or terrorist acts in another State or acquiescing in organized activities within its territory directed towards the commission of such acts, when the acts referred to in the present paragraph involve a threat or use of force.[408]

While the ICJ found in its *Nicaragua* judgment that not every assistance to such groups would constitute a violation of the prohibition of the use of force, it also did not set out criteria that would make such assistance a violation.[409]

In addition, the ICJ, in *Nuclear Weapons* opinion, observed that prohibition "do[es] not refer to specific weapons. [It] appl[ies] to any use of force, regardless of the weapons employed."[410] Since no definite or universally agreed criteria show which acts violate the prohibition, the evaluation must be carried out case-by-case.

3.5.1. Prohibition of Threat of Force

Article 2/4 also forbids States from threatening other States with the use of force. The prohibition of the threat of force is closely linked with the prohibition of the use of force, as the ICJ has associated them with each other. The Court observed that

---

[406] Simma, *UN Charter Commentary*, 211.

[407] UNGA, *Friendly Relations Declaration*, Principle 1.

[408] UNGA, *Friendly Relations Declaration*, Principle 1.

[409] Simma, *UN Charter Commentary*, 212.

[410] ICJ, *Nuclear Weapons*, para 39.

> [t]he notions of "threat" and "use" of force under Article 2, paragraph 4, of the Charter stand together in the sense that if the use of force itself in a given case is illegal - for whatever reason - the threat to use such force will likewise be illegal. In short, if it is to be lawful, the declared readiness of a State to use force must be a use of force that is in conformity with the Charter.[411]

In this regard, the prohibition of the threat of force shares similarities with the prohibition on the use of force; specifically, both are components of customary international law and both are subject to the same exceptions: self-defense under Article 51 of the UN Charter and UNSC authorization under Chapter VII of the Charter.[412] It can be said that "the prohibition of the threat of force is symmetrical to that of the use of force."[413]

Although the concept is overlooked in comparison to the actual use of force and no agreed definition exists among scholars,[414] it can nevertheless be defined as "an express or implied promise by a government of a resort to force conditional on non-acceptance of certain demands of that government."[415]

Contrary to arguments that the threat of force has no distinct meaning from the use of force, State practice and international courts consider it a separate concept.[416] For instance, the Friendly Relations Declaration mentions both the threat and use of force simultaneously while commenting on the State's duties regarding prohibition, as it observed "[e]very State has the duty to refrain in its international relations from the threat or use of force … Such a threat or use of force constitutes a violation of

---

[411] ICJ, *Nuclear Weapons*, para 47.

[412] Delerue, *Cyber Operations,* 313.

[413] Anne Lagerwall and François Dubuisson, "The Threat of the Use of Force and Ultimata," in *The Oxford Handbook of the Use of Force in International Law*, ed. Marc Weller (Oxford University Press, 2016), 915.

[414] Triantafyllos Kouloufakos, "Cyber Operations as Threats of Force: A Welcome Addition or Splitting Hair?," in *Global Cybersecurity and International Law*, ed. Antonio Segura-Serrano (Routledge, 2024), 12.

[415] Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press, 1963), 364.

[416] Kouloufakos, "Cyber Operations as Threats," 12.

international law."[417] The prohibition of the threat of force is also included in various treaties, such as the 1982 UN Convention on the Law of the Sea, the 1979 Moon Treaty, the Pact of Bogotá, the NATO Treaty, the Charter of the Organization of Islamic Conference, and the Charter of the Shanghai Cooperation Organization.[418]

On the other hand, the ICJ treated the threat of force distinctly in its *Corfu Chanel*,[419] *Nicaragua*[420] judgments, and *Nuclear Weapons*[421] advisory opinion. Lastly, the *ad hoc* arbitral tribunal constituted to handle the dispute between Guyana and Suriname decided that Suriname violated the prohibition against the threat of force with its conduct.[422]

A threat of force only becomes unlawful if such force is unlawful under Article 2/4.[423] A State must declare its readiness to use force; the method of communication that the State uses to this end does not matter. In this regard, the prohibited threat of force can take various forms and can be expressed directly or implicitly. It can be articulated verbally or in written statements; it may also be included in defensive alliance pacts or bilateral military assistance treaties, or it can be implicitly made by positive acts such as military maneuvers, drills, or positioning army units close to a target State's borders.[424] Various methods, including economic sanctions, propaganda, and manipulation, can also accompany the threat of force.[425] It also does not need to

[417] UNGA, *Friendly Relations Declaration*, Principle 1.

[418] Marco Roscini, "Threats of Armed Force and Contemporary Internatıonal Law," *Netherlands International Law Review* 54, no. 2 (2007): 244, https://doi.org/10.1017/s0165070x0700229x.

[419] ICJ, *Corfu Chanel*, 35.

[420] ICJ, *Nicaragu*a, para 227.

[421] ICJ, *Nuclear Weapons*, para 47.

[422] *Arbitration between Guyana and Suriname (Guyana v. Suriname),* PCA Case No. 2004-04, Award, 17 September 2007, paras. 439-440.

[423] ICJ, *Nuclear Weapons,* para. 47.

[424] Romana Sadurska, "Threats of Force," *American Journal of International Law* 82, no. 2 (1988): 242-243, https://doi.org/10.2307/2203188.

[425] Sadurska, "Threats of Force," 244.

include a specific demand; the communicative nature of the threat is the determinative factor.[426] The key aspect here is that the threat must not be overly vague or general; it should target an identifiable State or a group of States.[427]

The threshold for the prohibited threat of force is not certain, and States have tolerated incidents of threats of force in the past to some degree.[428] It has been witnessed that States tolerated threats of force if they were articulated due to security concerns, vindication of a denied right, prudence, or economy, and that, the consequences of the threat were also taken account.[429] Some States even claim that threats can be positive in international relations in some cases by deterring acts contrary to international law without negative results.[430]

It should be highlighted that the ICJ embraces a strict approach regarding the subject, in which the Court identifies an act as a threat if certain circumstances demonstrate that the act in question constitutes political coercion to gain something from the victim State by indicating a willingness to react.[431] On the other hand, the ICJ rejected the notion that mere possession of nuclear weapons or building nuclear capacity violates Article 2/4 by itself.[432] It also pointed out that there is no restriction on State armament in general international law.[433] Lastly, just as with the use of force, the threat of force should be evaluated on a case-by-case basis, and it can only be violated by States or non-State actors whose acts are attributable to a State.

---

[426] Schmitt, *Tallinn Manual,* 338.

[427] Lagerwall and Dubuisson, "Ultimata," 913.

[428] Crawford, *Brownlie's Principles*, 720.

[429] Sadurska, "Threats of Force," 260-266.

[430] Roscini, "Threats of Armed Force," 250.

[431] Lagerwall and Dubuisson, "Ultimata," 915.

[432] ICJ, *Nuclear Weapons*, paras. 48.

[433] ICJ, *Nicaragua*, para 269.

Finally, the relationship between the principle of non-intervention and the prohibition of threats and the use of force should be emphasized. These principles are closely related, overlapping, and reinforcing each other.[434] The main difference between them is the degree of coercion involved in the act. In cases of a violation of the use of force, the act is typically more severe and damaging in scale and effects than a non-intervention violation.[435] Secondly, while the prohibition of the threat or use of force is limited to military action, the principle of non-intervention has a broader scope that encompasses other methods of coercion, such as economic and political coercion. Accordingly, an act that does not violate the use of force may still constitute a violation of non-intervention.

3.5.2. The Right of Self-Defense

The right of self-defense constitutes one of two exceptions to the prohibition of threat or use of force in international law. The right of self-defense is part both of customary international law and treaty law, which is enshrined in Article 51 of the UN Charter:

> Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken the measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.[436]

Accordingly, States are entitled to respond with force to an armed attack against them, either individually or collectively, within the boundaries of international law as the ICJ has emphasized that

[434] Delerue, *Cyber Operations,* 280.

[435] Watts, "Low-Intensity Cyber Operations," 149.

[436] UN Charter, Article 51.

> Article 51 of the Charter may justify a use of force in self-defence only within the strict confines there laid down. It does not allow the use of force by a State to protect perceived security interests beyond these.[437]

The core of the right to self-defense is self-help; in this regard, it can be said that the right of self-defense is "a permissible form of armed self-help."[438] The fact that self-defense is a right, not a duty, is well established in international law; therefore, a State faced with an armed attack can also choose not to resort to force and instead seek a political solution.[439] It should also be underlined that every State, whether it is a member of the UN or not, is vested with the right of self-defense.[440]

The right of self-defense precludes the wrongfulness of an act "if the act constitutes a lawful measure of self-defense taken in conformity with the Charter of the United Nations."[441] The important point to note here is that although self-defense legitimizes the use of force against an armed attack, States must comply with legal rules while exercising self-defense, particularly the rules of international humanitarian law, as the right of self-defense does not absolve States from their obligations under international law.[442]

While the Charter does not distinguish between individual and collective self-defense, subsequent State practice and jurisprudence treat them differently.[443] Since their conditions differ slightly, these two types of self-defense will be examined separately.

---

[437] ICJ, *Armed Activities*, para. 148.

[438] Yoram Dinstein, *War, Aggression, And Self-Defence*, 5th ed (Cambridge University Press, 2012), 187.

[439] Dinstein, *Self-Defence*, 190.

[440] Christopher Greenwood, "Self-Defence," in *The Max Planck Encyclopedia of Public International Law,* ed. Rüdiger Wolfrum, 1st ed., vol. 9 (Oxford University Press, 2012), 108.

[441] International Law Commission, *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (United Nations, 2001), https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

[442] Greenwood, "Self-Defence,", 105.

[443] Greenwood, "Self-Defence," 105.

3.5.2.1. Individual Self-Defense

As mentioned above, States have the right to individually resort to force against an armed attack within the limits imposed by international law. For a resort to force to constitute lawful self-defense, three conditions must be met. Firstly, the force in question must respond to an armed attack. Secondly, the force must be necessary, proportionate, and immediate.[444] Lastly, the situation must be reported to the Security Council and be terminated when the Council takes appropriate measures to maintain international peace.[445]

3.5.2.1.1. Armed Attack Threshold

According to Article 51, the right of self-defense is granted to a State in cases of armed attacks. In this context, "armed attack" serves as a threshold for the right of self-defense.[446] Although the term "armed attack" is not defined in the UN Charter, the ICJ in the *Nicaragua* judgment distinguished "the most grave forms of the use of force (those constituting an armed attack) from other less grave forms."[447]

In its judgment, the Court observed that a certain gap exists between Articles 2(4) and 51, with the main difference being the "scale and effects" of the force in question.[448] In this regard, by virtue of Article 3(e) of the Definition of Aggression, the Court notes that an armed attack encompasses not only acts of "regular armed forces across an international border" but also includes

> sending by a State of armed bands to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack rather than as a mere frontier incident had it been carried out by regular armed forces.[449]

[444] Dinstein, *Self-Defence*, 230.

[445] Greenwood, "Self-Defence," 108.

[446] Dinstein, *Self-Defence*, 193.

[447] ICJ, *Nicaragua*, para. 191.

[448] ICJ, *Nicaragua*, para. 195

[449] ICJ, *Nicaragua*, para. 195

The Court reiterated this conclusion in the *Oil Platforms* judgment.[450] The same conclusion is also supported by the UNGA's Definition of Aggression and its preparatory work.[451]

Accordingly, for a use of force to constitute an armed attack that triggers the right of self-defense, it should possess a certain gravity. While this is the case, there is no need to set the bar too high, as small-scale attacks may also qualify as armed attacks if they cause or could possibly cause human casualties or material damage to objects.[452]

On the other hand, attacks that cannot themselves amount to an armed attack may do so when considered cumulatively. This "accumulation of events" theory "deals with situations where consecutive attacks take place that are linked in time, source and cause"[453] and argues that such attacks might constitute an armed attack, even though they do not when taken in isolation.[454] While the theory is not free of controversy, it receives significant support in the legal doctrine.[455] The ICJ also embraced the theory in the *Nicaragua,*[456] *Oil Platforms*,[457] and *Armed Activities*[458] judgments.

As for the targets of armed attacks, there is a wide range of possible targets, which include the territory of a State as well as objects and persons within it, along with the State's external manifestations abroad.[459] While it is clear that external manifestations

---

[450] *Case Concerning Oil Platforms (Islamic Republic of Iran v. USA),* Judgment, 2003 ICJ Rep. 161, para 51.

[451] Tom Ruys, *"Armed Attack" and Article 51 of the UN Charter: Evolutions in Customary Law and Practice* (Cambridge University Press, 2010), 151.

[452] Ruys, *Armed Attack*, 155.

[453] Ruys, *Armed Attack*, 168.

[454] Delerue, *Cyber Operations,* 334.

[455] Ruys, *Armed Attack*, 169.

[456] ICJ, *Nicaragua*, para 231.

[457] ICJ, *Oil Platforms*, para 64.

[458] ICJ, *Armed Activities*, para 147.

[459] Ruys, *Armed Attack*, 152.

of States include State organs such as military units, the situation becomes controversial when considering private merchant vessels and nationals.[460]

With regard to actors, while it is settled that the right of self-defense is triggered in response to armed attacks conducted by State or non-State actors when those actions can be attributed to a State, the question of whether armed attacks by non-State actors whose actions cannot be attributed to a State remains controversial and lacks a definitive answer.[461] The attacker's intent is also important in determining whether an act constitutes an armed attack. The element of intention, "*animus aggressionis*," requires either a general hostile intent or deliberate intention to cause loss of life and material damage to objects.[462] The ICJ in the *Oil Platforms* case examined whether there was a specific intention while evaluating the case.[463] It should also be noted that there were instances when States did not regard a particular use of force as an armed attack due to a lack of hostile intent, such as NATO's killing of four Chinese nationals in Belgrade during the 1999 Operation Allied Force.[464]

Lastly, it should be noted that the burden of proof to demonstrate that an armed attack triggering the right of self-defense exists with the party justifying its use of force under this right, as observed by the ICJ in the *Oil Platforms* case.[465]

3.5.2.1.2. The Elements of Necessity, Proportionality and Immediacy

The second criterion for the use of force under the right of self-defense to be lawful is the presence of the elements of necessity, proportionality, and immediacy. Although these elements are not explicitly referred to in the UN Charter, they are part of

[460] Greenwood, "Self-Defence," 108.

[461] Delerue, *Cyber Operations,* 463-464.

[462] Ruys, *Armed Attack*, 177.

[463] ICJ, *Oil Platforms*, para 64.

[464] Ruys, *Armed Attack*, 165.

[465] ICJ, *Oil Platforms*, para 57,119.

customary international law.[466] In the words of the ICJ, "specific rule whereby self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it, a rule well established in customary international law,"[467] and "[t]his dual condition applies equally to Article 51 of the Charter, whatever the means of force employed."[468] The ICJ affirms this fact in the *Armed Activities*[469] and *Oil Platforms*[470] judgments. These elements apply separately to each incident.[471]

The element of necessity means that a self-defending State has no other option than to respond with force to an armed attack it faces.[472] In this regard, the self-defending State must resort to force as a last option after exhausting all non-forcible measures before triggering self-defense, and the force used under self-defense must be necessary to respond to such an attack.[473] The conduct of the State should be assessed as a whole when evaluating whether the act meets the element of necessity.[474]

On the other hand, the element of proportionality means that the scale and duration of the force employed by the self-defending State correspond to the armed attack that the self-defending State faces.[475] Branded as "the essence of self-defense," the element of proportionality serves as a "standard of reasonableness" for the force employed by the self-defending State.[476] The conduct of a State should be assessed with reference to

---

[466] Dinstein, *Self-Defence*, 230.

[467] ICJ, *Nicaragua*, para 176.

[468] ICJ, *Nuclear Weapons*, para 41.

[469] ICJ, *Armed Activities*, para 147.

[470] ICJ, *Oil Platforms*, para 76.

[471] Delerue, *Cyber Operations,* 478.

[472] Schmitt and Pakkam, "Regulation of Cyber Warfare," 211.

[473] Delerue, *Cyber Operations,* 479.

[474] Greenwood, "Self-Defence," 109.

[475] Crawford, *Brownlie's Principles*, 723.

[476] Dinstein, *Self-Defence*, 232.

the threat of an armed attack.[477] In this regard, the force employed by the self-defending State must be proportionate to the legitimate objective of self-defense.[478] It should also be noted that the force employed does not need to use the same weapons: as long as the necessity and proportionality elements are met, a self-defending State can employ non-kinetic force against a kinetic force and vice versa.[479]

Lastly, the element of immediacy means that an identifiable armed attack against the self-defending State has occurred or is ongoing, or is under preparation and requires "concrete danger of an imminent attack which is objectively verifiable."[480] To meet the immediacy criterion, there should be no excessive time period between the armed attack and self-defense.[481] In the *Nicaragua* Case, the ICJ found that self-defense measures taken months after the armed attacks cannot be labeled as necessary measures.[482] In this regard, it should be emphasized that the element of immediacy does not refer to a right to anticipatory self-defense, a controversial issue that is opposed by most States and the literature.[483] Instead, immediacy means "the period following the execution of an armed attack within which the victim State may reasonably respond in self-defence," and factors like "the temporal proximity between attack and response," "the period necessary to identify the attacker," and "the time required to prepare a response" are significant for this element.[484]

[477] Greenwood, "Self-Defence," 109.

[478] Delerue, *Cyber Operations,* 481.

[479] Schmitt and Pakkam, "Regulation of Cyber Warfare," 211.

[480] Noam Lubell, "The Problem of Imminence in an Uncertain World," in *The Oxford Handbook of the Use of Force in International Law*, ed. Marc Weller (Oxford University Press, 2015), 704.

[481] Dinstein, *Self-Defence*, 233.

[482] ICJ, *Nicaragua*, para 237.

[483] Delerue, *Cyber Operations,* 467.

[484] Schmitt, *Tallinn Manual,* 353.

3.5.2.1.3. Notification of the UN Security Council

The last criterion for lawful self-defense is the notification of the UN Security Council. Accordingly, a self-defending State is obliged to report the measures it took to the Security Council under Article 51. It should be noted that this obligation does not imply prior approval for the right of self-defense from the Council.[485] In this regard, while being a violation of the UN Charter on its own, failure to notify the Security Council about self-defense measures does not automatically render the self-defense unlawful; however, it does erode the perceived legality of these measures within the framework of Article 51.[486] This conclusion is supported by the ICJ in both the *Nicaragua*[487] and *Armed Activities*[488] judgments.

On the other hand, Article 51 also imposes a temporal limitation on the exercise of self-defense by stating that the right of self-defense is valid "until the Security Council has taken the measures necessary to maintain international peace and security."[489] Accordingly, States can use their right of self-defense until the Security Council decides to terminate it by adopting a decision under Chapter VII or until it takes measures necessary to maintain international peace and security, which refers to effective actions that go beyond the simple adoption of a resolution.[490]

3.5.2.2. Collective Self-Defense

Article 51 of the UN Charter also grants States the right of collective self-defense. Collective self-defense is viewed as an innovation and serves as the foundation for many regional treaties, including the NATO Treaty and the Warsaw Pact.[491] In

[485] Dinstein, *Self-Defence*, 235.

[486] Greenwood, "Self-Defence," 109.

[487] ICJ, *Nicaragua*, para 235.

[488] ICJ, *Armed Activities*, para 145.

[489] UN Charter, Article 51.

[490] Greenwood, "Self-Defence," 110.

[491] Gray, "The Use of Force," 618.

addition to alliances, collective self-defense treaties can also take the form of mutual assistance and guarantee treaties.[492] Similar to individual self-defense, its customary law status is recognized by the ICJ.[493]

In its *Nicaragua* judgement, the ICJ stated that there are 2 additional criteria exist for the collective self-defense as it observed that "[w]here collective self-defense is invoked, it is to be expected that the State for whose benefit this right is used will have declared itself to be the victim of an armed attack"[494] and "the requirement of a request by the State which is the victim of the alleged attack is additional to the requirement that such a State should have declared itself to have been attacked."[495] Accordingly, for the right of collective self-defense to be triggered, a State must first face an armed attack and possess the right of self-defense under international law; second, that victim State must declare itself to be the victim of an armed attack; third, the victim State must request assistance for self-defense. The other criteria for the lawfulness of individual self-defense -the elements of necessity, proportionality, immediacy, and the obligation to notify the UN Security Council- also apply to collective self-defense.[496]

3.5.3. Prohibition of Threat/Use of Force in Cyberspace

Application of the prohibition of the threat/ the use of force in cyberspace is affirmed by the UN GGE:

> In their use of ICTs, and as per the Charter of the United Nations, States shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any State or in any other manner inconsistent with the purposes of the United Nations.[497]

[492] Dinstein, *Self-Defence*, 283.

[493] ICJ, *Nicaragua*, para 193.

[494] ICJ, *Nicaragua*, para 195.

[495] ICJ, *Nicaragua*, para 199.

[496] Dinstein, *Self-Defence*, 296.

[497] UN GGE, "2021 Report," 18.

Affirmation of the prohibition of the threat or use of force in GGE processes is also supported by the declared national positions. For instance, the common position of the European Union underlines that "[p]ursuant to Article 2(4) of the UN Charter and customary international law, the threat or use of force … is prohibited."[498] Likewise, the common position of the African Union observes that "[t]he prohibition on the threat or use of force is a rule of *jus cogens* and a fundamental and cardinal rule of general international law … This rule of international law applies in cyberspace."[499] According to the declared national positions so far, the applicability of the prohibition in cyberspace has broad support, and it is not contested by States.[500] Accordingly, the prohibition applies in cyberspace under the conditions that the cyber operation in question is either conducted by a State or a non-State actor whose acts can be attributed to a State; the cyber operation must reach the use of force threshold, and the cyber operation in question must be executed in the conduct of international relations.[501]

Although the applicability of prohibition is affirmed, the question of when to apply the prohibition is subject to debate,[502] and there is no settled State practice.[503] Cyber operations differ from traditional military operations in the sense that they can cause significant effects without physical consequences, complicating the application of the conventional understanding of the prohibition of the use of force in cyberspace.[504] To overcome this issue, three different approaches to assessing whether a cyber operation qualifies as a threat or use of force have been proposed. These approaches are based

[498] Council of the European Union, *International Law in Cyberspace*, 6.

[499] African Union Peace and Security Council, *Common African Position*, 6.

[500] *See* "Common and National Positions," International Cyber Law: Interactive Toolkit,at https://cyberlaw.ccdcoe.org/wiki/List_of_articles.

[501] Marco Roscini, "Cyber Operations as a Use of Force", in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar Publishing, 2021), 299.

[502] Schmitt and Pakkam, "Regulation of Cyber Warfare," 200.

[503] Delerue, *Cyber Operations,* 286.

[504] Anusha Pakkam, "The Evolving Interpretation of the Use of Force in Cyber Operations: Insights from State Practices," Lieber Institute West Point, 25 November 2024, https://lieber.westpoint.edu/evolving-interpretation-use-of-force-cyber-operations-insights-State-practices/.

on the existing international legal framework regarding the prohibition of the use of force.[505]

The first approach is the instrument-based approach, which focuses on the means used to carry out the act in question. Traditionally, it was used to separate armed force from other types of coercion, such as economic and political coercion.[506] Under this approach, a cyber operation might constitute a use of force to the extent that cyber weapon employed resembles traditional weapons.[507] It lost its credibility due to the differences between emerging new technologies and traditional means of warfare.[508]

The second approach is the target-based approach, which asserts that cyber operations targeting national critical infrastructure qualify as a use of force.[509] This approach was developed within the framework of self-defense. Accordingly, the targeting of critical infrastructure allows States to resort to force as a self-help measure.[510] This approach is criticized for being over-inclusive, as it does not consider the effects or nature of the cyber operation.[511]

The third and the most supported approach is the consequence-based approach, which focuses on the results of cyber operations. This approach argues that the primary factor in cyber use of force assessments is its impact, regardless of the technical methods used in its conduct.[512] It is endorsed by "every State that has tackled the question"[513]

---

[505] Delerue, *Cyber Operations,* 290.

[506] Roscini, "Cyber Operations," 300.

[507] Delerue, *Cyber Operations,* 289.

[508] Delerue, *Cyber Operations,* 289.

[509] Roscini, "Cyber Operations," 300.

[510] Delerue, *Cyber Operations,* 288.

[511] Roscini, "Cyber Operations," 300.

[512] Pakkam, "Use of Force in Cyber Operations."

[513] Schmitt and Pakkam, "Regulation of Cyber Warfare," 200.

and advocated by the Tallinn Manual.[514] For instance, Germany states that "with regard to the definition of 'use of force', emphasis needs to be put on the effects rather than on the means used."[515] The United States observes that "cyber activities that proximately result in death, injury, or significant destruction, or represent an imminent threat thereof, would likely be viewed as a use of force / armed attack."[516]

This study maintains that a consequence-based approach offers the most robust and practical method for evaluating the use of force threshold in cyberspace. In contrast to the instrument-based approach, which depends on analogies with traditional kinetic weapons, the consequence-based model focuses on the actual harm inflicted on a State. On the other hand, a target-based approach would be over inclusive as any cyber operation conducted against CIs would qualify as use of force. Focusing on the ultimate impact of a cyber operation rather than means or targets would allow international law to remain adaptable to rapid technological developments and ensures that severe cyber operations targeting CIs are covered under prohibition of use of force.

In a consequence-based approach, determining whether a cyber operation constitutes a prohibited use of force involves comparing it to other kinetic or non-kinetic actions that are classified as such. Thus, if such actions are deemed a use of force, cyber operations with comparable scale and impact would also fall into that category.[517] This analogy can be seen in various national positions. For example, the United States observes that "[i]f the physical consequences of a cyber activity result in the kind of damage that dropping a bomb or firing a missile would, that cyber activity should equally be considered a use of force."[518] In the same manner, Australia observes that

[514] Schmitt, *Tallinn Manual,* 330.

[515] Federal Government of Germany, *Application of International Law in Cyberspace*, 6.

[516] UNGA, *Official Compendium*, 137.

[517] Schmitt, *Tallinn Manual,* 333.

[518] UNGA, *Official Compendium*, 137.

> [i]n determining whether a cyber activity constitutes a use of force, States should consider whether the activity's scale and effects are comparable to traditional kinetic operations that rise to the level of use of force under international law.[519]

On the other hand, the Tallinn Manual states that "[a] cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."[520]

In this regard, two types of impacts caused by cyber operations should be distinguished: the first involves cyber operations that cause physical damage to objects or injury to persons. The second refers to cyber operations that do not cause such effects. While there is less controversy about whether the first kind of cyber operations constitutes a use of force, the situation is less clear for the second type of cyber operations.

3.5.3.1. Cyber Operations That Cause Physical Damage to Objects or Injury/Death to Persons

There is broad agreement that cyber operations that cause physical damage to objects or injury/death to persons do qualify as prohibited use of force.[521] No State has objected to classifying cyber operations generating such consequences as use of force.[522] For example, Denmark expresses that "where a cyber operation results in injury, death, or significant physical damage, this *prima facie* qualifies as use of force."[523] In a similar terms, Italy considers that "a cyber operation conducted by a State against another State as a use of force … resulting in physical damage of

[519] UNGA, *Official Compendium*, 5.

[520] Schmitt, *Tallinn Manual,* 330.

[521] Schmitt and Pakkam, "Regulation of Cyber Warfare," 201.

[522] Pakkam, "Use of Force in Cyber Operations."

[523] Jeppe Mejer Kjelgaard and Ulf Melgaard, "Denmark's Position Paper on the Application of International Law in Cyberspace: Introduction," *Nordic Journal of International Law* 92, no. 3 (2023): 451, https://doi.org/10.1163/15718107-20230001.

property, human injury or loss of life."[524] On the other hand, according to Tallinn Manual, cyber operations that injure or kill persons or physically damage or destroy property amount to the use of force.[525] It further notes that the consequences of such operations are subject to a *de minimis* rule in determining whether they qualify as a use of force.[526]

3.5.3.2. Non-Destructive or Non-Injurious Cyber Operations

Although it is clear that cyber operations causing physical damage to objects or injury or death to persons qualify as a use of force, the situation is less clear for cyber operations that do not produce such consequences. Some argue that it would be inappropriate to classify such cyber operations as a use of force; however, they can produce large-scale consequences even without physical damage.[527] This situation is also reflected in State's positions, as France does not "rule out the possibility that a cyberoperation without physical effects may also be characterised as a use of force. In the absence of physical damage, a cyberoperation may be deemed a use of force."[528]

There is no consensus among States on the necessary threshold for use of force in cyber operations that do not cause physical damage to objects or injury to persons. In this regard, the Tallinn Manual offers an analysis based on the "scale and effects" of cyber operations. This approach offers a more nuanced way to assess the use of force, enabling cyber operations that produce non-physical effects to be classified as such. As expressed in the Manual, "scale and effects is a shorthand term that captures the quantitative and qualitative factors to be analysed in determining whether a cyber

[524] Ministry of Foreign Affairs and International Cooperation of Italian Republic, *Italian Position Paper on International Law and Cyberspace* (Ministry of Foreign Affairs and International Cooperation of Italian Republic, 2021), 8, https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf

[525] Schmitt, *Tallinn Manual,* 333.

[526] Schmitt, *Tallinn Manual,* 334.

[527] Delerue, *Cyber Operations,* 298.

[528] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 3.

operation amounts to a use of force."[529] While developing this framework, the experts who drafted the Manual took note of the ICJ's reasoning in the *Nicaragua* judgment.[530]

To date, no State has opposed the "scale and effects" analysis; on the contrary, some are openly supporting it.[531] For instance, Norway notes that "[w]hether a cyber operation violates the prohibition on the threat or use of force in Article 2(4) of the UN Charter depends on its scale and effects, physical or otherwise."[532] Other supportive States include Canada, Denmark, Estonia, Germany, New Zealand, Italy, Ireland, Romania, and Sweden.[533] Nevertheless, it should be kept in mind that the "scale and effects" analysis is not a determinant legal criterion for cyber use of force assessments.

Acknowledging that cases are not always obvious, for example, when the effects of cyber operations are non-injurious and non-destructive, the Manual introduces several factors that may States consider in identifying use of force. These factors are severity, immediacy, directness, invasiveness, measurability of effects, military character, State involvement, and presumptive legality.[534] It should be noted that these factors are not exhaustive, and States can consider other factors.[535] In this approach, the nature of the consequences is decisive. Only the severity criterion can decisively determine whether the cyber operation in question amounts to a use of force.[536] Apart from clear cases, other factors should be assessed in combination.[537] Moreover, the more immediate,

[529] Schmitt, *Tallinn Manual,* 331.

[530] Schmitt, *Tallinn Manual,* 330.

[531] Schmitt and Pakkam, "Regulation of Cyber Warfare," 203.

[532] UNGA, *Official Compendium*, 69.

[533] *See* International cyber law: interactive toolkit.

[534] Schmitt, *Tallinn Manual,* 334-336.

[535] Schmitt, *Tallinn Manual,* 337.

[536] Michael N. Schmitt, "The Use of Cyber Force and International Law," in *The Oxford Handbook of the Use of Force in International Law*, ed. Marc Weller, (Oxford University Press, 2016), 1114.

[537] Schmitt and Pakkam, "Regulation of Cyber Warfare," 205.

direct, invasive, and measurable a cyber operation's effects are, the more likely States are to classify it as a use of force.[538]

It should also be emphasized that the assessment should be made case by case and that more State practice and *opinio juris* are needed to define the threshold.[539] A number of States have listed criteria for use of force assessments in their national positions. For example, Singapore identified factors such as "the prevailing circumstances at the time of the cyber operation, the origin … the effects caused or sought by… the degree of intrusion of the cyber operation, and the nature of the target."[540] In a similar terms, African Union identified additional factors, including "the duration of the attack, the nature of the targets attacked, the locations of the targets attacked, and the types of weapons used … damage caused by the attack."[541]

3.5.4. Prohibition of Threat of Force in Cyberspace

Just as the prohibition of the use of force exists, the prohibition of the threat of force also applies in cyberspace. As demonstrated above, its applicability is affirmed by the UN GGE and supported by various national positions. Accordingly, the threat of cyber force by State or non-State actors whose actions are attributable to a State against other States is unlawful. This holds true for situations in which the threatened cyber action would amount to an unlawful use of force. This situation is best exemplified by Rule 70 of the Tallinn Manual, which states that "[a] cyber operation, or threatened cyber operation, constitutes an unlawful threat of force when the threatened action, if carried out, would be an unlawful use of force."[542] A cyber operation that may not constitute a use of force nevertheless may constitute a threat of force.[543]

---

[538] Schmitt, "Use of Cyber Force," 1115.

[539] Schmitt and Watts, "Beyond State-Centrism," 608.

[540] UNGA, *Official Compendium*, 83.

[541] African Union Peace and Security Council, *Common African Position*, 7.

[542] Schmitt, *Tallinn Manual,* 338.

[543] Kouloufakos, "Cyber Operations as Threats," 19.

Assessment of the threat of force is contextual and dependent on the circumstances of the event: the threat can be open or implicit, and its credibility and perception by the target State hold utmost importance.[544] In this regard, the threat to resort to cyber force may be open, or it can be executed through demonstrations of cyber force such as denial-of-service (DDoS) attacks.[545] On the other hand, military exercises in cyberspace differ from their traditional counterparts, given that such cyber exercises are not visible or detectable in a manner that can be perceived as a threat of force by other States.[546] It should also be highlighted that the building of cyber capabilities or the mere possession of cyber weapons does not constitute a threat of force.[547]

3.5.5. The Right of Self-Defense in Cyberspace

Unlike the topics discussed so far, the question of whether States have a right to self-defense in cyberspace was not easily affirmed during the discussions in the GGE or OEWG processes. While the 2013 and 2015 GGE Reports made no reference to the right of self-defense, the issue contributed to the collapse of the 2017 GGE process. During the discussions in the 2017 process, the States opposing the inclusion of the right of self-defense in the final report argued that this would pave the way for the militarization of cyberspace, turning it "into a realm of endless conflict."[548] Nevertheless, after recalling that the Charter applies in its entirety, the 2021 GGE Report noted "the inherent right of States to take measures consistent with international law and as recognized in the Charter and the need for continued study on this matter."[549] This conclusion can be interpreted as an implicit acceptance that States have the right to self-defense in cyberspace, given that the word "inherent" appears only in Article 51 within the entire Charter.[550]

---

[544] Delerue, *Cyber Operations,* 318.

[545] Kouloufakos, "Cyber Operations as Threats," 18.

[546] Delerue, *Cyber Operations,* 325.

[547] Delerue, *Cyber Operations,* 326.

[548] Väljataga, "Back to Square One."

[549] UN GGE, *2021 Report*, 18.

[550] Schmitt and Pakkam, "Regulation of Cyber Warfare," 209.

The majority of national positions by States on this subject also support the notion that States have the right to self-defense in cyberspace.[551] Accordingly, it can be accepted that States have right of self-defense in cyberspace just as they do in the physical realm. On the other hand, the Tallinn Manual remarks that "[a] State that is the target of a cyber operation that rises to the level of an armed attack may exercise its inherent right of self-defence."[552]

Like any other form of attack, cyber operations can potentially constitute an armed attack on their own, granting a State the right to self-defense under Article 51 of the Charter.[553] Most States and the Tallinn Manual adopt the approach of the ICJ, which distinguishes the use of force from its most severe forms, basing the distinction on the consequences of the specific cyber operation in question.[554] In this context, Finland stated that

> [w]hile there is currently no established definition of a cyberattack that would pass the threshold of "use of force" in the sense of article 2(4) of the UN Charter, or "armed attack" in the sense of Article 51, it is widely recognized that such a qualification depends on the consequences of a cyberattack.[555]

Accordingly, a cyber operation will constitute an armed attack if its scale and effect are sufficient to qualify it as a "most grave form of use of force."[556] For instance, the African Union observes that whether a cyber operation constitutes an armed attack "should be thoroughly substantiated on the basis of an assessment of the scale and effects of the particular cyber operation."[557] Just as assessments of the use of force, the

---

[551] *See* International cyber law: interactive toolkit, "Common and National Positions."

[552] Schmitt, *Tallinn Manual,* 339.

[553] Schmitt, *Tallinn Manual,* 340.

[554] Schmitt and Pakkam, "Regulation of Cyber Warfare," 213.

[555] Ministry of Foreign Affairs of Finland, *International Law and Cyberspace*, 6.

[556] Carlo Focarelli, "Self-Defence in Cyberspace," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar Publishing, 2021), 328.

[557] African Union Peace and Security Council, *Common African Position*, 7.

assessment of armed attacks is also made in comparison to non-cyber operations.[558] As stated by Germany, "[m]alicious cyber operations can constitute an armed attack whenever they are comparable to traditional kinetic armed attack in scale and effect."[559] The assessment is contextual, as Norway observes that

> [a] cyber operation may constitute use of force or even an armed attack if its scale and effects are comparable to those of the use of force or an armed attack by conventional means. This must be determined based on a case-by-case assessment having regard to the specific circumstances.[560]

In this regard, both cyber operations that cause physical consequences, such as death or injury to individuals or damage to property, and cyber operations that do not cause such consequences may constitute an armed attack if their scale and effects reach a level comparable to the most grave forms of the use of force under traditional kinetic armed attacks.[561] The effects also include all reasonably foreseeable consequences of the cyber operation in question.[562] This conclusion can be seen in the national position of Singapore, which states that

> [m]alicious cyber activity attributable to a State that causes death, injury, physical damage or destruction equivalent to a traditional non-cyber armed attack, or presenting an imminent threat thereof, would constitute an armed attack. … In Singapore's view, it is also possible that, in certain limited circumstances, malicious cyber activity may amount to an armed attack even if it does not necessarily cause death, injury, physical damage or destruction, taking into account the scale and effects of the cyber activity.[563]

The accumulation of events theory referred to earlier is also valid in cyberspace. It holds that cyber operations that do not constitute an armed attack on their own may

---

[558] Schmitt and Pakkam, "Regulation of Cyber Warfare," 217.

[559] Federal Government of Germany, *Application of International Law in Cyberspace*, 6.

[560] UNGA, *Official Compendium*, 70.

[561] Delerue, *Cyber Operations,* 332-333.

[562] Schmitt, *Tallinn Manual,* 343.

[563] UNGA, *Official Compendium*, 84.

cumulatively amount to an armed attack.[564] Given that below the threshold cyber operations are widespread in cyberspace, assessing each operation in isolation may fail to capture the true gravity of the operation. In this context, when multiple attacks are linked by timing, origin, and intent they must be assessed cumulatively.[565] The accumulation of events theory in cyberspace finds support in the national positions of several States. For example, France underlines that

> [c]yberattacks which do not reach the threshold of an armed attack when taken in isolation could be categorised as such if the accumulation of their effects reaches a sufficient threshold of gravity, or if they are carried out concurrently with operations in the physical sphere which constitute an armed attack, where such attacks are coordinated and stem from the same entity or from different entities acting in concert.[566]

The matter of anticipatory self-defense in cyberspace is as controversial as it is in the physical realm. While the African Union expressed its skepticism by noting that the issue remains contentious and "from a policy perspective, the maintenance of international peace and security favors the continued adoption of a restrictive interpretation of the exceptions to the prohibition on the use of force."[567] Australia, on the other hand, underlines that

> [a] State may act in anticipatory self-defence against an armed attack when the attacker is clearly committed to launching an armed attack, in circumstances where the victim will lose its last opportunity to effectively defend itself unless it acts.[568]

The majority of the Tallinn Manual experts adopted the "last feasible window of opportunity" approach, permitting a State to conduct anticipatory self-defense "against an armed attack, whether cyber or kinetic, when the attacker is clearly committed to launching an armed attack and the victim State will lose its opportunity to effectively

---

[564] Delerue, *Cyber Operations,* 334.

[565] Schmitt, *Tallinn Manual,* 342.

[566] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 7.

[567] African Union Peace and Security Council, *Common African Position*, 7.

[568] UNGA, *Official Compendium*, 6.

defend itself unless it acts."[569] Although this is the case, it does not seem appealing to grant the right of anticipatory self-defense to States in cyberspace, since the identification and assessment of a cyber operation that would amount to an armed attack are inherently difficult,[570] and that the right of anticipatory self-defense is opposed by the majority of States and doctrine in international law, as mentioned above.

Just as with anticipatory self-defense whether the right of self-defense applies only to States or also extends to non-State actors whose actions are not attributable to a State remains controversial. For instance, while France states that "France does not recognise the extension of the right to self-defence to acts perpetrated by non-State actors whose actions are not attributable, directly or indirectly, to a State,"[571] the United States, on the contrary, observes that "[t]his inherent right of self-defense against an actual or imminent armed attack in or through cyberspace applies whether the attacker is a State actor or a non-State actor."[572] On the other hand, according to the Tallinn Manual, this right applies not only against cyber operations conducted by States but also against those conducted by non-State actors whose actions cannot be attributed to any State, such as terrorist or rebel groups.[573]

Lastly, self-defense in cyberspace must be necessary, proportionate, and immediate,[574] and the UN Security Council must be notified.[575] This aspect is supported by the national positions of the States. For instance, Brazil observes that

[569] Schmitt, *Tallinn Manual,* 351.

[570] Delerue, *Cyber Operations,* 447.

[571] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 7.

[572] UNGA, *Official Compendium*, 137.

[573] Schmitt, *Tallinn Manual,* 345.

[574] Schmitt, *Tallinn Manual,* 347.

[575] Schmitt, *Tallinn Manual,* 355.

> self-defense should be a temporary remedy. Member States that exercise their right to self-defense must immediately report it to the Security Council, in line with Article 51 of the Charter. Given the novelty of cyberattacks and the uncertainties related to it, reporting to the Security Council is even more important. … Finally, as with responses to armed activities using conventional weapons, self-defense against armed attacks caused by digital means must be necessary and proportionate.[576]

States also have the right to collective self-defense under the additional conditions of declaration and request by the victim State and "may only be exercised at the request of the victim State and within the scope of the request."[577] This conclusion is reflected in the common position of the European Union, which states that

> [w]hen a State invokes the right of self-defence in response to an armed attack, it may ask other States to act in its support or on its behalf. The right of self-defence may thus be exercised collectively but only at the specific request of the victim State. All relevant rules and limitations of self-defence equally apply to collective self-defence.[578]

Accordingly, States are entitled to use the right of collective self-defense when a State declares itself the victim of an armed attack and makes a request for assistance. Collective self-defense is also subject to the same limitations as individual self-defense in order to be lawful. In this regard, collective self-defense must be necessary, proportionate, and immediate, and it must also be reported to the UN Security Council.

3.5.6. Prohibition of Threat/Use of Force and Critical Infrastructures

Cyber operations against critical infrastructures might violate the prohibition of use of force, targeting national critical infrastructure in cyber operations is an important factor in assessing the use of force. A cyber-attack that does not qualify as a use of force may still be considered as such under the same circumstances if it targets critical

[576] UNGA, *Official Compendium*, 20.

[577] Schmitt, *Tallinn Manual,* 354.

[578] Council of the European Union, *International Law in Cyberspace*, 10.

infrastructure.[579] This fact is even more relevant if a target-based approach is embraced in assessing the use of force.

While it is clear that cyber operations resulting in physical damage to CIs would constitute a use of force, it is less certain that cyber operations against CIs that cause no physical effects. Nonetheless, a cyber-attack that only leads to a loss of functionality of CI might amount to the use of force if that loss is significant enough to threaten national or State security.[580] It should be noted that not all cyber operations against CI without physical consequences qualify as a use of force; a cyber operation that causes limited effects may not qualify as a use of force: the cyber operation in question must cause a significant disruption of essential services by rendering CI ineffective or unusable.[581]

The fact that cyber operations targeting CIs might constitute a prohibited use of force is also reflected in the national positions of States. Norway exemplified that "a cyber operation causing severe disruption to the functioning of the … governmental or private power grid- or telecommunications infrastructure … could amount to the use of force in violation of Article 2(4)."[582] Likewise, the African Union observes that "a cyber operation that destroys, inflicts damage, or permanently disables critical infrastructure or civilian objects within a State, may be considered as amounting to a use of force under international law."[583]

The issue of cyber operations causing severe economic consequences without any physical effects by targeting financial and banking systems, which are considered critical infrastructures, remains unresolved.[584] Some States advocate that cyber

[579] Delerue, *Cyber Operations,* 304.

[580] Roscini, "Cyber Operations," 308.

[581] Roscini, "Cyber Operations," 312.

[582] UNGA, *Official Compendium*, 70.

[583] African Union Peace and Security Council, *Common African Position*, 6-7.

[584] Schmitt and Pakkam, "Regulation of Cyber Warfare," 207.

operations with severe economic consequences may constitute a use of force. For instance, the Netherlands observes that "at this time it cannot be ruled out that a cyber operation with a very serious financial or economic impact may qualify as the use of force."[585] Similarly, Norway notes that "the use of crypto viruses or other forms of digital sabotage against a State's financial and banking system, or other operations that cause widespread economic effects and destabilisation, may amount to the use of force."[586]

Cyber operations targeting critical infrastructures may also violate the prohibition of the threat of force if a State directly or indirectly declares that it will target critical infrastructures in a manner that could constitute an unlawful use of force when executed. Just as the prohibition on the use of force is reflected in the national positions of States, the prohibition on the threat of force is similarly recognized. For instance, Estonia observes that "[a] cyber operation that targets critical infrastructure and results in serious damage, injury or death, or a threat of such an operation, would be an example of use of force."[587]

Cyber operations against CIs may also constitute an armed attack, which is the most grave form of use of force,[588] and would trigger a State's right to self-defense under Article 51 of the UN Charter if the cyber operation in question reaches the armed attack threshold in terms of its scale and effects. This is particularly relevant because cyber operations against CIs are more likely to cause death or injury to people or damage to objects, which would classify such operations as an armed attack.[589]

[585] UNGA, *Official Compendium*, 58.

[586] UNGA, *Official Compendium*, 70.

[587] UNGA, *Official Compendium*, 26.

[588] ICJ, *Nicaragua*, para 191.

[589] Focarelli, "Self-Defense," 329.

It should also be noted that a cyber operation that constitutes a use of force but does not amount to an armed attack can still do so if the same cyber operation targets CIs.[590] For instance, France states that "an operation in cyberspace that caused a failure of critical infrastructure with significant consequences."[591] might constitute an armed attack. Similarly, New Zealand exemplifies that "cyber activity that disables the cooling process in a nuclear reactor … would constitute an armed attack."[592] Australia also observes that a State might act in self-defense to an "armed attack in the form of an offensive cyber operation ... which could cause large-scale … damage to critical infrastructure."[593] On the other hand, Norway states that "the nature of the target (such as critical infrastructure)" is one of the factors that may be included in the assessments of armed attacks.[594] Accordingly, cyber operations targeting CIs could be considered an armed attack if they reach the necessary scale and effects.

The best example demonstrating how cyber operations can constitute a prohibited use of force or even amount to an armed attack is the Stuxnet incident in 2010. Although not labeled as such by the victim of the attack, Iran, Tallinn Manual experts unanimously believe that it constitutes a prohibited use of force, with some experts also labeling Stuxnet as an armed attack triggering the right of self-defense.[595]

In conclusion, this chapter establishes that the protection of CIs in cyberspace is anchored in the dynamic interplay of several core rules of international law. Although the rules analyzed in this chapter predates cyberspace, they can form a coherent legal framework when interpreted in an adaptive manner that reflects realities of cyberspace. This study argues that treating sovereignty as standalone rule is crucial to close the

[590] Delerue, *Cyber Operations,* 342.

[591] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 5-6.

[592] Ministry of Foreign Affairs and Trade of New Zealand, *Application of International Law in Cyberspace*, para. 8.

[593] UNGA, *Official Compendium*, 6.

[594] UNGA, *Official Compendium*, 70.

[595] Schmitt, *Tallinn Manual,* 342.

protection gap created by cyber operations that fall below a prohibited intervention but nevertheless cause significant functional disruptions to CIs.

Furthermore, the complementary obligation of due diligence emerges as an important mechanism for engaging State responsibility in the face of the attribution challenge. Regarding the most serious cyber threats, this study argues that the prohibition on the use of force is most effectively applied through a consequence-based approach, which finds the most State support in the national positions on the matter, where strategic significance of the target, most notably CIs, serves as a key of the operation's scale and effects.

Ultimately, this legal framework of peacetime ensures that CIs are not merely technical assets but legally protected pillars of societal stability, where the legality of a cyber operation is determined by its potential to paralyze essential societal functions.

CHAPTER 4

PROTECTION OF CRITICAL INFRASTRUCTURES IN ARMED CONFLICT

International Humanitarian Law (IHL) is the branch of international law that regulates the conduct of hostilities during armed conflict, which can be described as

> a set of rules that seeks, for humanitarian reasons, to limit the effects of armed conflict. It protects persons who are not, or are no longer, directly or actively participating in hostilities, and imposes limits on the means and methods of warfare.[596]

Regulation of the conduct of hostilities and warfare is not a new phenomenon; throughout history, various civilizations, including the West, the Islamic world, Japan, and China, have developed their own rules and traditions regarding wartime situations.[597] Until the codification of the First Geneva Convention in 1864, IHL existed as customary law, with rules governing warfare embedded in traditions and customs.[598]

During the codification efforts between 1864 and the adoption of the 1949 Geneva Conventions (GC), which updated the 1864 Convention, two strands of the law of armed conflict emerged: while Geneva law primarily focused on the protection of victims of armed conflicts and emphasized the humanitarian aspect, Hague law evolved with the 1899 and 1907 Regulations, which addressed the conduct of

[596] International Committee of Red Cross, *What is International Humanitarian Law* (ICRC, 2022), 1.

[597] Amanda Alexander, "A Short History of International Humanitarian Law", *European Journal of International Law* 26, no 1 (2015): 112, https://doi.org/10.1093/ejil/chv002.

[598] Jean-Marie Henckaerts, "History and Sources", in *The Oxford Guide to International Humanitarian Law*, ed. Ben Saul and Dapo Akande, (Oxford University Press, 2020), 2.

hostilities with a focus on the means and methods of warfare.[599] These two strands merged through the adoption of the 1977 Additional Protocol I (AP I) to the 1949 Geneva Conventions.[600]

As of today, IHL stands as one of the most codified branches of international law, encompassing various treaties concerning subjects such as weapons and methods of warfare, the protection of cultural property, and international criminal law.[601] The 1949 Geneva Conventions, along with their Additional Protocols, constitute the main treaties that enjoy universal acceptance and adherence.[602]

Although IHL is rich in treaty law, customary law continues to play a major role within this body of international law. Article 1(2) of AP I, which reflects the Martens Clause included in the Hague Conventions of 1899 and 1907,[603] states that "in cases not covered by this Protocol or by other international agreements, civilians and combatants remain under the protection and authority of the principles of international law derived from established custom."[604] In this regard, customary law fills the gap left by treaty law and binds parties to a conflict, whether or not they have ratified a particular IHL treaty.[605] Military manuals, battlefield behavior, verbal acts, and the treatment of persons by States can be utilized when identifying customary IHL rules.[606]

---

[599] Henckaerts, "History and Sources," 3.

[600] Henckaerts, "History and Sources," 3.

[601] Robert Kolb and Katherine Del Mar, "Treaties for Armed Conflict," in *The Oxford Handbook of International Law in Armed Conflict*, ed. Andrew Clapham and Paola Gaeta, (Oxford University Press, 2014), 60-65.

[602] David Turns, "The Law of Armed Conflict (International Humanitarian Law)," in *International Law*, ed. Malcolm Evans, 5th ed. (Oxford University Press, 2018), 842.

[603] International Committee of Red Cross, *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949* (Martinus Nijhoff Publishers, 1987), 38.

[604] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), opened for signature June 8, 1977, 1125 UNTS 3, Article 1(2).

[605] Marco Sassòli, *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*, 2nd ed., (Edward Elgar Publishing, 2024), 55.

[606] Henckaerts, "History and Sources," 17.

In addition to treaty and customary law, general principles of IHL are also important for its application. Although these principles are not directly applicable to certain situations, they are useful in interpreting existing rules and filling the gaps left by both treaty and customary law.[607] The role of the general principles of IHL is acknowledged by AP I and the ICJ.[608] General principles of IHL include the principles of humanity, military necessity, distinction and prohibition of causing unnecessary suffering.[609]

After discussing how international law can be utilized in peacetime for CI protection, this section will focus on the CI protection in times of cyber armed conflicts. In this regard, this section will examine the threshold of a cyber armed conflict, which triggers application of the IHL and later how IHL's relevant rules and primary principles of distinction, proportionality, and precautions apply in cyberspace and how they can be utilized in CI protection in times of armed conflicts.

4.1. Applicability of International Humanitarian Law: Cyber Armed Conflicts

According to Common Articles 2 and 3 of the Geneva Conventions, IHL applies in situations of armed conflict, whether international and non-international in character. Although the Geneva Conventions and Additional Protocols do not offer a definition of the term "armed conflict," the International Criminal Tribunal for the Former Yugoslavia (ICTY) defined the term in the *Tadić* case by observing that

> armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State. International humanitarian law applies from the initiation of such armed conflicts.[610]

[607] Sassòli, *International Humanitarian Law*, 57.

[608] ICJ, *Nuclear Weapons*, para 78, 87.

[609] Henckaerts, "History and Sources," 21.

[610] International Criminal Tribunal for the Former Yugoslavia (ICTY), *The Prosecutor v. Dusko Tadić*, Case No. IT-94-1, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, October 2 1995, para 70, https://www.icty.org/x/cases/tadic/acdec/en/51002.htm.

The presence of an armed conflict, whether international or non-international, is a prerequisite for the application of IHL, and the conduct subject to IHL rules must be connected to the armed conflict.[611] Therefore, if no armed conflict exists, IHL does not apply. The same holds true for conduct that has no connection to armed conflict. Determining the existence of an armed conflict depends on the facts on the ground.[612] As a result, IHL applies when armed conflict exists, regardless of whether the parties involved recognize it as such.[613] The existence of armed conflicts can be assessed by various actors, such as the parties to the conflict, the UN, and the ICRC, and this assessment must be made in good faith in accordance with the facts on the ground and the criteria established by IHL, regardless of who conducts the assessment.[614] However, as exceptions, it should be noted that there are some rules that apply in peacetime, such as Articles 47, 49, and 54 of the First Convention.[615]

IHL regulates and distinguishes between two types of armed conflicts: International armed conflicts (IACs) and non-international armed conflicts (NIACs). This distinction has its roots in the evolution of IHL: it emerged to regulate armed conflicts between equal sovereign States, and it is impossible for a State to legitimize and extend the rights granted by IHL, which are for its equal sovereign opponents, to the individuals or groups that fight against it within its own territory, a place where the State maintains a monopoly on the use of force.[616] There are also among some States that the uniform application of IHL rules could harm State sovereignty by legitimizing

[611] Sassòli, *International Humanitarian Law*, 16.

[612] Sassòli, *International Humanitarian Law*, 21.

[613] International Committee of the Red Cross (ICRC), *Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field* (Cambridge University Press, 2016), 77.

[614] ICRC, *Commentary on GC I*, 78.

[615] ICRC, *Commentary on GC I*, 72.

[616] Geoffrey S. Corn et. al., *The Law of Armed Conflict: An Operational Approach*, First edition, Aspen Casebook Series (Wolters Kluwer, 2012), 67-70.

secessionist movements under international law and paving the way for international intervention on behalf of non-State groups.[617]

Although this separation has narrowed in recent times, as the ICRC observed that 136 out of 161 customary IHL rules apply equally to both IACs and NIACs, the IHL regimes for these two types of armed conflicts remain different.[618] For instance, it is generally accepted today that the type of armed conflict is of little relevance regarding the rules governing the conduct of hostilities; however, the rules regarding the status of the parties to the conflict remain different for both types of conflicts.[619] In this regard, the ICTY observed that "[s]ince the 1930s … international legal rules have increasingly emerged or have been agreed upon to regulate internal armed conflict"[620] and observed that some IHL rules originally designed to regulate IACs-covering issues such as "protection of civilians from hostilities," "protection of civilian objects," and "prohibition of means of warfare proscribed in international armed conflicts and ban of certain methods of conducting hostilities" extend to NIACs.[621] It also emphasized that "[p]rinciples and rules of humanitarian law reflect "elementary considerations of humanity" widely recognized as the mandatory minimum for conduct in armed conflicts of any kind,"[622] but nevertheless went on to state that

> only a number of rules and principles governing international armed conflicts have gradually been extended to apply to internal conflicts; and this extension has not taken place in the form of a full and mechanical transplant of those rules to internal conflicts; rather, the general essence of those rules, and not the detailed regulation they may contain, has become applicable to internal conflicts.[623]

---

[617] Dapo Akande, "Classification of Armed Conflicts," in *The Oxford Guide to International Humanitarian Law*, ed. Ben Saul ve Dapo Akande, (Oxford University Press, 2020), 32.

[618] Sassòli, *International Humanitarian Law*, 19-20.

[619] Louise Arimatsu, "Classifying Cyber Warfare," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar Publishing, 2021), 410.

[620] ICTY, Tadić Appeal on Jurisdiction, para. 97.

[621] ICTY, Tadić Appeal on Jurisdiction, para. 127.

[622] ICTY, Tadić Appeal on Jurisdiction, para. 129.

[623] ICTY, Tadić Appeal on Jurisdiction, para. 126.

Since they remain distinct, the legal regime for IACs and NIACs will be examined separately.

4.1.1. International Armed Conflicts

International humanitarian law is applicable in situations of international armed conflicts under Common Article 2 of the Geneva Conventions:

> In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the State of war is not recognized by one of them.[624]

Accordingly, IHL applies when an armed conflict arises between two or more States. In addition to conflicts between States, IHL also applies in situations of belligerent occupation,[625] as well as in wars waged to realize the right of self-determination under the UN Charter.[626]

An assessment of the existence of an IAC depends on the *de facto* situation on the ground: If a State is attacked by another State or a non-State actor whose actions are attributable to a State, an IAC comes into existence and IHL starts to apply under Common Article 2 of the Conventions.[627] There is no threshold of intensity of violence required to trigger the application of IHL in IACs, as the ICTY observed that "the existence of armed force between States is sufficient of itself to trigger the application of international humanitarian law."[628] The ICRC has stated that "any unconsented-to military operations by one State in the territory of another State should be interpreted

---

[624] "Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field," (First Geneva Convention) opened for signature August 12, 1949, 75 U.N.T.S. 31, Article 2. https://treaties.un.org/doc/Publication/UNTS/Volume%2075/volume-75-I-970-English.pdf

[625] First Geneva Convention, Article 2.

[626] Additional Protocol I, Article 1(4).

[627] Sassòli, *International Humanitarian Law*, 187-188.

[628] International Criminal Tribunal for the Former Yugoslavia (ICTY), *The Prosecutor v. Mucić et al*., Case No. IT-96-21, Judgment, November 16, 1998, para 184, https://www.icty.org/x/cases/mucic/tjug/en/

as an armed interference in the latter's sphere of sovereignty and thus may be an international armed conflict."[629]

In such situations, IHL applies whether there is a declaration of war between States and regardless of the intensity of the force used by the attacking State.[630] Likewise, there is no need for State parties to recognize each other to trigger the applicability of IHL, as long as the other party is the *de jure* government of a State or has *de facto* control over one.[631] Accordingly, an armed attack perpetrated by a State against the victim State's territory, population, and objects, including military and civilian infrastructure, triggers the application of IHL.[632]

Similarly, an IAC may also come into existence when a State intervenes in a conflict taking place in the territory of another State between that State and a non-State group fighting against it in support of that group.[633] Although the assessment of whether an IAC exists depends on the facts on the ground, the Statehood of the parties and the attribution of actions of non-State actors to a State are governed by other branches of international law, namely the law of Statehood and the law of State responsibility.[634] It should also be emphasized that joining multinational military operations does not absolve States of their obligations under IHL, given that States retain a degree of authority over their national military units participating in such operations.[635] In a similar fashion, international organizations conducting military operations are bound by customary IHL, as they cannot be parties to the Conventions but are nevertheless subjects of international law.[636]

---

[629] ICRC, *Commentary on GC I*, 236.

[630] ICRC, *Commentary on GC I*, 78, 85.

[631] Sassòli, *International Humanitarian Law*, 188.

[632] ICRC, *Commentary on GC I*, 81-82.

[633] ICRC, *Commentary on GC I*, 94-95.

[634] Sassòli, *International Humanitarian Law*, 188.

[635] ICRC, *Commentary on GC I*, 41.

[636] ICRC, *Commentary on GC I*, 42.

International humanitarian law begins to apply at the moment an IAC exists[637] and ceases to apply with the "general close of military operations."[638] Just as assessing the existence of IACs relies on the facts on the ground, the evaluation of "general close of military operations" also depends on these facts.[639] These facts must demonstrate that the conflict in question is effectively terminated.[640] In this regard, while a ceasefire, armistice, or peace treaty might serve as a sign that conflict has effectively ended, they alone are insufficient if the situation on the ground reflects a different reality.[641]

On the other hand, IHL remains applicable throughout the entire territory, territorial waters, and airspace of the parties involved in the conflict, as demonstrated by the ICTY in the *Tadić* case "international humanitarian law continues to apply in the whole territory of the warring States … whether or not actual combat takes place there."[642] The other States that are not a party to the conflict are subject to the law of neutrality, which stipulates that the conduct of hostilities in the territory of a neutral State is prohibited.[643]

Lastly, whether the IAC in question is initiated in accordance with *jus ad bellum* carries no importance regarding the applicability of the IHL rules: IHL rules apply in the same manner to IACs, regardless of whether the conflict was started justly or not.[644] Likewise, *jus ad bellum* rules cannot be utilized to interpret IHL rules.[645]

---

[637] Emily Crawford, "The Temporal and Geographic Reach of International Humanitarian Law," in *The Oxford Guide to International Humanitarian Law*, ed. Ben Saul and Dapo Akande (Oxford University Press, 2020), 57.

[638] Additional Protocol I, Article 3(b).

[639] ICRC, *Commentary on GC I*, 103.

[640] Crawford, "Temporal and Geographic Reach," 62.

[641] ICRC, *Commentary on GC I*, 103.

[642] ICTY, Tadić Appeal on Jurisdiction, para 70.

[643] Crawford, "Temporal and Geographic Reach," 69.

[644] ICRC, *Commentary on GC I*, 61.

[645] Sassòli, *International Humanitarian Law*, 500.

4.1.2. Non-International Armed Conflicts

Another situation in which IHL applies is non-international armed conflicts under Common Article 3 of the Geneva Conventions, which triggers the application of IHL "[i]n the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties."[646] In this regard, Common Article 3, the core provision for non-international conflicts, outlines the minimum obligations that parties to a conflict must follow. As such, it is labeled as "Convention in miniature."[647] The ICJ acknowledges the fundamental character of Common Article 3 as it "constitute[s] a minimum yardstick" for all kinds of armed conflicts and reflects "elementary considerations of humanity."[648] Accordingly, a non-international armed conflict within the meaning of Common Article 3 involves at least one non-State actor. In this context, Common Article 3 applies not only to armed conflicts between a State and a non-State actor but also to armed conflicts between two or more non-State actors.[649]

Conditions for the applicability of IHL in a NIAC are different from IACs, where IHL is triggered at the moment there is an armed conflict between States. Unlike IACs, NIACs must meet two conditions to trigger the application of IHL: firstly, the non-State actor or actors that become parties to a NIAC must have a degree of organization, and second, the violence in the conflict must reach a certain level of intensity.[650] Whether a NIAC exists depends on the facts on the ground, and both criteria must be met cumulatively.[651]

To meet the organization criteria, it is not necessary for a non-State group's level of organization to reach that of State armed forces. Instead, the non-State group "ha[s] to

[646] First Geneva Convention, Article 3.

[647] ICRC, *Commentary on GC I*, 131.

[648] ICJ, *Nicaragua*, para. 218.

[649] ICRC, *Commentary on GC I*, 143.

[650] Sassòli, *International Humanitarian Law*, 199-200.

[651] ICRC, *Commentary on GC I*, 158.

be under a certain command structure and have the capacity to sustain military operations" and the group in question "must possess a certain level of hierarchy and discipline and the ability to implement the basic obligations of IHL."[652] While there are no definite criteria in international law for assessing whether a non-State actor is sufficiently organized, the ICTY in the *Haradinaj* judgment observed that some factors can be indicative and listed these factors as

> the existence of a command structure and disciplinary rules and mechanisms within the group; the existence of a headquarters; the fact that the group controls a certain territory; the ability of the group to gain access to weapons, other military equipment, recruits and military training; its ability to plan, coordinate and carry out military operations, including troop movements and logistics; its ability to define a unified military strategy and use military tactics; and its ability to speak with one voice and negotiate and conclude agreements such as ceasefire or peace accords.[653]

In addition to the organization requirement, violence between parties must reach a certain degree of intensity. Similar to the organizational criteria, no specific standards exist for assessing whether violence in a NIAC meets the necessary intensity to trigger the application of IHL. ICTY in the *Haradinaj* judgment highlighted indicative factors for evaluating the intensity criteria, such as

> number, duration and intensity of individual confrontations; the type of weapons and other military equipment used; the number and calibre of munitions fired; the number of persons and type of forces partaking in the fighting; the number of casualties; the extent of material destruction; and the number of civilians fleeing combat zones. The involvement of the UN Security Council may also be a reflection of the intensity of a conflict.[654]

On the other hand, the application of Additional Protocol II (AP II), which governs NIACs, is slightly different from the application of Common Article 3. According to AP II, the Protocol applies to NIACs that take place

---

[652] ICRC, *Commentary on GC I*, 156.

[653] International Criminal Tribunal for the Former Yugoslavia (ICTY), *The Prosecutor v. Haradinaj et al.,* Case No. IT-04-84, Judgment, April 3, 2008, para. 60, https://www.icty.org/x/cases/haradinaj/tjug/en/121129_judgement_en.pdf.

[654] ICTY, Haradinaj Judgement, para 49.

> which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations.[655]

In this regard, Article 1 of AP II adds additional criteria for its application: namely, the NIAC regulated by AP II must take place within the territory of a signatory State to AP II, its armed must be involved, and the non-State actor must control a portion of that State's territory. It should be further noted that AP II is supplementary to Common Article 3 "without modifying its existing conditions of application."[656]

IHL applies to NIACs from the moment they exist and ceases to apply when a peaceful settlement is reached.[657] The assessment of cessation of a NIAC must be based on facts on the ground.[658] From the beginning of its application, IHL binds all parties to the conflict, whether they are a State or non-State actor, and those actors must comply with the guarantees set in Common Article 3.[659] Parties to a NIAC are bound by the customary IHL rules regarding NIACs and international human rights law.[660] Geographically, IHL applies equally across the entire territory of the State where the NIAC occurs for conduct that has a sufficient nexus to the NIAC in question.[661] Conduct that does not have a sufficient nexus to the NIAC falls outside the scope of IHL and is subject to the domestic law of the State.[662] It is also possible for IHL to

---

[655] "Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Additional Protocol II)," opened for signature June 8, 1977, U.N.T.S. 609, Article 1(1), https://treaties.un.org/doc/Publication/UNTS/Volume%201125/volume-1125-I-17513-English.pdf.

[656] Additional Protocol II, Article 1(1).

[657] ICTY, Tadić Appeal on Jurisdiction, para 70.

[658] ICRC, *Commentary on GC I*, 175.

[659] ICRC, *Commentary on GC I*, 182.

[660] ICRC, *Commentary on GC I*, 183.

[661] Sassòli, *International Humanitarian Law*, 206.

[662] ICRC, *Commentary on GC I*, 166.

apply to NIACs that have spilled over into the territories of other States if the conduct occurring in the territory of another State is connected to the NIAC in question.[663]

4.1.3. Notion of Attack in International Humanitarian Law

After dealing with the situations to which IHL applies, the notion of "attack" in IHL will be briefly discussed, as most IHL rules regulate attacks as forms of conduct. The notion of "attack" is defined in Article 49(1) of AP I, which states that "[a]ttacks mean acts of violence against the adversary, whether in offence or in defence."[664] This definition in AP I is also valid in the context of NIACs.[665] The definition provided by AP I is broader than the vocabulary meaning of the concept, as it encompasses both offensive and defensive acts.[666] In this regard, the concept "refers simply to the use of armed force to carry out a military operation at the beginning or during the course of armed conflict"[667] as a "technical term relating to a specific military operation limited in time and place."[668]

Whether an act conducted in a military campaign qualifies as an attack and thus falls under IHL rules depends on the consequences of the act in question, which must meet a threshold of harm.[669] Consequently, a military operation that causes destructive consequences, such as death and injury to individuals or physical harm to property, may be classified an attack.[670] Violence occupies a central place in qualifying an act as an attack; therefore, military operations such as espionage, psychological operations, or propaganda that do not cause such effects would not qualify as attacks

[663] Akande, "Classification of Armed Conflicts," 42.

[664] Additional Protocol I, Article 49(1).

[665] ICRC, *Commentary on Additional Protocols,* 1452.

[666] ICRC, *Commentary on Additional Protocols,* 603.

[667] ICRC, *Commentary on Additional Protocols,* 603.

[668] ICRC, *Commentary on Additional Protocols,* 1452.

[669] Schmitt, *Tallinn Manual,* 416.

[670] Schmitt, *Tallinn Manual,* 417.

and are excluded from the scope of IHL.[671] However, the notion of attack is not limited to conduct that produces kinetic force: it is accepted that chemical, biological, and radiological attacks, which do not generally produce such effects, constitute attacks under Article 49(1) of AP I.[672]

4.1.4. Applicability of International Humanitarian Law in Cyberspace

In the cyber context, it is widely accepted among States that IHL rules apply to cyber operations that take place in the context of an armed conflict. Although disagreement over the applicability of IHL rules is one of the reasons for the collapse of the 2017 GGE process, States affirmed that

> international humanitarian law applies only in situations of armed conflict … established international legal principles including, where applicable, the principles of humanity, necessity, proportionality, and distinction … and underscored that recalling these principles by no means legitimizes or encourages conflict.[673]

This view confirms the consensus among legal experts[674] and reflects the position of international organizations such as NATO, the EU, and the ICRC.[675] For instance, the African Union affirms that although "most rules of IHL emerged before the appearance of cyberspace, IHL applies, concurrently with any other applicable rules of international law, to cyber-operations that may be undertaken in the context of an armed conflict."[676] Similarly, the European Union observes that "[i]nternational

---

[671] Michael Bothe, Karl Josef Partsch, and Waldemar A. Solf, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, 2nd ed. (Martinus Nijhoff Publishers, 2013), 329.

[672] Schmitt, *Tallinn Manual,* 415.

[673] UN GGE, *2021 Report*, 18.

[674] International Committee of Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts* (ICRC, 2024), 57, https://www.icrc.org/en/report/2024-icrc-report-ihl-challenges.

[675] Michael N. Schmitt, "Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations," *International Review of the Red Cross* 101, no. 910 (2019): 334, https://doi.org/10.1017/S1816383119000018.

[676] African Union Peace and Security Council, *Common African Position*, 8.

humanitarian law (IHL) applies to cyber operations conducted in the context of an armed conflict, whether international or non-international in character."[677] Likewise, Cuba, which openly opposed the applicability of IHL in cyberspace during 2017 GGE process, went on to declare that "International Humanitarian Law (IHL) only applies in conflict situations. The applicability of IHL is not limited to cyberspace, nor to any other physical or abstract realm."[678] On the other hand, the Tallinn Manual embraces this view by stating "[c]yber operations executed in the context of an armed conflict are subject to the law of armed conflict."[679] In this regard, ICRC defines such cyber operations as "operations against a computer system or network, or another connected device, through a data stream, when used as means or method of warfare in the context of an armed conflict."[680]

The applicability of IHL to cyberspace is also supported by both treaty law and ICJ jurisprudence. Article 36 of AP I obliges States to determine whether the use of a new weapon is prohibited by the Protocol or any international legal rule in "the study, development, acquisition or adoption of a new weapon, means or method of warfare."[681] Similarly, the ICJ in its *Nuclear Weapons* advisory opinion noted that

> [i]ndeed, nuclear weapons were invented after most of the principles and rules of humanitarian law applicable in armed conflict had already come into existence; the Conferences of 1949 and 1974–1977 left these weapons aside, and there is a qualitative as well as quantitative difference between nuclear weapons and all conventional arms. However, it cannot be concluded from this that the established principles and rules of humanitarian law applicable in armed conflict did not apply to nuclear weapons. Such a conclusion would be incompatible with the intrinsically humanitarian character of the legal principles in question which permeates the entire law of armed conflict and

[677] Council of the European Union, *International Law in Cyberspace*, 7.

[678] NATO Cooperative Cyber Defence Centre of Excellence, "National Position of Cuba (2024)," International cyber law: interactive toolkit, 31 January 2025, https://cyberlaw.ccdcoe.org/wiki/National_position_of_Cuba_(2024).

[679] Schmitt, *Tallinn Manual,* 375.

[680] Laurent Gisel, Tilman Rodenhäuser, and Knut Dörmann, "Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts," *International Review of the Red Cross* 102, no. 913 (2020): 297, https://doi.org/10.1017/S1816383120000387.

[681] Additional Protocol I, Article 36.

> applies to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future.[682]

Accordingly, there is no reason not to apply IHL to cyberspace, even though IHL rules were developed before the advent of cyber operations.

As regards to which cyber operations are subject to IHL, while it is certain that cyber operations conducted as part of, or in support of conventional armed conflict are subject to the rules of IHL, it is less certain whether a cyber operation itself would amount to an armed conflict.[683] Although no cyber operation itself has qualified as an armed conflict to date, and such a possibility seems unlikely,[684] it is still possible for cyber operations to qualify as armed conflicts in the absence of kinetic force.[685] In this regard, cyber operations would qualify as armed conflict in their own right if they meet the conditions established by Common Articles 2 and 3 of the Geneva Conventions.[686] Accordingly, cyber operations conducted against a State by another State or a non-State actor whose actions can be attributed to a State would trigger IHL applicable to IACs, and intense cyber operations carried out by a sufficiently organized non-State actor against other States or non-State actors would activate IHL applicable to NIACs.[687] This conclusion finds support in the positions of States. For instance, Brazil observes that

> [t]here are two instances where IHL might apply to cyber activities. First, if they are carried out as part of an ongoing armed conflict, contributing to conventional operations conducted by the parties. Second, if the cyber

[682] ICJ, *Nuclear Weapons*, para 86.

[683] ICRC, *Commentary on GC I*, 92.

[684] Terry D. Gill, "International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality and The Notion of Attack Under The Humanitarian Law of Armed Conflict," in *Research Handbook on International Law and Cyberspace*,ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar Publishing, 2021), 460.

[685] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 303.

[686] Schmitt, *Tallinn Manual,* 384.

[687] Sassòli, *International Humanitarian Law*, 581.

> activities themselves cross the threshold of violence to be characterized as an armed conflict.[688]

Similarly, Finland states that

> International humanitarian law only applies to cyber operations when such operations are part of, or amount to, an armed conflict. Most so far known cyberattacks have not been launched in the context of an armed conflict or met the threshold of armed conflict. At the same time, when cyber means are used in the context of a pre-existing armed conflict, as has been done in many current conflicts, there is no reason to deny the need for the protections that international humanitarian law provides.[689]

Rules 82 and 83 of the Tallinn Manual are also dedicated to how cyber operations can be classified as IACs or NIACs.[690]

Regarding temporal and geographical limitations, the Tallinn Manual addresses only geographical limitations. Rule 81 of the Manual states that "[c]yber operations are subject to geographical limitations imposed by the relevant provisions of international law applicable during an armed conflict,"[691] and Rule 150 emphasizes that "[t]he exercise of belligerent rights by cyber means directed against neutral cyber infrastructure is prohibited."[692] Although the Manual remains silent on temporal limitations, it can still be asserted that the temporal limitations of IHL in cyberspace are also subject to the relevant provisions of international law.

4.1.4.1. Notion of Attack in Cyberspace

As mentioned above, IHL rules regulate "attacks," which hold the same meaning for both IACs and NIACs in an armed conflict. Since cyber operations can be subject to IHL as standalone armed conflicts or as part of one, these cyber operations are

[688] UNGA, *Official Compendium*, 22.

[689] Ministry of Foreign Affairs of Finland, *International Law and Cyberspace*, 7.

[690] Schmitt, *Tallinn Manual,* 379, 385.

[691] Schmitt, *Tallinn Manual,* 378.

[692] Schmitt, *Tallinn Manual,* 555.

governed by IHL if they qualify as an "attack" under Article 49(1) of AP I. The definition provided in Article 49(1) is based on the act's consequences, namely violence; this definition allows for the classification of acts committed by non-kinetic weapons as attacks when their effects are violent.[693] How cyber operations fit into the definition of an attack in Article 49(1) is controversial, considering that cyber operations can disrupt the functionality of objects without causing physical damage.[694] The interpretation of the concept of attack in the cyber context has significant consequences for civilians and infrastructure in relation to cyber attacks.[695]

Before discussing the controversial aspects, it should be noted that there is a general consensus among States, the ICRC, and experts that cyber operations causing or reasonably expected to cause death or injury to persons or physical damage to objects constitute attacks under IHL.[696] For example, Canada observes that "[c]yber activities are an attack under IHL, whether in offence or defence, where their effects are reasonably expected to cause injury or death to persons or damage or destruction to objects."[697] Similarly, Switzerland underlines that cyber operations that constitute cyber attacks under Article 49(1) "encompasses at the very least cyber operations that are reasonably expected to cause, directly or indirectly, injury or death to persons, or physical damage or destruction to objects."[698] ICRC also states that "[i]t is widely accepted that cyber operations expected to cause death, injury or physical damage

[693] Karine Bannelier, "Is the Principle of Distinction Still Relevant in Cyberwarfare? From Doctrinal Discourse to States Practice," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar Publishing, 2021), 433.

[694] Cordula Droege, "Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians," *International Review of the Red Cross* 94, no. 886 (2012): 557, https://doi.org/10.1017/S1816383113000246.

[695] International Committee of Red Cross (ICRC), *International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper,* (ICRC, 2019), 7, https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

[696] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 312.

[697] Government of Canada, *International Law Applicable in Cyberspace*, para. 49.

[698] UNGA, *Official Compendium*, 94.

constitute attacks under IHL."[699] Tallinn Manual also emphasizes that "a cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[700]

Some States and ICRC also advocate that the indirect or reverberating effects of cyber operations might constitute "attacks" under IHL.[701] In this regard, Denmark believes that cyber operations would "constitute an attack if it can be reasonably expected to cause injury, death, or physical damage to individuals or objects. This definition also includes activity where substantial destruction is caused as a foreseeable secondary effect."[702] ICRC also observes that attack-constituting effects also

> include harm due to the foreseeable direct and indirect (or reverberating) effects of an attack, for example the death of patients in intensive-care units caused by a cyber operation on an electricity network that results in cutting off a hospital's electricity supply.[703]

Contrary to the consensus that cyber operations causing or reasonably expected to cause death or injury to persons, as well as physical damage to objects, constitute an attack under Article 49(1), the issue becomes more controversial for cyber operations that interfere with the functionality of an object without causing physical damage.[704] This topic is particularly significant, given that cyber operations can lead to substantial disruptions in networks and systems without any physical damage.[705]

Most States, along with experts addressing the issue and the ICRC, agree that cyber operations that disable objects without causing any physical damage could be

---

[699] ICRC, *Position Paper,* 7.

[700] Schmitt, *Tallinn Manual,* 415.

[701] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 313.

[702] Kjelgaard and Melgaard, "Denmark's Position Paper," 455.

[703] ICRC, *Position Paper,* 7.

[704] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 313.

[705] ICRC, *Contemporary Armed Conflicts*, 58.

considered an attack under Article 49(1).[706] For example, New Zealand observes that "[a] cyber activity may constitute an "attack" for the purposes of international humanitarian law where it results in death, injury, or physical damage, including loss of functionality."[707] Italy also qualifies cyber operations as attacks "if they constitute an act of violence resulting in more than minimal physical damage of property or disruption in the functioning of critical infrastructure, or human injury and loss of life."[708] Likewise, France observes that cyber operations may amount to an attack under Article 49(1)

> even if there is no human injury or loss of life, or physical damage to goods. Thus, a cyberoperation constitutes an attack if the targeted equipment or systems can no longer provide the service for which they were implemented, including temporarily or reversibly, where action by the adversary is required in order to restore the infrastructure or the system.[709]

Parallel to State's position, the ICRC also emphasizes that "during an armed conflict an operation designed to disable a computer or a computer network constitutes an attack under IHL, whether the object is disabled through kinetic or cyber means."[710] The Tallinn Manual also does not limit effects to only physical ones. The majority of the Manual experts concluded that "interference with functionality qualifies as damage if restoration of functionality requires replacement of physical components."[711]

It should be noted that the ICRC's position and the Manual's conclusion slightly differ: While the Tallinn Manual states that cyber operations would amount to an attack when

---

[706] ICRC, *Contemporary Armed Conflicts*, 58.

[707] Ministry of Foreign Affairs and Trade of New Zealand, *Application of International Law in Cyberspace*, para. 25.

[708] Ministry of Foreign Affairs and International Cooperation of Italian Republic, *Italian Position Paper*, 9-10.

[709] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 12.

[710] ICRC, *Position Paper,* 7-8.

[711] Schmitt, *Tallinn Manual,* 417.

"restoration of functionality requires replacement of physical components,"[712] the ICRC does not seek such a consequence for a cyber operation that causes disruption of functionality of a civilian object to amount an attack under Article 49(1) of AP I.[713] It should also be noted that some experts of the Tallinn Manual also extend this requirement "to situations in which reinstallation of the operating system or of particular data is required in order for the targeted cyber infrastructure to perform the function for which it was designed."[714]

There are also proponents of a narrower approach regarding cyber operations that cause severe disruption of objects without any physical damage, emphasizing that such operations do not constitute an attack under Article 49(1).[715] For instance, Israel observes that "[o]nly when a cyber operation is expected to cause physical damage, will it satisfy this element of an attack under LOAC … the mere loss or impairment of functionality to infrastructure would be insufficient."[716]

Given that cyber operations can cause severe disruptions to the functioning of objects without causing physical harm, it would be better to embrace a broader interpretation so that they are included under the protective umbrella of IHL, which at its core seeks to protect civilians and civilian objects from the damage of armed conflicts. If IHL protections are only triggered by only by destruction or harm comparable to kinetic attacks, cyber operations that cause paralyze a State's energy grid or financial system without physical harm would remain in a gray zone. In addition, Article 52(2) of AP I, which offers a definition for military objectives, explicitly refers to "neutralization" as a possible outcome of attacks.[717] In this regard, the notion of "attack" under Article 49(1) should also be understood to include operations that disrupt objects without

[712] Schmitt, *Tallinn Manual,* 417.

[713] ICRC, *Position Paper,* 8.

[714] Schmitt, *Tallinn Manual,* 417.

[715] Bannelier, "Principle of Distinction," 440.

[716] Schöndorf, "Israel's Perspective," 400.

[717] Additional Protocol I, Article 52(2).

causing physical damage.[718] However, not all cyber operations that produce such outcomes constitute an attack when these operations are solely aimed at blocking communications, provided that they are not part of an assault intended to disrupt the functioning of a civilian object.[719] Aside from that, it is important to note that not all cyber operations can be classified as attacks. For instance, cyber espionage cannot be considered an attack since espionage is excluded from the definition of attack under Article 49(1).[720]

Although a cyber operation falls outside the scope of the definition of "attack," it may still be subject to other rules of IHL.[721] In this context, such operations must not target civilians or civilian objects unless there is a military necessity, and they must also adhere to the general principles of IHL.[722]

In conclusion, cyber operations are subject to IHL when they are conducted alongside an armed conflict or when they amount to an IAC or NIAC themselves. In such situations, cyber operations that constitute an attack in the sense of Article 49(1) of AP I are subject to IHL rules. Cyber operations constitute an attack if they cause death or injury to persons or physical damage to objects. They also constitute an attack if they disrupt the functionality of objects without causing physical damage. In this regard, a cyber operation conducted in the context of an armed conflict that causes damage to a CI or disrupts its functionality without physical damage would be subject to the rules of IHL. How IHL rules can be utilized to protect CI during armed conflicts will be examined below.

[718] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 313.

[719] Droege, "Cyber Warfare," 560.

[720] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 316.

[721] Schmitt, "Wired Warfare 3.0," 338.

[722] United States Department of Defense, *Department of Defense Law of War Manual* (US Department of Defense, 2023), 1035.

4.2. Distinction

Distinction is a fundamental rule of IHL that aims to protect civilians and civilian objects from the effects of war, separating combatants from non-combatants.[723] It requires parties to a conflict to distinguish between civilians and combatants, as well as between military objectives and civilian objects, whenever they conduct their military operations.[724] Having its roots in the customs of war that upheld a distinction between combatants and non-combatants since ancient times,[725] Distinction was first included in the Lieber Code of 1863 and has been consistently reaffirmed in various treaties as well as customary international law since then.[726] Distinction is one of the "cardinal principle[s]" of the law of armed conflict and also "intransgressible principles of international customary law."[727] Given that distinction is "intransgressible," no justification exists for violations of it.[728] Distinction applies equally as a part of customary law, regardless of the conflict's classification as IAC or NIAC.[729] The general nature of the distinction is described in AP I, which mandates that

> [i]n order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives.[730]

---

[723] David Turns, "Military Objectives," in *Routledge Handbook of the Law of Armed Conflict*, ed. Rain Liivoja and Tim McCormack (Routledge, 2020), 139.

[724] Droege, "Cyber Warfare," 561.

[725] Turns, "Military Objectives," 140.

[726] Bannelier, "Principle of Distinction," 427.

[727] ICJ, *Nuclear Weapons*, paras 78-79.

[728] Schmitt, *Tallinn Manual,* 422.

[729] ICTY, Tadić Appeal on Jurisdiction, para. 112, 127.

[730] Additional Protocol I, Article 48.

Article 48 of AP I reflects the universally accepted formulation of distinction today.[731] Article 48 serves as a general rule and is operationalized in the subsequent Articles. In this regard, other articles of AP I outline the obligations of States concerning the distinction. Accordingly, civilians and civilian objects are defined in Articles 50 and 52(2) of AP I. It is also stated that the civilian population and individual civilians are afforded protection and cannot be the object of attack;[732] that indiscriminate attacks are prohibited,[733] and attacks must be strictly limited to military objectives that, by their nature, location, purpose, or use, make an effective contribution to military action, and their targeting must also offer a definitive military advantage under the prevailing conditions.[734] Each of these obligations will be examined separately.

4.2.1. Prohibition of Targeting Civilians

IHL prohibits parties to a conflict from targeting civilians and civilian populations, as expressed in AP I that "[t]he civilian population and individual civilians shall enjoy general protection against dangers arising from military operations."[735] This protection applies to both IACs[736] and NIACs,[737] as part of both treaty and customary law.[738] The prohibition against targeting civilians is absolute, and deliberate targeting constitutes a war crime.[739] Additionally, IHL prohibits "acts or threats of violence the primary purpose of which is to spread terror among the civilian population."[740]

---

[731] Turns, "Military Objectives," 139.

[732] Additional Protocol I, Article 51.

[733] Additional Protocol I, Article 51(4).

[734] Additional Protocol I, Article 51(1), (2).

[735] Additional Protocol I, Article 51(1).

[736] Additional Protocol I, Article 51(3).

[737] Additional Protocol II, Article 13(3).

[738] Kubo Mačák, "Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield," *International Review of the Red Cross* 105, no 923 (2023): 970, https://doi.org/10.1017/s1816383123000152.

[739] Emanuela-Chira Gillard, "Protection of Civilians in the Conduct of Hostilities," in *Routledge Handbook of the Law of Armed Conflict*, ed. Rain Liivoja and Tim McCormack (Routledge, 2020), 160.

[740] Additional Protocol I, Article 51(2).

Civilians are defined in AP I as "any person who does not belong to one of the categories of persons referred to in Article 4A (1), (2), (3) and (6) of the Third Convention and in Article 43 of this Protocol."[741] The categories mentioned in the Article are

> members of the regular armed forces, including militia or volunteer corps like the reserves, that are part of the armed forces; members of a militia and other volunteer groups, including resistance movements, that belong to a party to the conflict and meet the conditions of being under responsible command, wearing attire or emblems that allow them to be distinguished from the civilian population, carrying their weapons openly, and, as a group, conducting their operations in accordance with IHL; members of the regular armed forces who have professed allegiance to a government or authority that is not recognized by the opposing party; and members of a *levée en masse*.[742]

Accordingly, Protocol defines civilians negatively: the civilian population consists of persons who are not members of the categories mentioned above.[743] Given that combatants and civilians are defined negatively, both categories are exclusive: a person is either a civilian or a combatant.[744] Civilians are afforded general protection from the dangers of military operations as long as they do not actively or directly engage in hostilities.[745] If civilians actively or directly participate in hostilities, they lose this protection for the duration of their participation in hostilities.[746]

Although "direct participation" is not defined in IHL, the ICRC offers three cumulative criteria for civilians' direct participation in hostilities.[747] The first criterion is the

---

[741] Additional Protocol I, Article 50(1).

[742] Michael N. Schmitt, "International Humanitarian Law and the Conduct of Hostilities," in *The Oxford Guide to International Humanitarian Law*, ed. Ben Saul and Dapo Akande, (Oxford University Press, 2020), 156-157.

[743] ICRC, *Commentary on Additional Protocols,* 610.

[744] Gillard, "Protection of Civilians," 159.

[745] Heather Harrison Dinniss, *Cyber Warfare and the Laws of War* (Cambridge University Press, 2012), 159.

[746] Gillard, "Protection of Civilians," 161.

[747] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law* (ICRC, 2009), 5.

threshold harm, whereby a certain act conducted by a civilian "must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack."[748]

The second criterion is direct causation, meaning that "there must be a direct causal link between a specific act and the harm likely to result either from that act or from a coordinated military operation of which that act constitutes an integral part."[749]

The last criterion is the belligerent nexus, which requires that "an act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another."[750] Accordingly, if an act committed by a civilian meets these three criteria cumulatively, the act in question amounts to direct participation in hostilities, and the protection granted by IHL is suspended until the direct participation continues.

4.2.2. Prohibition of Targeting Civilian Objects

In addition to prohibiting attacks targeting civilians, IHL also prohibits attacks targeting civilian objects, as stated in Article 52(1) of AP I "[c]ivilian objects shall not be the object of attack or of reprisals,"[751] and "[a]ttacks shall be limited strictly to military objectives."[752] Accordingly, attacks must be limited to military objectives, and it is prohibited for the parties to a conflict to target civilian objects as long as they retain their civilian character and are not turned into military objectives.[753] The

[748] Melzer, *Interpretive Guidance,* 47.

[749] Melzer, *Interpretive Guidance,* 51.

[750] Melzer, *Interpretive Guidance,* 58.

[751] Additional Protocol I, Article 52(1).

[752] Additional Protocol I, Article 52(2).

[753] Corn et. al., *The Law of Armed Conflict*, 176.

prohibition to target civilian objects stated in AP I reflects customary international law applicable in both IACs and NIACs.[754]

Just as with the civilian population, the Protocol defines civilian objects negatively in relation to military objectives by stating, "[c]ivilian objects are all objects which are not military objectives as defined in paragraph 2."[755] In paragraph 2, the Protocol defines military objectives as

> [i]n so far as objects are concerned, 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.[756]

Accordingly, to qualify as a military object and become targetable, the object in question must meet two cumulative criteria: First, it must make an effective contribution to military action by its nature, location, purpose, or use; and second, the object's destruction, capture, or neutralization must offer a definite military advantage in the circumstances prevailing at the time.[757] By imposing two cumulative criteria, the Protocol aims to prevent conflicting parties from regarding every object as a military objective by considering indirect contributions and potential future benefits.[758]

Regarding the first criterion, the meaning of the terms should be explained. Accordingly, the criterion of "nature" includes all objects directly utilized by armed forces in relation to the parties to conflict, such as weapons, equipment, fortifications, etc.[759] The criterion of "location" refers to objects "which is of special importance for

---

[754] Schmitt, "Conduct of Hostilities," 161.

[755] Additional Protocol I, Article 52(1).

[756] Additional Protocol I, Article 52(2).

[757] ICRC, *Commentary on Additional Protocols,* 635.

[758] Sassòli, *International Humanitarian Law*, 379.

[759] ICRC, *Commentary on Additional Protocols,* 636.

military operations in view of its location."[760] The criteria of "purpose" and "use" are interlinked, given that they are essentially the same but temporally different: while "use" refers to an object's current utilization, the "purpose" refers to the future intended utilization of the object for military aims.[761] On the other hand, effective contribution means that the object in question is useful for the enemy's conducting of military action, regardless of how small or large it is.[762]

The US position in this regard extends the interpretation of effective contribution to include "war-fighting," "war-supporting," and "war-sustaining."[763] As a result, this would enable the US to target "economic objects associated with military operations or with war-supporting or war-sustaining industries."[764] This approach should be highlighted, as it raises controversy.[765] The American approach is criticized for extending the notion too broadly, which undermines the requirement for a close nexus between the target and military operations.[766]

The second cumulative criterion is that an object's total or partial destruction, capture, or neutralization must provide a definite military advantage under the prevailing circumstances. The definite military advantage offered by the attack must be concrete and perceptible[767] and can be achieved at either the tactical or operational level.[768] Additionally, the military advantage must be military in nature and derived from the attack as a whole, rather than from isolated or specific parts of the attack.[769] Reflecting

[760] ICRC, *Commentary on Additional Protocols,* 636.

[761] Turns, "Military Objectives," 150.

[762] Schmitt, "Conduct of Hostilities," 164.

[763] United States Department of Defense, *Law of War Manual*, 222.

[764] United States Department of Defense, *Law of War Manual*, 227.

[765] Schmitt, "Conduct of Hostilities," 163.

[766] Dinniss, *Laws of War*, 189.

[767] Bothe, Partsch and Solf, *New Rules for Victims,* 367.

[768] Schmitt, "Conduct of Hostilities," 164.

[769] Dinniss, *Laws of War*, 191.

the dynamic nature of armed conflicts, this criterion also states that military advantage must be assessed based on the circumstances prevailing at the time, which means that relevant assessment depends on the facts on the ground at that time and is therefore contextual.[770] In summary, the object in question must meet these two criteria to be considered a military object and a lawful target. If an object does not meet these criteria cumulatively, it is classified as a civilian object, which is protected under IHL.

Lastly, Article 51 also creates a presumption as it states that "[i]n case of doubt whether an object which is normally dedicated to civilian purposes … is being used to make an effective contribution to military action, it shall be presumed not to be so used."[771] Accordingly, if there is a suspicion regarding whether an object that normally has no significant military function, such as an apartment, school, or house of worship, is used for military purposes, it shouldn't be regarded as such and should be treated as a civilian object.

4.2.3. Prohibition to Conduct Indiscriminate Attacks

Another limitation imposed by IHL on parties to a conflict for the protection of civilians is the prohibition to conduct indiscriminate attacks, which is a rule of customary law applicable in both IACs and NIACs.[772] This prohibition is outlined in Article 51(4) of AP I:

> Indiscriminate attacks are prohibited. Indiscriminate attacks are:
> *(a)* those which are not directed at a specific military objective;
> *(b)* those which employ a method or means of combat which cannot be directed at a specific military objective; or
> *(c)* those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol;
> and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.[773]

[770] Turns, "Military Objectives," 149.

[771] Additional Protocol I, Article 51(3).

[772] Jean-Marie Henckaerts and Louise Doswald-Beck, *Customary International Humanitarian Law,* vol. 1, (Cambridge University Press, 2005), 40.

[773] Additional Protocol I, Article 51(4).

Accordingly, the Protocol first prohibits attacks that do not target a specific military objective. Such attacks may be those that intend to target military objectives but where no effort has been made by the attacker to direct the attack at a particular military objective, or attacks that target separate military objectives within a single targeting area.[774] Second, the Protocol prohibits means or methods of warfare that cannot be directed at a specific objective, which focuses on weapons used to conduct attacks.[775] While the term "means" refers to weapons used in an attack, the term "methods" refers to how these weapons are used in an attack.[776] This aspect prohibits blind weapons that can not distinguish between legitimate military objectives and protected civilian targets.[777] Third, Protocol emphasizes effects and bans means and methods that cannot be limited according to the Protocol. This means a weapon can be precise enough to be lawful but may be prohibited if its effects are uncontrollable.[778] The attack's effects must be limited in both space and time to comply with the prohibition.[779]

The main difference between indiscriminate attacks and direct attacks against civilians, both forbidden by IHL, is the attacker's intent: while civilian casualties are not a concern for the attacker in a discriminate attack, the attacker aims to target civilians directly in a direct attack.[780] Whether the prohibition to conduct indiscriminate attacks is violated must be determined on a case-by-case basis unless the weapon or weapons used in the attack are specifically prohibited, as in the case of landmines.[781] An attack that would be lawful might become indiscriminate in a

[774] Gillard, "Protection of Civilians," 163.

[775] Schmitt, "Conduct of Hostilities," 155.

[776] ICRC, *Commentary on Additional Protocols,* 621.

[777] Bothe, Partsch and Solf., *New Rules for Victims,* 346.

[778] Schmitt, "Conduct of Hostilities," 156.

[779] Gillard, "Protection of Civilians," 163.

[780] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict*, 3rd ed. (Cambridge University Press, 2015), 147.

[781] Gillard, "Protection of Civilians," 163.

different context.[782] The assessment also evolves with technological advancements.[783] An attack doesn't need to succeed to be considered a violation of the prohibition,[784] and violating this prohibition constitutes a war crime.[785]

4.2.4. Special Protection Granted by IHL

In addition to the general protection granted to civilians and civilian objects by IHL through the principle of distinction discussed above, IHL also offers special protection to certain categories of persons and objects because they are considered particularly vulnerable.[786] For the purposes of this study, only three categories of objects that receive special protection under IHL will be examined: medical units, objects indispensable to the survival of the civilian population and works or installations containing dangerous forces.

4.2.4.1. Medical Units

Medical units are defined in AP I as

> establishments and other units, whether military or civilian, organized for medical purposes, namely the search for, collection, transportation, diagnosis or treatment — including first-aid treatment — of the wounded, sick and shipwrecked, or for the prevention of disease.[787]

Special protection granted to medical units is included both in the treaty law and customary law, and it is one of the oldest rules of IHL.[788] The special protection for

[782] Bothe, Partsch and Solf, *New Rules for Victims,* 347.

[783] Schmitt, "Conduct of Hostilities," 156.

[784] Schmitt, *Tallinn Manual,* 469.

[785] Gillard, "Protection of Civilians," 162.

[786] Robin Geiß and Christophe Paulussen "Specifically Protected Persons and Objects," in *The Oxford Guide to International Humanitarian Law*, ed. Ben Saul and Dapo Akande, (Oxford University Press, 2020), 175.

[787] Additional Protocol I, Article 8(e).

[788] ICRC, *Commentary on GC I*, 630.

medical units is outlined in GC I as "[f]ixed establishments and mobile medical units of the Medical Service may in no circumstances be attacked, but shall at all times be respected and protected by the Parties to the conflict."[789] Special protection for military medical units, originally outlined by the GC I, was expanded in AP I to also include civilian medical units.[790] It is also incorporated into AP II.[791] Additionally, it is a part of customary international law that applies in both IACs and NIACs.[792] Accordingly, it is prohibited to attack or harm medical units, including obstructing their functions or purpose.[793] This obligation must be followed as long as the medical unit is dedicated solely to medical purposes, regardless of whether patients are being treated there.[794]

To receive special protection, a medical unit must either "belong to one of the Parties to the conflict," or be "recognized and authorized by the competent authority of one of the Parties to the conflict."[795] In this regard, the Parties to the conflict must exercise a certain level of control over the medical units in question to ensure that these units are used exclusively for medical purposes.[796] Additionally, the special protection also covers medical units assigned by a neutral State, a third State that does not participate in hostilities, or an international humanitarian organization, according to Article 12(2)(c) of the AP I.[797]

[789] First Geneva Convention, Article 19.

[790] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 92.

[791] Additional Protocol II, Article 11.

[792] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 92.

[793] ICRC, *Commentary on Additional Protocols,* 166.

[794] ICRC, *Commentary on Additional Protocols,* 167.

[795] Additional Protocol I, Article 12(2).

[796] ICRC, *Commentary on Additional Protocols,* 167.

[797] ICRC, *Commentary on Additional Protocols,* 169.

The special protection terminates when a medical unit is "used to commit, outside their humanitarian function, acts harmful to the enemy."[798] Conditions outlined in the article are cumulative.[799] Given that the term "acts harmful to enemy" is not defined in the Protocol, ICRC defines such act as "Acts the purpose or effect of which is to harm the adverse Party, by facilitating or impeding military operations,"[800] and such acts are exemplified as " firing at the enemy for reasons other than individual self-defence, installing a firing position in a medical post, the use of a hospital as a shelter for able-bodied combatants, as an arms or ammunition dump."[801] Accordingly, when a medical unit is used to commit acts harmful to the enemy outside of its humanitarian function, it loses its special protection. Additionally, the protection ends "only after a warning has been given setting, whenever appropriate, a reasonable time-limit, and after such a warning has remained unheeded."[802]

4.2.4.2. Objects Indispensable to the Survival of the Civilian Population

Article 54(2) of AP I grants special protection to objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas, crops, livestock, drinking water, and irrigation systems, and prohibits to "attack, destroy, remove or render useless" such objects "for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party."[803] In this regard, the Article establishes broader protection for indispensable objects, as it prohibits not only attacks against them but also their destruction, removal, or rendering them useless.[804] The Protocol also prohibits reprisals against such objects.[805] This

[798] Additional Protocol I, Article 13(1).

[799] ICRC, *Commentary on GC I*, 652

[800] ICRC, *Commentary on Additional Protocols,* 175.

[801] ICRC, *Commentary on GC I*, 653.

[802] Additional Protocol I, Article 13(1).

[803] Additional Protocol I, Article 54(2).

[804] Sassòli, *International Humanitarian Law*, 404.

[805] Additional Protocol I, Article 54(4).

prohibition is also included in AP II,[806] and it is part of customary international law that applies to both IACs and NIACs.[807] The list of objects mentioned in Article 54(2) is not exhaustive.[808] The special protection applies regardless of whether the object is privately or publicly owned.[809]

There are two exceptions to the special protection granted to indispensable objects: Firstly, such objects are outside the scope of the special protection if they are only used for the sustenance of the military forces, or if they are used in direct support of the military action.[810] Even when these objects constitute a military objective as mentioned, they cannot be attacked if it is expected that the attack would cause starvation or displacement of the civilian population.[811] It is also stated that a party defending its national territory against an invasion might derogate from the special protection if such action is necessary due to imperative military necessity.[812] Such exception is only valid for the defending party of the invasion within its own territory.[813]

4.2.4.3. Works and Installations Containing Dangerous Forces

The last category to be examined in this study is works and installations containing dangerous forces. Article 56 of AP I outlines the special protection granted to such works and installations:

> Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the

[806] Additional Protocol II, Article 14.

[807] Henckaerts and Doswald-Beck., *Customary International Humanitarian Law,* 189.

[808] Henckaerts and Doswald-Beck., *Customary International Humanitarian Law,* 193.

[809] Sassòli, *International Humanitarian Law*, 404.

[810] Additional Protocol I, Article 54(3).

[811] Sassòli, *International Humanitarian Law*, 404.

[812] Additional Protocol I, Article 54(5).

[813] Sassòli, *International Humanitarian Law*, 404.

> release of dangerous forces and consequent severe losses among the civilian population.[814]

Not only is it prohibited to attack such installations, but it is also prohibited to attack military objectives located at or near such installations if such an attack would cause the release of dangerous forces and severe civilian losses consequently. The special protection is also included in AP II[815] and is part of customary international law applicable in both IACs and NIACs.[816] In addition to targeting, such work and installations cannot be made objects of reprisals.[817]

These installations are granted special protection because releasing dangerous forces from them could cause catastrophic effects for the civilian population and objects.[818] Although the Protocol limits the special protection only to dams, dykes, and nuclear electrical generating stations, and no consensus was reached to include other works and installations during the drafting of AP I, the term should also be understood to include other installations such as chemical plants or oil refineries.[819]

The special protection granted to works and installations containing dangerous forces terminates only if such installations provide "regular, significant and direct support of military operations" and the attack aimed at them "is the only feasible way to terminate such support."[820] Therefore, Article 56(2) sets a higher standard regarding contribution to military operations, and thus, the special protection terminates only in extreme circumstances.[821] Even though the special protection ends and works and installations containing dangerous forces can become targets as military objectives, the attacker

[814] Additional Protocol I, Article 56(1).

[815] Additional Protocol II, Article 15.

[816] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 139.

[817] Additional Protocol I, Article 56(4).

[818] Sassòli, *International Humanitarian Law*, 405.

[819] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 141-142.

[820] Additional Protocol I, Article 56(2).

[821] Dinstein, *Conduct of Hostilities*, 228.

must take all practical precautions to prevent the release of dangerous forces.[822] In this regard, it is still prohibited to attack a work or installation that has lost its special protection if the attack could cause serious civilian casualties due to the release of dangerous forces.[823]

4.2.5. Distinction in Cyberspace

The applicability of distinction in cyberspace is acknowledged by States in the GGE processes,[824] although with an emphasis on the need for further research into how and when distinction applies.[825] Along with the GGE processes, individual State positions on the subject also support the view that the distinction applies in cyberspace. For example, the African Union "underscores the importance of the principle of distinction, which prohibits attacks that are directed at civilians or civilian objects, including ICTs, whether such attacks are undertaken using kinetic or cyber means."[826] Similarly, the EU observes that "[t]he principle of distinction applies irrespective of whether the cyber attack is exercised in an offensive or a defensive context."[827] Likewise, the ICRC states that "direct attacks against civilians and civilian objects are prohibited, including when using cyber means or methods of warfare."[828] Tallinn Manual also remarks that "[t]he principle of distinction applies to cyber attacks."[829] It should also be noted that distinction is applicable by virtue of its position as part of customary international law.

Accordingly, distinction applies in cyberspace and cyber operations when conduct attributable to a party also constitutes an attack under Article 49(1) of AP I. Such

[822] Additional Protocol I, Article 56(3).

[823] ICRC, *Commentary on Additional Protocols,* 669.

[824] UN GGE, *2015 Report*, 13.

[825] UN GGE, *2021 Report*, 18.

[826] African Union Peace and Security Council, *Common African Position*, 8.

[827] Council of the European Union, *International Law in Cyberspace*, 7.

[828] ICRC, *Position Paper,* 5.

[829] Schmitt, *Tallinn Manual,* 420.

conduct is subject to limitations arising from distinction, which include the prohibition to target civilian populations and objects, as well as the prohibition to conduct indiscriminate attacks. Cyber operations must also respect objects that IHL grants special protection, which is a broader obligation than just prohibiting attacks.[830] Likewise, contrary to claims that cyber weapons are inherently indiscriminate, experts agree that cyber weapons can be designed to avoid causing indiscriminate effects.[831] In this regard, States are also obligated to assess whether the newly developed cyber weapons they acquire or modify are prohibited by international law, which applies not only to the new acquisitions but also to updates and modifications.[832]

Although it is certain that rules emanating from distinction apply to cyber operations that amount to an attack, the issue of whether the principle applies to cyber operations that do not amount to an attack remains controversial. The Tallinn Manual asserts that the distinction is relevant only to cyber operations that constitute an attack;[833] however, this interpretation is endorsed solely by Israel, and State practice remains insufficient.[834] On the other hand, ICRC states that "most rules stemming from the principles of distinction, proportionality and precautions – which provide general protection for civilians and civilian objects – apply only to military operations that qualify as 'attacks' as defined in IHL."[835] There are also proponents who argue that distinction extends to military operations that fall below the attack threshold, as outlined in Articles 48, 51, and 57, which state that civilians should be protected from the dangers of military operations and belligerents must only target military objectives.[836] Although the text of these articles indicates that military operations are

[830] Sassòli, *International Humanitarian Law*, 482.

[831] Bannelier, "Principle of Distinction," 449-450.

[832] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 330-331.

[833] Schmitt, *Tallinn Manual,* 423.

[834] Bannelier, "Principle of Distinction," 445.

[835] ICRC, *Position Paper,* 7.

[836] Bannelier, "Principle of Distinction," 444-448; Dinniss, *Laws of War*, 196-202.

not immune from the distinction, this issue has yet to be resolved in the cyber context.[837]

Apart from this issue, cyberspace's unique characteristics pose other challenges for applying the principle of distinction, namely how dual-use objects can be protected by IHL and whether data constitutes an object. These two issues will be examined separately below.

4.2.5.1. Question of Dual-Use Objects

Cyberspace presents significant challenges to the applicability of the principle of distinction. The first challenge arises from the fact that most of the cyber infrastructure is dual-use; that is, it serves both civilian and military purposes. This challenge arises from the interconnectedness of military and civilian systems and networks. Many military networks depend on civilian infrastructure such as fiber optic undersea cables or satellites, many civilian networks, incorporate technologies that were originally developed as military technologies, most notable one being the GPS technology.[838] For example, it is estimated that 98% of the US Government's communications go through civilian networks.[839] In this regard, clearly distinguishing between dual-use objects has proven challenging for States and experts, and the predominantly civilian nature of cyberspace makes the situation even more complicated.[840] More specifically, it is almost impossible to separate dual-use objects from the few that are solely dedicated to military use.[841] The level of interconnectedness between military and civilian networks in cyberspace naturally

[837] Sassòli, *International Humanitarian Law*, 582.

[838] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 320.

[839] Benjamin Weitz, "Updating the Law of Targeting for an Era of Cyberwarfare," *University of Pennysylvania Journal of International Law* 40, no. 3 (2019): 762, https://scholarship.law.upenn.edu/jil/vol40/iss3/5/.

[840] Bannelier, "Principle of Distinction," 450-452.

[841] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 320.

occurs because any part of a cyber infrastructure can be utilized for both civilian and military purposes at the same time or interchangeably.[842]

This level of integration between military and civilian networks has the potential to turn every civilian part of cyberspace into a military objective, which in turn would make the principle of distinction meaningless in cyberspace.[843]

As mentioned earlier, the principle of distinction depends on distinguishing between civilians and combatants, as well as between civilian and military objects. The Protocol does not provide a clear definition of what constitutes a civilian object; instead, it defines civilian objects in contrast to military objectives. For something to qualify as a legitimate military target, it must contribute effectively to military action based on its nature, location, use, or purpose, and its total or partial destruction must provide a definite military advantage in the given context. Therefore, in the cyber context, any cyber equipment that has an intrinsically military character, is utilized by armed forces, or is intended for military purposes falls under this classification.[844] In this context, it is generally accepted that an object can qualify as a military objective when the object is used for military purposes, even if it also has civilian uses at the same time.[845]

In line with this understanding, France notes that "ICT infrastructure or a system used for both civilian and military purposes may, after detailed analysis on a case-by-case basis, be deemed a military objective."[846] Similarly, Tallinn Manual states that "an object used for both civilian and military purposes-including computers, computer

[842] Robin Geiß and Henning Lahmann, "Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space," *Israel Law Review* 45, no 3 (2012): 388, https://doi.org/10.1017/s0021223712000179.

[843] Droege, "Cyber Warfare," 565.

[844] Heather A Harrison Dinniss, "The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives", *Israel Law Review* 48, no. 1 (2015): 47, https://doi.org/10.1017/s0021223714000272.

[845] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 321.

[846] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 14.

networks, and cyber infrastructure is a military objective."[847] Accordingly, a dual-use infrastructure used for military purposes is considered a military objective that can be targeted as long as it meets the definition in Article 52(2). Even though dual-use cyber infrastructures can constitute military objectives, this does not give States the freedom to attack all dual-use objects. Austria illustrates this point by noting that

> the fact that a dual-use object is a military objective does not automatically render every attack directed against it lawful. Stopping or impairing the civilian use of an object in violation of core IHL principles renders the attack unlawful despite the object's classification as a military objective.[848]

In light of these, this study argues that the fact that an infrastructure is used for both military and civilian purposes does not give the attacker a blank check to target the entire network. Instead, attackers are legally required to direct their operations to only the specific and separable military components. Treating the entirety of the network as military objective would undermine the distinction and would render it ineffective in cyberspace.

In this context, first of all, the attacker must individually analyze and identify parts of the dual-use network in question, such as computers, nodes, or routers that constitute a military objective.[849] States cannot target clearly distinct and separate military objectives that are part of a cyber network primarily used for civilian purposes in their entirety if the attack would cause damage to protected persons or objects.[850] Such an attack would be unlawful, given that military parts of the networks could have been targeted separately.[851]

---

[847] Schmitt, *Tallinn Manual,* 445.

[848] Federal Ministry for European and International Affairs of Republic of Austria, *Position Paper of the Republic of Austria: Cyber Activities and International Law* (Federal Ministry for European and International Affairs of Republic of Austria, 2024), 19, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf

[849] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 321.

[850] Schmitt, *Tallinn Manual,* 469.

[851] Schmitt, *Tallinn Manual,* 470.

Secondly, considering the flexibility of cyberspace that allows data traffic to be transferred immediately after an attack, the assessment of whether destroying or neutralizing the dual-use object would offer a definite military advantage must be examined more carefully.[852] Thirdly, if there is doubt that a dual-use object, which is normally used for civilian purposes, is being used for military purposes, it should be presumed not to be used for military purposes.[853] Lastly, even if it is permissible to target a dual-use object under the principle of distinction, the attack must also comply with the principles of proportionality and precautions, which will be discussed later in this chapter.

4.2.5.2. Question of Data

Another challenge arising from cyberspace for the principle of distinction is whether data qualifies as an object under IHL. This debate is significant because data is an integral part of cyberspace and plays a vital role in civilians' everyday lives: information such as social security data, tax records, bank accounts, and election records is essential for the proper functioning of society.[854] Cyber operations can affect data in various ways: they can alter, corrupt, manipulate, rewrite, or delete the data they target using viruses, worms, and Trojan horses.[855] In this context, the answer to this question will influence how data is protected during times of armed conflict: If data does not qualify as an object, then it will fall outside the general protection provided by the IHL rules and principles.[856]

Before discussing the controversial aspects of the question, a few points should be clarified. First, the question to be discussed is whether cyber operations that target data itself are subject to IHL rules: If cyber operations target data in a way that causes injury or death to persons, or physical damage to objects, the cyber operation in question

[852] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 321.

[853] Additional Protocol I, Article 52(3).

[854] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 317.

[855] Robin Geiß and Henning Lahmann, "Protection of Data in Armed Conflict," *International Law Studies* 97, no. 1 (2021): 563.

[856] Schmitt, "Wired Warfare 3.0," 340.

qualifies as an attack and becomes subject to IHL, regardless of whether data constitutes an object or not.[857] Secondly, data is protected against cyber operations regardless of whether it is an object or not, if it is part of an object that IHL grants special protection; for example, medical data of a medical unit is protected whether or not the data constitutes an object under IHL.[858]

Apart from these two situations, the question is not easy to tackle given that State opinion and practice are scarce, and doctrine is fragmented.[859] It can be said that there are two strands of thought on the issue among the experts. The first group argues that data does not constitute an object because it does not fit the definition provided in Article 52(2) of AP I, as the definition applies only to tangible, visible, and material objects described in the 1987 ICRC Commentary.[860] This view is accepted by the majority of Tallinn Manual experts, which contend that data does not constitute an object since "data is intangible and therefore neither falls within the 'ordinary meaning' of the term object, nor comports with the explanation of it offered in the ICRC Additional Protocols 1987 Commentary."[861] This argument is also endorsed by Israel, which states that "[o]bjects for the purposes of LOAC have always been understood to be tangible things and this understanding is not domain-specific. It is therefore our position that … only tangible things can constitute objects,"[862] and Denmark that notes that "digital data cannot generally in and of itself be considered an object under IHL."[863]

[857] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 317.

[858] Geiß and Lahmann, "Protection of Data," 564.

[859] Bannelier, "Principle of Distinction," 443.

[860] Geiß and Lahmann, "Protection of Data," 565.

[861] Schmitt, *Tallinn Manual,* 437.

[862] Schöndorf, "Israel's Perspective," 401.

[863] Kjelgaard and Melgaard, "Denmark's Position Paper," 455.

On the other hand, the second group argues that data constitutes an object under IHL, given that not doing so would go against the purpose of Article 48 of AP I.[864] The two different ways support this argument. One argument is that the concept of "object" as defined in AP I should be adjusted to current conditions in an evolutionary manner to include data within its scope, aligning with the goals and purpose of IHL.[865] The second argument distinguishes between "operational-level data," which provides networks with their functionality, and "content-level" data.[866] Focusing on the latter type of data, it is argued that data can constitute a military objective, and therefore an object, if it fits the definition in AP I, regardless of its intangibility.[867] Several States endorse the view that data constitutes an object under IHL. For instance, France observes that "[g]iven the current State of digital dependence, content data (such as civilian, bank or medical data, etc.) are protected under the principle of distinction."[868] Similarly, Austria is of the view that

> civilian data are to be considered an "object" for the rules governing the conduct of hostilities and are protected under the principle of distinction. Similarly, ICT equipment and services of medical facilities and humanitarian relief organizations must be respected and protected. A cyber activity that deletes or manipulates data in a manner that renders useless objects indispensable to the survival of the civilian population, such as drinking water installations, is prohibited.[869]

This argument also reflects ICRC's position, which states that "[e]xcluding essential civilian data from the protection afforded by IHL to civilian objects would result in an important protection gap.[870]

---

[864] Schmitt, *Tallinn Manual,* 437.

[865] Kubo Mačák, "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law," *Israel Law Review* 48, no 1 (2015): 80, https://doi.org/10.1017/s0021223714000260.

[866] Dinniss, "Cyber Military Objectives," 41.

[867] Dinniss, "Cyber Military Objectives," 54.

[868] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 14.

[869] Federal Ministry for European and International Affairs of Republic of Austria, *Position Paper of the Republic of Austria*, 18.

[870] ICRC, *Position Paper,* 8.

While the issue remains disputed and no consensus has been reached, it is more appropriate to categorize data as an object under IHL, since civilian life—the primary focus of IHL protections—becomes increasingly dependent on data day by day. As critics of the first position point out, ICRC's 1987 Commentary introduced the criterion of tangibility to distinguish objects from abstract concepts like "civilian morale"[871] and did not intend to differentiate between tangible and intangible objects.[872] A strictly tangible interpretation of objects has become increasingly outdated in a digitalized world where civilian life depends on data integrity. Excluding essential data, such as medical or financial records, from the protection of IHL would cause a serious protection gap, which would undermine humanitarian aims and purposes of the Geneva Conventions and their Additional Protocols.

4.2.6. Distinction and Critical Infrastructures

Cyber operations targeting CIs would likely qualify as an attack because of the effects they cause and would be subject to limitations imposed by IHL. Accordingly, CIs are protected by distinction and relevant IHL rules due to their importance for the healthy functioning of civilian life.

Their purpose and importance qualify them as civilian objects as defined in the AP I. Some of the CIs, such as health facilities, nuclear facilities, and drinking water systems, are also granted special protection by the IHL, which provides higher protection for these objects. Accordingly, they are protected from both attacks specifically aimed at them and from indiscriminate attacks carried out by any of the parties. This protection also covers their data, which enables their functionality. Even if a CI is used for both military and civilian purposes and qualifies as a legitimate military objective, it is not permitted to attack its entirety. Belligerents must identify and target only the parts used for military purposes, while also respecting the principles of proportionality and precaution. Conducting attacks that target CIs in a manner that

[871] Geiß and Lahmann, "Protection of Data," 566.

[872] Gisel, Rodenhäuser and Dörmann, "Twenty Years on," 318.

violates the distinction and relevant rules of IHL not only entails State responsibility but also constitutes a war crime that may trigger personal criminal liability.

4.3. Proportionality

An attack targeting a legitimate military objective may be prohibited if it is expected to cause excessive harm in comparison to the concrete and direct military advantage anticipated from the attack. This rule is known as proportionality, which is articulated in Article 51(5)(b) of Additional Protocol I, which states that

> an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.[873]

In addition, Article 57(2)(iii) also forbids parties to a conflict to "refrain from deciding to launch any attack … which would be excessive in relation to the concrete and direct military advantage anticipated."[874] Apart from its inclusion in AP I, proportionality is also part of customary law applicable in both IACs and NIACs.[875] The ICJ also recognizes the its applicability.[876] Proportionality binds everyone involved in an attack, including planners, capable commanders, and personnel carrying out the attack.[877] Violating proportionality is considered a serious breach of the Protocol,[878] and a war crime in the context of IACs.[879]

[873] Additional Protocol I, Article 51(5)(b).

[874] Additional Protocol I, Article 57(2)(iii).

[875] Henckaerts and Doswald-Beck., *Customary International Humanitarian Law,* 46.

[876] ICJ, *Nuclear Weapons*, para 30.

[877] Schmitt, "Conduct of Hostilities," 155.

[878] Additional Protocol I, Article 85.

[879] Sassòli, *International Humanitarian Law*, 389.

Proportionality links collateral damage to military advantage.[880] Contrary to arguments, proportionality does not justify excessive harm to civilians and civilian objects, which would violate core rules of IHL.[881] It demands a balance between the harm inflicted on civilians by the attack and the military advantage expected from it.[882]

Accordingly, planners, decision makers, and executors of an attack must balance the collateral damage and military advantage by assessing the impact on civilians and determining whether these effects are excessive compared to the expected military advantage.[883] In this context, a proportionality assessment must be conducted during the attack's planning, and planners should use all reasonably available information at the time of the planning.[884] Decisions must be made in good faith and with due diligence.[885] In the words of ICTY, while doing the proportionality assessment

> it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack.[886]

There are several factors to consider in proportionality assessments, such as the location of civilians, weapon accuracy, the nature of military objectives, and the technical skill of combatants.[887] Knock-on effects should also be considered in the

[880] Schmitt, "Conduct of Hostilities," 154.

[881] ICRC, *Commentary on Additional Protocols,* 626.

[882] Dinstein, *Conduct of Hostilities*, 154.

[883] Bothe, Partsch and Solf, *New Rules for Victims,* 351.

[884] Bothe, Partsch and Solf, *New Rules for Victims,* 351.

[885] ICRC, *Commentary on Additional Protocols,* 683.

[886] International Criminal Tribunal for the Former Yugoslavia (ICTY), *The Prosecutor v. Stanislav Galic*, Case No. IT-98-29-T, Trial Judgement, December 5, 2003, para 58, https://www.icty.org/x/cases/galic/tjug/en/

[887] ICRC, *Commentary on Additional Protocols,* 684.

proportionality assessment because the scope of the provision is broad enough to cover attacks likely to cause excessive harm to civilians.[888]

In addition, the cumulative effects of the repetitive attacks should also be included in the assessment.[889] On the other hand, although the terms "concrete and direct" were not defined in the Protocol, the perceivable military advantage should be substantial and close, and should not be speculative; several States expressed that the military advantage should be assessed in terms of the entire attack.[890] In this regard, the term excludes vague, hypothetical, or long-term military advantages.[891] Accordingly, an excessive attack prohibited by the principle of proportionality occurs "when there is a significant imbalance between the military advantage anticipated, on the one hand, and the expected collateral damage to civilians and civilian objects, on the other."[892]

4.3.1. Proportionality in Cyberspace

States acknowledged the applicability of proportionality in cyberspace in GGE processes.[893] In addition, its applicability is clearly reflected in the national positions of States. For instance, the African Union emphasizes "the importance of the principle of proportionality, which prohibits attacks that are expected to cause incidental civilian harm that would be excessive to what is necessary to achieve a definite military advantage."[894]

Similarly, Czechia observes that

[888] Dinniss, *Laws of War*, 139.
[889] Sassòli, *International Humanitarian Law*, 390.

[890] Heather A. Harrison Dinniss, "The Regulation of Cyber Warfare Under Jus in Bello," in *Cyber Warfare: A Multidisciplinary Analysis*, ed. James A.Green (Routledge, Taylor & Francis Group, 2016), 138.

[891] Sassòli, *International Humanitarian Law*, 385.

[892] Schmitt, "Conduct of Hostilities," 153.

[893] UN GGE, *2015 Report*, 13.

[894] African Union Peace and Security Council, *Common African Position*, 8.

> [c]yber operations that may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated, are prohibited.[895]

Likewise, the Tallinn Manual states that such cyber attacks are prohibited based on the proportionality.[896]

Proportionality is vital in cyberspace because of the interconnectedness of networks and the military-civilian nature of cyber infrastructure. Due to the characteristics of cyberspace, a proportionality assessment is almost always necessary before conducting a cyber operation.[897]

Cyber operations that qualify as attacks are subject to proportionality assessments, regardless of whether the cyber-attack is carried out alongside traditional means of warfare or independently. Accordingly, not only cyber operations that cause death or injury to persons or damage to civilian objects but also those that result in the loss of functionality of civilian infrastructure are subject to proportionality assessment.[898]

A cyber operation's all reasonably foreseeable direct and indirect effects must be included in the proportionality assessment.[899] Additionally, a cyber operation can cause collateral damage by itself or during transit, and both forms are subject to proportionality.[900] How a cyber operation's proportionality assessment is well demonstrated in Austria's position:

---

[895] Ministry of Foreign Affairs of the Czech Republic, *Position Paper on the Application of International Law in Cyberspace* (Ministry of Foreign Affairs of Czech Republic, 2024), 12, https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf

[896] Schmitt, *Tallinn Manual,* 470.

[897] Peter Pascucci, "Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution," *Minnesota Journal of International Law.* 26 no. 2 (2017): 446, https://scholarship.law.umn.edu/mjil/257.

[898] Droege, "Cyber Warfare," 572.

[899] Schmitt, *Tallinn Manual,* 472.

[900] Schmitt, *Tallinn Manual,* 471.

> When assessing incidental civilian harm, possible non-kinetic effects of an attack, such as the temporary deprivation of functionality of an ICT system, and possible indirect effects, need to be considered. Unexpected or unforeseeable harm to civilians or civilian objects is not to be considered in this assessment.[901]

The dual-use nature of cyberspace allows cyber operations to have a greater impact on civilian infrastructure and makes distinguishing between military and civilian objects more difficult.[902] At the same time, the interconnectedness of cyberspace complicates determining the scope and effects caused by cyber operations.[903] In this regard, greater care must be taken in the proportionality assessment in cyber operations due to the unique characteristics of cyberspace and infrastructure. The specific cyber-attack must be evaluated in its entirety, utilizing all reasonable available knowledge; planners and commanders should consult specialists, if necessary, given that they are obliged to act with due diligence and in good faith.[904] To this end, military commanders should be expected to exercise more due diligence by consulting technical experts to predict how a cyber operation might impact civilian CIs, so that benefit anticipated would not be disproportionate to damage.

4.3.2. Proportionality and Critical Infrastructures

Proportionality is crucial for protecting CIs because of the high degree of dual-use infrastructures and interconnectedness in cyberspace. Not only would a cyber operation targeting a CI cause more harm to civilians than traditional attacks, but it could also spread to more networks than the attackers intended. In this context, even a CI becomes a legitimate military objective under IHL, this alone does not mean that the CI in question can be targeted, as it would still be prohibited to target it if the cyber

---

[901] Federal Ministry for European and International Affairs of Republic of Austria, *Position Paper of the Republic of Austria*, 19.

[902] Hensey A Fenton III, "Proportionality and its Applicability in the Realm of Cyber-Attacks," *Duke Journal of Comparative & International Law* 29, no. 2 (2018): 350, https://scholarship.law.duke.edu/djcil/vol29/iss2/6/.

[903] Fenton, "Proportionality and its Applicability," 351.

[904] Dinniss, *Laws of War*, 207.

operation conducted will or is expected to cause excessive civilian harm compared to the concrete and direct military advantage anticipated.

In this context, a cyber operation targeting a dual-use CI would be prohibited if the potential civilian harm outweighs the military advantage to be gained from the operation. Similarly, a cyber operation that physically harms or impairs the function of a dual-use CI is restricted by proportionality if the harm to civilians exceeds the military advantage. In addition to direct effects, the indirect effects of a cyber operation targeting a CI would also render the operation prohibited by the principle of proportionality. Given the importance of CIs for civilian life, the fact that a CI is targeted also tips the balance in the proportionality assessment.

4.4. Precautions

The last IHL rule to be analyzed in this study is the precautions, which requires parties to a conflict to take precautionary measures to minimize harm to civilian populations, civilians, and civilian objects during military operations.[905] This rule is considered also part of customary international law in both IACs and NIACs.[906] Even if an attack complies with the principles of distinction and proportionality, it must also adhere to the principle of precautions, the violation of which constitutes a grave breach of AP I.[907]

Precautions is codified and operationalized in Articles 57 and 58 of AP I. Article 57(1) establishes a general obligation: "In the conduct of military operations, constant care shall be taken to spare the civilian population, civilians, and civilian objects."[908] As it is evident, the principle of precautions supplements the principle of distinction by imposing duties on both attacking and defending parties to protect civilians and objects

[905] Additional Protocol I, Article 57.

[906] Schmitt, *Tallinn Manual,* 476.

[907] Additional Protocol I, Article 85.

[908] Additional Protocol I, Article 57(1).

from collateral damage.[909] This general obligation outlined in Article 57(1) has a broader scope since it applies to military operations, whereas the subsequent precautionary obligations apply to attacks as defined in Article 49(1) of AP I.[910]

Apart from this general obligation, precautions to be taken by the attacking and defending parties differ as AP I sets stricter precautionary obligations for the attacker than the defender, with the main responsibility lying on the attacker.[911] The attacker and defender are not defined by the *jus ad bellum* but rather by who conducts the violent act in offense or defense.[912] While precautions taken by the attacker are called "active precautions," those taken by the defender are called "passive precautions."[913] In this context, precautionary obligations for both sides will be examined separately.

4.4.1. Active Precautions

Precautionary obligations of the attacking side are outlined in Article 57 of AP I. Firstly, Article 57(2)(a)(i) requires planners and decision-makers of an attack to "do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives."[914] Accordingly, military commanders and decision-makers are required to do everything possible to verify that the target of the attack is lawful under IHL. This obligation helps ensure that attacks only hit military objectives and supports the distinction between civilian and military targets.[915] The term "feasible" serves as a standard of reasonableness that includes precautionary measures that are "practicable or practically possible, taking into account all circumstances prevailing at the time,

[909] Bothe, Partsch and Solf, *New Rules for Victims,* 413.

[910] Jean-François Quéguiner, "Precautions under the Law Governing the Conduct of Hostilities," *International Review of the Red Cross* 88, no. 864 (2006): 797, https://doi.org/10.1017/s1816383107000872.

[911] Sassòli, *International Humanitarian Law*, 401.

[912] Sassòli, *International Humanitarian Law*, 393.

[913] Schmitt, "Conduct of Hostilities," 169.

[914] Additional Protocol I, Article 57(2)(a)(i).

[915] Quéguiner, "Precautions under the Law," 797.

including humanitarian and military considerations."[916] What is feasible can be influenced by the attacker's technical and other capacities,[917] and military and humanitarian considerations.[918]

In all cases, the interpretation of feasibility must be based on common sense and good faith, with the important point being that the necessary verification process is carried out promptly to minimize risks to civilians.[919] To ensure the most effective verification, commanders and decision-makers are required to obtain the best and most reliable intelligence covering various aspects of the target.[920] Additionally, commanders and decision-makers must not hesitate to gather further information if there is any doubt.[921]

Second, Article 57(2)(a)(ii) obliges planners and decision-makers of an attack to implement every "feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects."[922] In this context, commanders and decision-makers are obliged to choose means and methods that are less harmful to civilians and civilian objects. Such precautionary assessments can include evaluations regarding "timing of attacks," "avoiding combat in populated areas," "the selection of means of warfare proportionate to the target," "the use of precision weapons," and "target selection."[923]

[916] Schmitt, "Conduct of Hostilities," 167.

[917] Schmitt, "Conduct of Hostilities," 169.

[918] Sassòli, *International Humanitarian Law*, 395.

[919] ICRC, *Commentary on Additional Protocols,* 682.

[920] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 55.

[921] ICRC, *Commentary on Additional Protocols,* 680.

[922] Additional Protocol I, Article 57(2)(a)(ii).

[923] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 58.

Third, Article 57(2)(b) requires an attack to be canceled or suspended if it is understood that the target is not a military objective, is under special protection, or the attack would be disproportionate according to the principle of proportionality.[924] Therefore, commanders, decision-makers, and ground personnel must cancel or stop the attack if such situations are identified either after planning or during execution.

Fourth, Article 57(2)(c) requires that an "effective advance warning shall be given of attacks which may affect the civilian population, unless circumstances do not permit."[925] This obligation requires the attacker to issue warnings before an attack that could affect civilians. A warning must meet several criteria to be effective: it must reach civilians who are in danger due to the attack, clearly instruct them to avoid harm, and be credible.[926] The warnings can be general or specifically indicate the targets to be attacked.[927] This obligation is valid "unless the circumstances do not permit," provided that the element of surprise is essential for the success of the attack or the security of the attacking or allied forces would be threatened; in such cases, there is no need for the attacker to issue warnings.[928] The obligations imposed by the IHL remain binding even if the civilian population is still present in the operational area after the warning by the attacker.[929]

Fifth, Article 57(3) obliges the attacking party to select the target that poses the least danger to civilian lives and objects, "[w]hen a choice is possible between several military objectives for obtaining a similar military advantage."[930] To follow this rule, the attacking party must choose among options to target the objective that would cause the least harm to civilians when attacked. A classic example of this obligation is

[924] Additional Protocol I, Article 57(2)(b).

[925] Additional Protocol I, Article 57(2)(c).

[926] Sassòli, *International Humanitarian Law*, 394.

[927] ICRC, *Commentary on Additional Protocols,* 687.

[928] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 64.

[929] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 65.

[930] Additional Protocol I, Article 57(3).

targeting a railway's critical points in an inhabited open area, rather than a railway station located in a populated town.[931] Although the third paragraph does not specify a priority between civilian lives and objects, it would be more appropriate to prioritize protecting civilian lives over objects, considering the humanitarian goal and purpose of IHL.[932]

The precautionary obligations of the attacker remain valid even if the defending party fails to fulfill its passive precautionary obligations.[933] After outlining the active precautionary obligations, the passive precautions of the defender will be discussed below.

4.4.2. Passive Precautions

In addition to active precautions that the attacking party must take, IHL also requires the defending party, which controls the civilian population, to take passive precautions to protect civilians and objects. These obligations are outlined in Article 58 of AP I, which instructs parties to take precautions against the effects of attacks to the "maximum extent feasible."[934] The passive precautions described in Article 58 complement the active precautions outlined in Article 58.[935] Weaker than their active counterparts, passive precautions are limited by feasibility just like active precautions.[936] This means that passive precautions are confined to those that are practicable or practically possible given all relevant circumstances at the time, including humanitarian and military considerations.[937]

---

[931] ICRC, *Commentary on Additional Protocols,* 687.

[932] Bothe, Partsch and Solf, *New Rules for Victims,* 411.

[933] Sassòli, *International Humanitarian Law*, 399.

[934] Additional Protocol I, Article 58.

[935] Bothe, Partsch and Solf, *New Rules for Victims,* 413.

[936] Sassòli, *International Humanitarian Law*, 397.

[937] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 70.

First, Article 58(a) obliges the defending party to "without prejudice to Article 49 of the Fourth Convention endeavour to remove the civilian population, individual civilians, and civilian objects under their control from the vicinity of military objectives."[938] This obligation is essential when military targets are closely connected to densely populated areas and cannot be practically separated from them.[939] Under this obligation, the defending party must endeavor to evacuate the civilian population and remove movable civilian objects from the vicinity of military objectives.[940] While immovable objects cannot be removed, the civilians located there must be evacuated.[941] This obligation applies when evacuation is the only way to protect the civilian population and objects, and lasts until the danger ceases.[942] In addition, an occupying power can only take such precautions by abiding by Article 49 of the Fourth Convention.

Second, Article 58(b) requires the defending party to "avoid locating military objectives within or near densely populated areas."[943] This obligation concerns the placement of both permanent and mobile military objectives in peacetime and during armed conflicts.[944] States should endeavour to locate permanent military objectives away from populated areas and avoid placing mobile military objectives in populated areas.[945] If States can not avoid densely populated areas during their movements, they must pass through the populated area as quickly as possible in a way that poses the least risk to civilians and objects.[946]

---

[938] Additional Protocol I, Article 58(a).

[939] Henckaerts and Doswald-Beck, *Customary International Humanitarian Law,* 76.

[940] ICRC, *Commentary on Additional Protocols,* 693.

[941] ICRC, *Commentary on Additional Protocols,* 694.

[942] Quéguiner, "Precautions under the Law," 818.

[943] Additional Protocol I, Article 58(b).

[944] Quéguiner, "Precautions under the Law," 818.

[945] ICRC, *Commentary on Additional Protocols,* 694.

[946] Quéguiner, "Precautions under the Law," 818.

Third, Article 58(c) obliges the defending party to "take the other necessary precautions to protect the civilian population, individual civilians and civilian objects under their control against the dangers resulting from military operations."[947] This obligation enables States to take additional precautionary measures within their capacity and other circumstances related to conflict.[948] Such measures can include providing shelters for the civilian population, organizing civil defense services, and establishing alert systems.[949]

4.4.3. Precautions in Cyberspace

Given that States affirmed that international humanitarian law applies in cyberspace,[950] the principle of precautions also applies in cyberspace given that precautions is both part of treaty law and international customary law. State positions reflect this as well. For example, Brazil observes that "the IHL principle of precaution is also applicable to the use of ICTs by States."[951] Similarly, France emphasizes that "[w]hen cyberoperations are conducted, constant care should be taken to spare the civilian population, civilians and civilian objects."[952] Likewise, Canada states that "cyber activities must respect relevant treaty and customary IHL rules applicable to attacks including … the requirement to take precautions in attack."[953] In the same direction, the Tallinn Manual states that "[d]uring hostilities involving cyber operations, constant care shall be taken to spare the civilian population, individual civilians, and civilian objects."[954] Accordingly, the principle of precautions applies in cyberspace.

---

[947] Additional Protocol I, Article 58(c).

[948] Quéguiner, "Precautions under the Law," 818.

[949] ICRC, *Commentary on Additional Protocols,* 694.

[950] UN GGE, *2021 Report*, 18.

[951] UNGA, *Official Compendium*, 22.

[952] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 15.

[953] Government of Canada, *International Law Applicable in Cyberspace*, para. 49.

[954] Schmitt, *Tallinn Manual,* 476.

In this context, commanders and ground personnel must exercise constant care during all phases of the operation, including planning and execution.[955] Just like traditional warfare, precautions in cyberspace is also subject to feasibility; commanders and ground personnel must do everything practicable, but their responsibility is limited to the circumstances known to them at the time.[956] Although the interconnectedness of civilian and military networks and the secretive nature of cyberspace make it more difficult to assess a cyber operation's effects, this does not release the attacking party from its precautionary obligations.[957]

Active obligations in Article 57 apply to cyber operations that qualify as armed attacks under IHL. First, military commanders must do everything feasible to verify that the target is a military objective.[958] While verifying their targets, commanders shall make decisions based on the available information at the time and receive intelligence from technical experts if necessary.[959] Such a verifying precaution might include mapping the network that will be targeted in a cyber operation.[960] Commanders must cease the attack if they realize that the target is a civilian object or an object under special protection, and they should refrain from attacking the target if they cannot feasibly acquire sufficient information.[961] The verification process would be more nuanced since cyberspace allows the attacking party to divide the targeted network into smaller parts.[962] This responsibility is crucial due to the interconnected nature of cyberspace, as an attack on one network can cause severe effects on others.

---

[955] Eric Talbot Jensen, "Cyber Attacks: Proportionality and Precautions in Attack," *International Law Studies* 89, no. 1 (2013): 202, https://digital-commons.usnwc.edu/ils/vol89/iss1/15/.

[956] Jensen, "Cyber Attacks: Proportionality and Precautions," 211.

[957] Yunus Emre Gül, "The Application of the Principle of Precautions to Cyber Operations," *The Military Law and the Law of War Review* 61, no. 1 (2023): 16, https://doi.org/10.4337/mllwr.2023.01.01.

[958] Dinniss, *Laws of War*, 211.

[959] Schmitt, *Tallinn Manual,* 477.

[960] Droege, "Cyber Warfare," 574.

[961] Schmitt, *Tallinn Manual,* 478-479.

[962] Dinniss, *Laws of War*, 216.

Secondly, military commanders must take feasible precautions regarding the cyber means and methods used in the attack to minimize collateral damage, including not only the means or methods employed but also how they are utilized.[963] If a cyber means or method would achieve a similar military advantage with less civilian harm compared to other alternatives, it should be chosen line with the principle of precautions.[964] When choices of means or methods are made, "[t]he risks inherent in cyberspace (immediacy of effects, intrinsic duality of military objectives, hyperconnectivity, difficulty of tracing operations, vulnerability of systems) must therefore be taken into account."[965] After selecting the cyber means or method, the commander must maintain oversight of the chosen means or method and be prepared to modify the operation if it begins to produce results that would be contrary to IHL rules.[966]

Third, commanders must select the option that would pose the least risk to civilians when attacked among targets offering similar advantages. In this regard, cyber operations must be directed at the target that would cause the least injury or death to persons or damage or destruction to objects, both directly and indirectly, with comparable military advantage, considering feasibility under the circumstances at the time.[967] Similarly, if commanders or those carrying out the attack realize that the cyber operation is disproportionate, they must suspend it, and if the attack has already started, they must cease it.[968]

Lastly, the attacker must issue effective warnings to the civilian population for cyber operations that could affect them if such warnings are appropriate under the

[963] Schmitt, *Tallinn Manual,* 480.

[964] Gül, "Precautions to Cyber Operations," 20.

[965] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 15.

[966] Jensen, "Cyber Attacks: Proportionality and Precautions," 203.

[967] Schmitt, *Tallinn Manual,* 482.

[968] Schmitt, *Tallinn Manual,* 481.

circumstances.[969] The warning should be clear and specific, aiming to reduce collateral damage, which can include the effects of the cyber operation and guidance on how civilians can protect themselves.[970] Effective warnings can be conveyed through both cyber means, such as the internet, websites, and texting applications, and conventional methods like media.[971] As mentioned above, the effectiveness of warning measures depends on the existence of appropriate circumstances. If a State has justifiable reasons, for example, if secrecy is required for the operation's success, it can choose not to issue warnings.[972]

As expressed by France in its national position, these active precautions discussed "are backed up by precautionary measures against the effects of an attack which a State should take in order to protect the civilian population and civilian objects against the dangers resulting from cyber operations."[973] In this context, passive precautions outlined in Article 58 of AP I, which must be taken by the defending party, are also applicable in cyberspace, as stated by the Tallinn Manual. "[t]he parties to an armed conflict shall, to the maximum extent feasible, take necessary precautions to protect the civilian population, individual civilians, and civilian objects under their control against the dangers resulting from cyber attacks."[974]

Territorial application of passive precautions poses a major challenge in cyberspace, especially concerning the notion of "control" in Article 58. In the cyber context, if a State has the authority to direct a network's operation, that network is effectively under the State's control, meaning the State is responsible for taking passive precautions to the maximum extent feasible.[975]

---

[969] Schmitt, *Tallinn Manual,* 484.

[970] Gül, "Precautions to Cyber Operations," 30.

[971] Schmitt, *Tallinn Manual,* 486.

[972] Gül, "Precautions to Cyber Operations," 29.

[973] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 16.

[974] Schmitt, *Tallinn Manual,* 487.

[975] Jensen, "Cyber Attacks: Proportionality and Precautions," 215.

Firstly, the defending party is required to segregate civilian and military networks to the maximum extent feasible, even if it is costly.[976] For example, the defending party can create a separate cyber infrastructure solely for military communications or move dual-use infrastructure that could become a military target away from civilians, civilian objects, and objects under special protection.[977] If the defending party cannot segregate the military and civilian networks, it is obligated to take necessary measures to protect civilians and objects from the direct and indirect effects of cyber operations.[978] Apart from these two instances, other passive precautions that the defending party can take include, but not limited to

> segregating computer systems on which critical civilian infrastructure depends from the Internet; backing up important civilian data; making advance arrangements to ensure the timely repair of important computer systems; digitally recording important cultural or spiritual objects to facilitate reconstruction in the event of their destruction; and using anti-virus measures to protect civilian systems that might suffer damage or destruction during an attack on military cyber infrastructure.[979]

Even if the defending party fails to take passive precautions, the attacking party remains bound by relevant IHL rules while conducting its cyber operations.[980]

4.4.4. Precautions and Critical Infrastructures

As demonstrated, subject to feasibility conditions, States are obliged to take various precautionary measures to reduce civilian harm when conducting their cyber operations, including those targeting CIs, as Denmark observed, that "States are required to take all reasonable precautions to spare the civilian population as well as

[976] Jensen, "Cyber Attacks: Proportionality and Precautions," 212.

[977] Gül, "Precautions to Cyber Operations," 35.

[978] Jensen, "Cyber Attacks: Proportionality and Precautions," 214.

[979] Schmitt, *Tallinn Manual,* 488.

[980] Schmitt, *Tallinn Manual,* 491.

civilian individuals and objects, including essential civilian infrastructure, services, and data, when planning or conducting cyber operations."[981]

Precautions is especially important for dual-use CI that can be legally targeted because they are also used for military purposes. In this regard, States must first take all feasible measures to verify that the CI to be targeted is not a civilian object or under special protection. To achieve this, military commanders must gather the best available intelligence and utilize technical expertise as needed.

If a CI has dual-use, meaning it is used for both military and civilian purposes, the components explicitly used for military purposes must be identified and targeted rather than the entire CI. Additionally, States should select cyber means and methods that cause the least civilian harm when carrying out cyber operations against a CI, as demonstrated by France, which states that "[t]he use of malware which deliberately reproduces and propagates with no possible control or reversibility and is hence likely to cause significant damage to critical civilian systems or infrastructure, is contrary to IHL."[982]

Another example could include targeting a dual-use CI at night or early morning when it is not heavily used by civilians.[983] Thirdly, if attacking a dual-use CI provides a comparable military advantage to targeting a purely military objective, then the cyber operation should be directed at the latter, since it would cause less harm to civilians. The same applies when choosing between two dual-use CIs.

Fourth, States must issue effective warnings when targeting CIs if circumstances permit. Lastly, commanders and ground personnel must cancel or suspend the attack if it becomes clear that the CI being targeted is a civilian object, under special protection, or if the attack would be disproportionate compared to the anticipated military advantage, as emphasized by Germany that

[981] Kjelgaard and Melgaard, "Denmark's Position Paper," 455.

[982] Ministry of Armed Forces, *International Law Applied in Cyberspace*, 16.

[983] Gül, "Precautions to Cyber Operations," 24.

> if it becomes apparent that the target is not a military one or is subject to special protection, those who plan, approve or execute the cyber attack must refrain from executing or suspend the attack. The same applies when the attack may be expected to cause excessive collateral damage to civilians and civilian objects.[984]

In addition to active precautions, States are obligated to implement passive precautions for CIs under the principle of precautions. In this context, States can take various measures, including segregating military and civilian CIs, establishing monitoring and warning systems for CIs, backing up civilian data, implementing necessary cybersecurity measures to deter cyber operations against CIs, such as antivirus software and firewalls, and locating military objectives away from civilian or specially protected areas and CIs.

In summary, this chapter demonstrates that IHL provides a comprehensive framework for the protection of CIs during armed conflicts, provided that its fundamental rules are interpreted in a way that reflects the specific features of cyberspace. This study identifies two essential shifts: treating loss of functionality as an attack and recognizing civilian data as a protected object. Given the widespread presence of dual-use infrastructures, this study concludes that proportionality and precautions carry even greater significance in cyberspace than in conventional warfare. In addition, this thesis argues that even if a CI is used for military purposes alongside with civilian purposes, humanitarian object and purpose of IHL must remain the priority, which requires attackers to adopt an approach that spares civilian functions as much as possible. In this regard, IHL does not only limit the methods of cyber warfare but also serves as a crucial safeguard for the survival and well-being of civilian population in a digitalized conflict environment.

[984] Federal Government of Germany, *Application of International Law in Cyberspace*, 10.

CHAPTER 5

CONCLUSION

Initially developed as a limited network for sharing information, cyberspace has grown into a complex and multidimensional fifth domain of human activity that transcends physical and political boundaries. Our daily lives are increasingly intertwined with cyberspace, serving purposes such as communication, knowledge sharing, political engagement, and economic transactions. This trend is likely to continue growing with the advent of new technologies.

Just like daily human life, the critical infrastructures vital for daily live, socioeconomic well-being of the society, and national security are also increasingly integrated with cyberspace. This increased digitalization has made individuals, societies, and States more vulnerable to cyber threats from both States and non-State actors in both peacetime and in times of armed conflicts.

Although it was initially claimed that cyberspace was a free domain outside State sovereignty and interference, States have extended their jurisdiction to cyberspace through legislation and regulation using various tools. The idea that cyberspace is subject to State sovereignty and jurisdiction is repeatedly affirmed by States in UN GGE and OEWG processes further supported by State practice. In light of this fact, it is now undisputed that States have the right to exercise prescriptive, enforcement, and adjudicative jurisdiction over cyber acts, based on the jurisdictional principles of international law stemming from their sovereign rights.

Similar to State sovereignty and jurisdiction, the applicability of international law in cyberspace is repeatedly affirmed by States in UN GGE and OEWG processes and is

likewise supported by State practice. Given that no special international regime exists for cyberspace, the international legal rules applied in cyberspace are derived from the existing framework of international law. In this regard, international legal rules applicable in cyberspace derive from the primary sources identified in Article 38 of the Statue of the International Court of Justice, while subsidiary means listed in the same Article assist in determining the scope and interpretation of these rules.

Despite a consensus on the applicability of international law in cyberspace, there are disagreements among States on how these legal rules apply. Several initiatives exist within various frameworks, the most prominent of which are the UN GGE and later OEWG processes, to allow States to discuss and clarify the exact scope and application of international legal rules in cyberspace. In addition to multilateral forums among States, there are also cyber norm development processes involving or led by different stakeholders, particularly the private sector. Different norm processes may operate, run, and exist simultaneously, serving as "soft law" for cybersecurity in the absence of a specific cyberspace regime.

Critical infrastructures are increasingly targeted in cyberspace through malicious cyber operations carried out by both States and non-State actors with various motives, ranging from political to purely economic purposes. Targeting critical infrastructures with cyber means can cause serious repercussions for States and societies by disrupting essential services, while also heightening the risk of conflicts between states by fostering mistrust. In this regard, international law, which governs interactions between sovereign and equal States, can be used to prevent these effects and promote a more stable and peaceful cyberspace.

States have both the right to designate what constitutes critical infrastructure and the duty to protect it. In this regard, the security of such infrastructures in cyberspace is among the prominent topics addressed by States and international organizations. Efforts by States and international organizations have led to the adoption of several norms in the UN GGE's 2015 report regarding the security of critical infrastructures in cyberspace, which urges States to refrain from targeting critical infrastructures, to take appropriate measures, and to promote international cooperation. In addition to

these non-binding norms, binding rules of international law also provide safeguards against the targeting of critical infrastructure during both peacetime and armed conflict.

In peacetime, international law provides protection for critical infrastructure in cyberspace through its relevant rules, specifically sovereignty, non-intervention, due diligence, and the prohibition of the threat or use of force. These rules apply exclusively between States. In this context, malicious cyber operations against critical infrastructures may violate these rules if conducted by a State or a non-State actor whose conduct can be attributed to a State under international law, which would trigger the responsibility of the perpetrator State.

In general terms, firstly, critical infrastructures are subject to the sovereignty of the State in which they are located, and malicious cyber operations that target them may violate the State's sovereignty if they cause physical damage, injury, or loss of functionality, or if such operations cause interference or usurpation of inherently governmental functions, regardless of whether the cyber operation causes those effects.

Secondly, such cyber operations might violate non-intervention if the cyber operation is conducted to coerce the victim State into doing or not doing something within its *domaine réservé*, which is left unregulated by international law to the discretion of the State, with the aim of gaining a benefit directly or indirectly, regardless of the operation's success.

Thirdly, such cyber operations may violate the prohibition of the use or threat of force if the operation's scale and effects meet the use of force threshold individually or collectively, or if a State directly or indirectly declares that it will conduct such a cyber operation. The fact that a cyber operation targets critical infrastructure may tilt the balance toward violating the prohibition of the use of force. Even if a cyber operation falls below the use of force threshold, it might nevertheless constitute a violation of the victim State's sovereignty, and if the coercive element is present, the principle of non-intervention. Moreover, such a cyber operation may trigger the victim State's

inherent right of self-defense if the operation's scale and effects constitute the most grave form of use of force. If such a situation occurs, the victim State must exercise its right of self-defense in a necessary, proportionate, and immediate manner and notify the UN Security Council.

Lastly, States are obliged to exercise due diligence to prevent, stop, or if these options are not possible, inform other States about malicious cyber operations that target another State's critical infrastructure, when they know or should have known that such operations, including those conducted by non-State actors, originate from areas under their jurisdiction. Due diligence obligation also applies to transit States if they have knowledge of malicious operations. Whether a State violated these rules must be assessed on a case-by-case basis.

International law also provides protection for critical infrastructures during armed conflicts, whether international or non-international, as regulated by the rules of international humanitarian law. Although disagreements over the applicability of IHL in cyberspace resulted in the collapse of the 2017 GGE process, the majority of States, international organizations, and legal experts affirm the applicability of IHL in cyberspace. These rules govern cyber operations conducted in the context of an armed conflict and qualify as an attack under IHL. In this context, cyber operations may qualify as an attack under IHL if they cause or are reasonably expected to cause death or injury to persons, physical damage to objects, or loss of functionality without any physical harm. IHL rules apply regardless of whether the armed conflict began in accordance with *jus ad bellum*. Several IHL rules can be used to protect critical infrastructures against cyber attacks during armed conflict, specifically distinction, proportionality, and precautions. For a cyber attack conducted in the context of an armed conflict to be legitimate, it must comply with these three rules.

Under distinction, it is forbidden to attack civilian populations and objects or conduct indiscriminate attacks. Civilian objects are defined negatively in AP I; an object is considered a civilian object as long as it does not qualify as a military objective, that by its nature, location, purpose, or use does not make an effective contribution to military action, and whose destruction, capture, or neutralization offers a definite

military advantage in circumstances prevailing at the time. In case of doubt, an object should be regarded as a civilian object. Accordingly, it is prohibited to attack critical infrastructures that do not constitute a military objective under distinction.

Whether dual-use objects and data are protected under distinction is controversial because dual-use objects can also be used for military purposes, and data does not fit the definition provided in AP I. However, an attacking party cannot freely attack a dual-use object: it must identify the parts and components used for military purposes and carefully assess whether the attack would provide a definite military advantage. Regarding data, it should be considered an object entitled to protection under the principle of distinction, given the purpose of IHL, which is to protect civilians from the dangers of armed conflicts.

IHL also grants special protection to certain categories of objects, namely medical units, objects indispensable for the survival of the civilian population, and works and installations containing dangerous forces, which cannot be attacked under any circumstances, including critical infrastructures that are part of such objects.

Even if an object is a legally targetable military objective, the attack on it must be proportionate; the expected concrete and direct military advantage from the attack should not cause excessive harm when compared to civilian harm. Proportionality is especially important given the high levels of dual-use infrastructure and interconnectedness in cyberspace. In this context, even if a critical infrastructure constitutes a legitimate military objective, it would still be forbidden to target it if the direct or indirect collateral damage would be excessive. Finally, parties to a conflict must take all feasible precautions to minimize harm to civilians. This includes verifying that the critical infrastructure targeted is not a civilian object or under special protection, identifying components used for military purposes in cases of dual-use functions, selecting cyber means and methods that cause the least civilian harm, separating military and civilian critical infrastructures, establishing warning systems, and implementing cybersecurity measures. All these rules provide significant protection to critical infrastructures in times of armed conflict.

In conclusion, this thesis demonstrates that cyberspace is not a lawless zone. Rather, it is a domain governed by international law, adapted through interpretation to meet the challenges of cyberspace. Although international law was not originally designed for cyberspace, its fundamental rules remain applicable and adaptable to this new domain. As established in Chapter 2, the international legal rules derived from the primary sources, namely treaties, custom and general principles possess a sufficient flexibility that allows them to adapt to developments in cyberspace. Through the interpretation guided by the VCLT, the object and purpose of foundational legal instruments such as the UN Charter and the 1949 Geneva Conventions remain fully applicable to cyber operations. Therefore, a cyber operation targeting a CI, such as a power grid, is a conduct that engages well established international legal obligations.

Furthermore, the synthesis of peacetime and armed conflict frameworks provides an important conclusion, namely that the protection of CIs constitutes an existing legal obligation under international law. The primary challenge therefore is not the absence of law, but clarifying how legal rules should be interpreted and applied to the unique characteristics of cyberspace. As CIs become increasingly integrated with emerging technologies, stability in cyberspace will rely on States' commitment to interpreting existing obligations in a responsible manner. By adhering to international law, States can prevent cyber operations targeting critical infrastructures, thereby promoting a more stable and secure cyber environment for States. In this regard, findings of this study suggest that rather than awaiting the adoption of a comprehensive cyber treaty, the international community should focus on strengthening and integrating existing legal norms. Through the articulation of national positions and multilateral processes such as the UN GGE and OEWG, States are already contributing to the gradual clarification and consolidation of customary international law in cyberspace.

By examining the rules applicable in both peacetime and armed conflict frameworks, this study concludes that, despite continuing disagreements among States regarding the precise application of international legal rules in cyberspace, the protection of CIs is not dependent on a single rule, but rather on a broader legal framework which different international legal rules converge. In addition, while the absence of a comprehensive global cyber regime remains a significant hurdle, the emergence of

“soft law” through the UN-led processes provides a crucial intermediate framework. These non-binding norms act as a bridge, offering States a flexible tool to respond to rapid technological developments. Taken together, these developments indicate that international law already provides an important framework for regulating cyber operations and strengthening the protection of CIs in evolving digital environment.

BIBLIOGRAPHY

Akande, Dapo. "Classification of Armed Conflicts." In The Oxford Guide to International Humanitarian Law, edited by Ben Saul and Dapo Akande, 1st ed. Oxford University Press, 2020. https://doi.org/10.1093/law/9780198855309.003.0002.

Alexander, Amanda. "A Short History of International Humanitarian Law." European Journal of International Law 26, no. 1 (2015): 38-109. https://doi.org/10.1093/ejil/chv002.

American Law Institute. Restatement of the Law: The Foreign Relations Law of the United States. American Law Institute Publishers, 1987.

Arimatsu, Louise. "Classifying Cyber Warfare." In Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias and Russell Buchan, 2nd ed. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.00031.

Bannelier, Karine. "Due Diligence as a Cardinal Principle in the Fight against Malicious Cyber Activities." In Global Cybersecurity and International Law. Routledge, 2024.

Bannelier, Karine. "Is the Principle of Distinction Still Relevant in Cyberwarfare? From Doctrinal Discourse to States Practice." In Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias and Russell Buchan, 2nd ed. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.00032.

Berk, Michael. "Recommendations 13 (g) and (h)." In Voluntary Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology - A Commentary. United Nations, 2017.

Besson, Samantha. "Sovereignty." In The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, 1st ed., vol. 9. Oxford University Press, 2012.

Bothe, Michael, Karl Josef Partsch, Waldemar A. Solf, and Martin Eaton. New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949. 2nd ed. Martinus Nijhoff Publishers, 2013.

Boyle, Alan. "Soft Law in International Law-Making." In International Law, 5th ed., edited by Malcolm D. Evans, 119-137, Oxford University Press, 2018.

Braverman, Suella. "International Law in Future Frontiers." Speech at Chatham House, May 19, 2022. https://www.gov.uk/government/speeches/international-law-in-future-frontiers

Brownlie, Ian. International Law and the Use of Force by States. Oxford University Press, 1963. https://doi.org/10.1093/acprof:oso/9780198251583.001.0001.

Coco, Antonio, and Talita De Souza Dias. "'Cyber Due Diligence': A Patchwork of Protective Obligations in International Law." European Journal of International Law 32, no. 3 (2021): 771–806. https://doi.org/10.1093/ejil/chab056.

Corn, Geoffrey S., Victor M. Hansen, Richard B. Jackson, Chris Jenks, Eric Jensen, and James A. Schoettler. The Law of Armed Conflict: An Operational Approach. First edition. Aspen Casebook Series. Wolters Kluwer, 2012.

Corten, Olivier. The Law against War: The Prohibition on the Use of Force in Contemporary International Law. 1st ed. Hart Publishing, 2010.

Costelloe, Daniel. "Conceptions of State Jurisdiction in the Jurisprudence of the International Court of Justice and the Permanent Court of International Justice." In The Oxford Handbook of Jurisdiction in International Law, edited by Stephen Allen et. al. Oxford University Press, 2019. https://doi.org/10.1093/law/9780198786146.003.0019.

Couzigou, Irène. "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations." International Review of Law, Computers & Technology 32, no. 1 (2018): 37–57. https://doi.org/10.1080/13600869.2018.1417763.

Crawford, Emily. “The Temporal and Geographic Reach of International Humanitarian Law.” In The Oxford Guide to International Humanitarian Law, edited by Ben Saul and Dapo Akande. Oxford University Press, 2020. https://doi.org/10.1093/law/9780198855309.003.0003.

Creemers, Rogier, Graham Webster, and Paul Triolo. “Translation: Cybersecurity Law of the People’s Republic of China (Effective June 1, 2017).” DigiChina. accessed April 12, 2025. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/.

Dinstein, Yoram. The Conduct of Hostilities under the Law of International Armed Conflict. 3rd ed. Cambridge University Press, 2015. https://doi.org/10.1017/cbo9781316389591.

Dinstein, Yoram. War, Aggression, and Self-Defence. 5th ed. Cambridge University Press, 2012.

Droege, Cordula. “Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians.” International Review of the Red Cross 94, no. 886 (2012): 533–78. https://doi.org/10.1017/S1816383113000246.

Efrony, Dan, and Yuval Shany. “A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice.” American Journal of International Law 112, no. 4 (2018): 583–657. https://doi.org/10.1017/ajil.2018.86.

Fenton III, Hensey A. “Proportionality and Its Applicability in the Realm of Cyber-Attacks.” Duke Journal of Comparative & International Law 29, no. 2 (2018): 335-368.

Finnemore, Martha, and Duncan B. Hollis. “Constructing Norms for Global Cybersecurity.” The American Journal of International Law 110, no. 3 (2016): 425–79.

Focarelli, Carlo. “Self-Defence in Cyberspace.” In Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias and Russell Buchan, 2nd ed. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.00026.

Gallant, Kenneth S. International Criminal Jurisdiction: Whose Law Must We Obey? Oxford University Press, 2022.

Geiß, Robin and Christophe Paulussen “Specifically Protected Persons and Objects.” In The Oxford Guide to International Humanitarian Law, edited by Ben Saul and Dapo Akande. Oxford University Press, 2020. https://doi.org/10.1093/law/9780198855309.003.0008.

Geiß, Robin, and Henning Lahmann. “Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space.” Israel Law Review 45, no. 3 (2012): 381–99. https://doi.org/10.1017/s0021223712000179.

Gill, Terry D. “International Humanitarian Law Applied to Cyber-Warfare: Precautions, Proportionality and the Notion of Attack under the Humanitarian Law of Armed Conflict.” In Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias and Russell Buchan, 2nd ed. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.00033.

Gisel, Laurent, Tilman Rodenhäuser, and Knut Dörmann. “Twenty Years on: International Humanitarian Law and the Protection of Civilians against the Effects of Cyber Operations during Armed Conflicts.” International Review of the Red Cross 102, no. 913 (2020): 287–334. https://doi.org/10.1017/S1816383120000387.

Gray, Christine. “The Use of Force and International Legal Order.” In International Law, edited by Malcolm Evans, 5th ed. Oxford University Press, 2018. https://doi.org/10.1093/he/9780198791836.003.0027.

Green, James A., ed. “The Regulation of Cyber Warfare Under Jus Ad Bellum.” In Cyber Warfare: A Multidisciplinary Analysis. Routledge, 2016.

Greenwood, Christopher. “Self-Defence.” In The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, 1st ed., vol. 9. Oxford University Press, 2012.

Gül, Yunus Emre. “The Application of the Principle of Precautions to Cyber Operations.” The Military Law and the Law of War Review 61, no. 1 (2023): 3–38. https://doi.org/10.4337/mllwr.2023.01.01.

Haataja, Samuli. “Cyber Operations against Critical Infrastructure under Norms of Responsible State Behaviour and International Law.” International Journal of Law and Information Technology 30, no. 4 (2022): 423–43. https://doi.org/10.1093/ijlit/eaad006.

Harrison Dinniss, Heather A. “The Nature of Objects: Targeting Networks and the Challenge of Defining Cyber Military Objectives.” Israel Law Review 48, no. 1 (2015): 39–54. https://doi.org/10.1017/s0021223714000272.

Harrison Dinniss, Heather. Cyber Warfare and the Laws of War. Cambridge University Press, 2012.

Henckaerts, Jean-Marie, Louise Doswald-Beck, and Carolin Alvermann eds. Customary International Humanitarian Law. Cambridge University Press, 2005.

Henckaerts, Jean-Marie. “History and Sources.” In The Oxford Guide to International Humanitarian Law, edited by Ben Saul and Dapo Akande. Oxford University Press, 2020. https://doi.org/10.1093/law/9780198855309.003.0001.

Hörnle, Julia, and Elif Mendos Kuskonmaz. “Criminal Jurisdiction—Concurrent Jurisdiction, Sovereignty, and the Urgent Requirement for Coordination.” In Internet Jurisdiction Law and Practice, edited by Julia Hörnle Oxford University Press, 2021. https://doi.org/10.1093/oso/9780198806929.003.0004.

International Committee of Red Cross (ICRC). International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. ICRC, 2024. https://www.icrc.org/en/report/2024-icrc-report-ihl-challenge

International Committee of Red Cross. Commentary on the First Geneva Convention: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Cambridge University Press, 2016. https://doi.org/10.1017/9781316755709.

International Committee of the Red Cross. What is International Humanitarian Law. ICRC, 2022. https://www.icrc.org/sites/default/files/document/file_list/what_is_ihl.pdf

Jensen, Eric Talbot. “Cyber Attacks: Proportionality and Precautions in Attack.” International Law Studies 89, no. 1 (2013): 198–217.

Joley, Jason. “Recommendation 13 (f).” In Voluntary Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology - A Commentary. United Nations, 2017.

Kenny, Jack. “Cyber Operations and the Status of Due Diligence Obligations in International Law.” International and Comparative Law Quarterly 73, no. 1 (2024): 135–76. https://doi.org/10.1017/S0020589323000489.

Kilovaty, Ido. “The International Law of Cyber Intervention.” in Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias and Russell Buchan, 2nd ed. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.00014.

Kjelgaard, Jeppe Mejer, and Ulf Melgaard. “Denmark’s Position Paper on the Application of International Law in Cyberspace: Introduction.” Nordic Journal of International Law 92, no. 3 (2023): 446–55. https://doi.org/10.1163/15718107-20230001.

Kohl, Uta. “Jurisdiction in Network Society.” In Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias and Russell Buchan, 2nd ed. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.00013.

Koivurova, Timo. “Due Diligence.” In The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, 1st ed., vol. 3. Oxford University Press, 2012.

Kolb, Robert, and Katherine Del Mar. “Treaties for Armed Conflict.” In The Oxford Handbook of International Law in Armed Conflict, edited by Andrew Clapham and Paola Gaeta. Oxford University Press, 2014. https://doi.org/10.1093/law/9780199559695.003.0004.

Kouloufakos, Triantafyllos. “Cyber Operations as Threats of Force: A Welcome Addition or Splitting Hair?” In Global Cybersecurity and International Law. Routledge, 2024.

Kulesza, Joanna. Due Diligence in International Law. Brill Nijhoff, 2016. https://doi.org/10.1163/9789004325197.

Kunig, Philip. "Intervention, Prohibition Of." In The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, 1st ed., vol. 6. Oxford University Press, 2012

Lagerwall, Anne, and François Dubuisson. "The Threat of the Use of Force and Ultimata." In The Oxford Handbook of the Use of Force in International Law, edited by Marc Weller. Oxford University Press, 2016. https://doi.org/10.1093/law/9780199673049.003.0043.

Lowe, Vaughan, and Antonios Tzanakopoulos. "Economic Warfare." In The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, 1st ed., vol. 3. Oxford University Press, 2012.

Lubell, Noam. "The Problem of Imminence in an Uncertain World." In The Oxford Handbook of the Use of Force in International Law, edited by Marc Weller. Oxford University Press, 2015. https://doi.org/10.1093/law/9780199673049.003.0032.

Mačák, Kubo. "Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law." Israel Law Review 48, no. 1 (2015): 55–80. https://doi.org/10.1017/s0021223714000260.

Mačák, Kubo. "Unblurring the Lines: Military Cyber Operations and International Law." Journal of Cyber Policy 6, no. 3 (2021): 411–28. https://doi.org/10.1080/23738871.2021.2014919.

Mačák, Kubo. "Will the Centre Hold? Countering the Erosion of the Principle of Distinction on the Digital Battlefield." International Review of the Red Cross 105, no. 923 (2023): 965–91. https://doi.org/10.1017/s1816383123000152.

McDonald, Neil. "The Role of Due Diligence in International Law." International and Comparative Law Quarterly 68, no. 4 (2019): 1041–54. https://doi.org/10.1017/S0020589319000344.

Melzer, Nils. Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law. International Committee of the Red Cross, 2009.

Milanovic, Marko. “Revisiting Coercion as an Element of Prohibited Intervention in International Law.” American Journal of International Law 117, no. 4 (2023): 601–50. https://doi.org/10.1017/ajil.2023.40.

Mills, Alex. “Rethinking Jurisdiction in International Law.” British Yearbook of International Law 84, no. 1 (2014): 187–239. https://doi.org/10.1093/bybil/bru003.

Moulin, Thibault. “Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward.” Journal of Conflict and Security Law 25, no. 3 (2020): 423–47. https://doi.org/10.1093/jcsl/kraa011.

Moynihan, Harriet. “The Vital Role of International Law in the Framework for Responsible State Behaviour in Cyberspace.” Journal of Cyber Policy 6, no. 3 (2021): 394–410. https://doi.org/10.1080/23738871.2020.1832550.

Moynihan, Harriet. “Unpacking Due Diligence in Cyberspace.” Journal of Cyber Policy 8, no. 1 (2023): 4–25. https://doi.org/10.1080/23738871.2023.2250358.

Moynihan, Harriet. The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention. The Royal Institute of International Affairs, 2019.

Ossoff, William. “Hacking the Domaine Reserve´: The Rule of Non-Intervention and Political Interference in Cyberspace.” Harvard International Law Journal 62, no. 1 (2021): 295–323.

Pascucci, Peter. “Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution.” Minnesota Journal of International Law 26, no. 2 (2017): 419.

Quéguiner, Jean-François. “Precautions under the Law Governing the Conduct of Hostilities.” International Review of the Red Cross 88, no. 864 (2006): 793–821. https://doi.org/10.1017/s1816383107000872.

Roberts, Anthea, and Sandesh Sivakumaran. “The Sources of International Law.” In International Law, 5th ed., edited by Malcolm D. Evans, 89-118. Oxford University Press, 2018.

Roscini, Marco. “Cyber Operations as a Use of Force.” In Research Handbook on International Law and Cyberspace, edited by Nicholas Tsagourias and Russell Buchan, 2nd ed. Edward Elgar Publishing, 2021. https://doi.org/10.4337/9781789904253.00025.

Roscini, Marco. “Threats of Armed Force and Contemporary International Law.” Netherlands International Law Review 54, no. 2 (2007): 229. https://doi.org/10.1017/S0165070X0700229X.

Roscini, Marco. International Law and the Principle of Non-Intervention: History, Theory, and Interactions with Other Principles. Oxford University Press, 2024. https://doi.org/10.1093/oso/9780198786894.001.0001.

Ruhl, Christian, Wyatt Hoffman, Tim Maurer, and Arthur Nelson. “Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at a Crossroads.” Working Paper. Carnegie Endowment for International Peace, 2020. https://carnegieendowment.org/research/2020/02/cyberspace-and-geopolitics-assessing-global-cybersecurity-norm-processes-at-a-crossroads?lang=en

Ruys, Tom. “Armed Attack” and Article 51 of the UN Charter: Evolutions in Customary Law and Practice. Cambridge University Press, 2010.

Sadurska, Romana. “Threats of Force.” American Journal of International Law 82, no. 2 (1988): 239–68. https://doi.org/10.2307/2203188.

Sandoz, Yves, Claude Pilloud, and Christophe Swinarski, eds. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Martinus Nijhoff Publishers, 1987.

Sassòli, Marco. International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare. Second edition. Edward Elgar Publishing, 2024.

Schmitt, Michael N. “Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention.” International Law Studies 96 (2020).

Schmitt, Michael N. “International Humanitarian Law and the Conduct of Hostilities.” In The Oxford Guide to International Humanitarian Law, edited by Ben Saul and Dapo Akande. Oxford University Press, 2020. https://doi.org/10.1093/law/9780198855309.003.0007.

Schmitt, Michael N. “The Use of Cyber Force and International Law.” In The Oxford Handbook of the Use of Force in International Law, edited by Marc Weller. Oxford University Press, 2016. https://doi.org/10.1093/law/9780199673049.003.0053.

Schmitt, Michael N. “Wired Warfare 3.0: Protecting the Civilian Population during Cyber Operations.” International Review of the Red Cross 101, no. 910 (2019): 333–55. https://doi.org/10.1017/S1816383119000018.

Schmitt, Michael N., and Anusha S. Pakkam. “Cyberspace and the Jus Ad Bellum: The State of Play.” International Law Studies 103, no. 1 (2024): 194–229.

Schmitt, Michael N., and Sean Watts. “Beyond State-Centrism: International Law and Non-State Actors in Cyberspace.” Journal of Conflict and Security Law 21, no. 3 (2016): 595–611. https://doi.org/10.1093/jcsl/krw019.

Schöndorf, Roy. “Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations.” International Law Studies 97, no. 1 (2021): 403. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2957&context=ils

Shackelford, Scott, Scott Russell, and Andreas Kuehn. “Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors.” Chicago Journal of International Law 17, no. 1 (2015): 1–50. https://doi.org/10.2139/ssrn.2652446.

Shaw, Malcolm N. International Law. 8th ed. Cambridge University Press, 2017.

Simma, Bruno, Hermann Mosler, Andreas Paulus, and Eleni Chaitidou eds. The Charter of the United Nations: A Commentary. 3rd edition. Oxford University Press, 2012.

Staker, Christopher. “Jurisdiction.” In International Law, edited by Malcolm Evans, 5th ed. Oxford University Press, 2018. https://doi.org/10.1093/he/9780198791836.003.0010.

Stoddart, Kristan. Cyberwarfare: Threats to Critical Infrastructure. Palgrave Macmillan Cham, 2022. https://doi.org/10.1007/978-3-030-97299-8.

Thirlway, Hugh. The Sources of International Law. 2nd ed. Oxford University Press, 2019.

Thürer, Daniel. “Soft Law.” In The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, vol. IX, 347–351. Oxford: Oxford University Press, 2012.

Treves, Tullio. “Customary International Law.” In The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, vol. II, 937–957. Oxford: Oxford University Press, 2012.

Turns, David. “The Law of Armed Conflict (International Humanitarian Law).” In International Law, edited by Malcolm Evans, 5th ed. Oxford University Press, 2018. https://doi.org/10.1093/he/9780198791836.003.0027.

United Nations Office for Disarmament Affairs. Voluntary Non-Binding Norms for Responsible State Behaviour in the Use of Information and Communications Technology - A Commentary. United Nations, 2018. https://doi.org/10.18356/3c01d394-en.

United Nations Office of Counter Terrorism (UNOCT). The Protection of Critical Infrastructures Against Terrorist Attacks:Compendium of Good Practices. United Nations, 2018. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_of_good_practices_eng.pdf.

United Kingdom. Data Protection Act 2018. King’s Printer of Acts of Parliament. https://www.legislation.gov.uk/ukpga/2018/12/contents

US Department of Defense. The United States Department of Defense Law of War Manual. Updated edition. US Department of Defense, 2020.

Watts, Sean. “Low-Intensity Cyber Operations and the Principle of Non-Intervention.” Baltic Yearbook of International Law 14, no. 1 (2015): 137–61. https://doi.org/10.1163/22115897-90000125.

Ziegler, Kaatja S. “Domaine Réservé.” In The Max Planck Encyclopedia of Public International Law, edited by Rüdiger Wolfrum, 1st ed., vol. 3. Oxford University Press, 2012.

ONLINE SOURCES

British Broadcasting Corporation (BBC). "Russia Internet: Law Introducing New Controls Comes into Force." BBC News, November 1, 2019. https://www.bbc.com/news/world-europe-50259597.

Data Protection Report. "Federal Cybersecurity Information Sharing Act Signed into Law." Data Protection Report, January 4, 2016. https://www.dataprotectionreport.com/2016/01/federal-cybersecurity-information-sharing-act-signed-into-law/.

German Marshall Fund of the United States. "Fact Sheet: What We Know about Russia's Interference Operations." German Marshall Fund of the United States. Accessed May 7, 2025. https://www.gmfus.org/news/fact-sheet-what-we-know-about-russias-interference-operations.

International Cyber Law: Interactive Toolkit. "List of Articles." NATO Cooperative Cyber Defence Centre of Excellence. Accessed September 23, 2025. https://cyberlaw.ccdcoe.org/wiki/List_of_articles.

Pakkam, Anusha. "The Evolving Interpretation of the Use of Force in Cyber Operations: Insights from State Practices." Lieber Institute West Point, November 25, 2024. https://lieber.westpoint.edu/evolving-interpretation-use-of-force-cyber-operations-insights-state-practices/.

Triana, Harold Bertot. "A Customary Rule against Unilateral Economic Sanctions of the Nature of the Helms-Burton Act? Regarding Another (Potential) Vote in the United Nations General Assembly against the 'Bloqueo.'" EJIL: Talk!, October 21, 2024. https://www.ejiltalk.org/a-customary-rule-against-unilateral-economic-sanctions-of-the-nature-of-the-helms-burton-act-regarding-another-potential-vote-in-the-united-nations-general-assembly-against-the-bloqueo/.

United Nations Conference on Trade and Development (UNCTAD). "Global Cyberlaw Tracker." UNCTAD. accessed 12 April 2025. https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide.

Väljataga, Ann. “Back to Square One? The Fifth UN GGE Fails to Submit a Conclusive Report at the UN General Assembly.” NATO Cooperative Cyber Defence Centre of Excellence. Accessed April 1, 2025. https://ccdcoe.org/incyder-articles/back-to-square-one-the-fifth-un-gge-fails-to-submit-a-conclusive-report-at-the-un-general-assembly/.

APPENDICES

A. TABLE OF AUTHORITIES

CASES

Arbitration between Guyana and Suriname (Guyana v. Suriname). Award, September 17, 2007. Permanent Court of Arbitration, PCA Case No. 2004–04.

International Court of Justice. Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro). Judgment of February 26, 2007. I.C.J. Reports 2007.

International Court of Justice. Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda). Judgment of December 19, 2005. I.C.J. Reports 2005.

International Court of Justice. Arrest Warrant of 11 April 2000 (Democratic Republic of the Congo v. Belgium). Judgment of February 14, 2002. I.C.J. Reports 2002.

International Court of Justice. Barcelona Traction, Light and Power Company, Limited (Belgium v. Spain). Judgment of February 5, 1970. I.C.J. Reports 1970.

International Court of Justice. Corfu Channel (United Kingdom v. Albania). Judgment of April 9, 1949. I.C.J. Reports 1949.

International Court of Justice. Legality of the Threat or Use of Nuclear Weapons. Advisory Opinion of July 8, 1996. I.C.J. Reports 1996

International Court of Justice. Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Judgment of June 27, 1986. I.C.J. Reports 1986.

International Court of Justice. Nottebohm Case (Liechtenstein v. Guatemala). Second Phase, Judgment of April 6, 1955. I.C.J. Reports 1955.

International Court of Justice. Oil Platforms (Islamic Republic of Iran v. United States of America). Judgment of November 6, 2003. I.C.J. Reports 2003.

International Criminal Tribunal for the Former Yugoslavia (ICTY). The Prosecutor v. Duško Tadić. Case No. IT-94-1. Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction. October 2, 1995. https://www.icty.org/x/cases/tadic/acdec/en/51002.htm

International Criminal Tribunal for the Former Yugoslavia (ICTY). The Prosecutor v. Mucić et al., Case No. IT-96-21-T. Judgment. November 16, 1998. https://www.icty.org/x/cases/mucic/tjug/en/981116_judg_en.pdf

International Criminal Tribunal for the Former Yugoslavia (ICTY). The Prosecutor v. Haradinaj et al. Case No. IT-04-84-T. Judgment. April 3, 2008. https://www.icty.org/x/cases/haradinaj/tjug/en/080403.pdf

International Criminal Tribunal for the Former Yugoslavia (ICTY). The Prosecutor v. Stanislav Galic. Case No. IT-98-29-T. Trial Judgement. December 5, 2003. https://www.icty.org/x/cases/galic/tjug/en

Island of Palmas (Netherlands v. United States of America). Award of April 4, 1928. 2 Reports of International Arbitral Awards 829.

Liberation Tigers of Tamil Eelam (LTTE) v Council of the European Union. Judgment of 16 October 2014. Case T-208/11. EU:T:2014:885.

Permanent Court of International Justice. Legal Status of Eastern Greenland (Denmark v. Norway). Judgment of April 5, 1933. Series A/B No. 53.

Permanent Court of International Justice. Nationality Decrees Issued in Tunis and Morocco (French Zone). Advisory Opinion of February 7, 1923. Series B No. 4.

Permanent Court of International Justice. The Case of the S.S. “Lotus” (France v. Turkey). Judgment of September 7, 1927. Series A No. 10.

Responsibilities and Obligations of States with Respect to Activities in the Area. Advisory Opinion. International Tribunal for the Law of the Sea, Case No. 17. [2011] ITLOS Reports 10.

EUROPEAN UNION RESOLUTIONS AND OTHER DOCUMENTS

Council of the European Union. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Official Journal of the European Union L 345/75 (2008). http://data.europa.eu/eli/dir/2008/114/oj/eng.

Council of the European Union. Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European Critical Infrastructures and the Assessment of the Need to Improve Their Protection. Official Journal of the European Union L 345/75 (2008). http://data.europa.eu/eli/dir/2008/114/oj/eng.

Council of the European Union. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. Official Journal of the European Union L 333/164 (2022).

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the Resilience of Critical Entities and Repealing Council Directive 2008/114/EC. Official Journal of the European Union L 333/164 (2022). https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation). Official Journal of the European Union L 119 (2016): 1–88.

GENERAL ASSEMBLY RESOLUTIONS AND OTHER DOCUMENTS

International Law Commission. Draft Articles on Responsibility of States for Internationally Wrongful Acts. United Nations, 2001. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf

International Law Commission. Draft Articles on Prevention of Transboundary Harm from Hazardous Activities with Commentaries. United Nations General Assembly, 2001.

International Law Commission. Report of the International Law Commission: Seventy-fourth Session (24 April–2 June and 3 July–4 August 2023). United Nations General Assembly, 2023.

International Law Commission. Report of the International Law Commission Seventy-Fifth Session (29 April–31 May and 1 July–2 August 2024). United Nations General Assembly, 2024. https://legal.un.org/ilc/reports/2024

United Nations General Assembly. Creation of a Global Culture of Cybersecurity and the Protection of Critical Information Infrastructures (A/RES/58/199). United Nations General Assembly, 2004. https://docs.un.org/en/A/RES/58/199

United Nations General Assembly. Declaration on Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations (A/RES/2625). United Nations General Assembly, 1970. https://digitallibrary.un.org/record/202170?v=pdf

United Nations General Assembly. Developments in the Field of Information and Telecommunications in the Context of International Security (A/RES/73/27). United Nations General Assembly, 2018. https://docs.un.org/en/A/res/73/27.

United Nations General 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 Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security Established Pursuant to General Assembly Resolution 73/266 (A/76/136). United Nations, 2021. https://digitallibrary.un.org/record/3933543?v=pdf.

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly, 2013. https://digitallibrary.un.org/record/753055?v=pdf

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN

GGE). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly, 2015. https://digitallibrary.un.org/record/799853?v=pdf

United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE). Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. United Nations General Assembly, 2021. https://digitallibrary.un.org/record/3934214?v=pdf

United Nations Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG). Final Substantive Report. United Nations General Assembly, 2021. https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

NATIONAL AND SHARED POSITIONS

African Union Peace and Security Council. Common African Position on the Application of International Law to the Use of Information and Communication Technologies in Cyberspace. African Union, 2024. https://papsrepository.africanunion.org/server/api/core/bitstreams/65bdfced-80d9-445b-b57f-31037616ccda/content.

Council of the European Union. Declaration on a Common Understanding of International Law in Cyberspace. European Union, 2024. https://data.consilium.europa.eu/doc/document/ST-15833-2024-INIT/en/pd

Federal Government of Germany. On the Application of International Law in Cyberspace. Federal Government of Germany, 2021. https://www.auswaertiges-amt.de/resource/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf

Federal Ministry for European and International Affairs of Republic of Austria. Position Paper of the Republic of Austria: Cyber Activities and International Law. Federal Ministry for European and International Affairs of Republic of Austria, 2024.

International Committee of Red Cross (ICRC). International Humanitarian Law and Cyber Operations during Armed Conflicts: ICRC Position Paper. ICRC, 2019. https://www.icrc.org/sites/default/files/document/file_list/icrc_ihl-and-cyber-operations-during-armed-conflicts.pdf

Government of Canada. International Law Applicable in Cyberspace. Government of Canada, 2022. https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a4

International Cyber Law: Interactive Toolkit. “National Position of Cuba (2024).” NATO Cooperative Cyber Defence Centre of Excellence. January 31, 2025. https://cyberlaw.ccdcoe.org/wiki/National_position_of_Cuba_(2024).

Ministry of Armed Forces of the French Republic. International Law Applied to Operations in Cyberspace. Ministry of Armed Forces, 2019. https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf

Ministry of Foreign Affairs and International Cooperation of the Italian Republic. Italian Position Paper on International Law and Cyberspace. Ministry of Foreign Affairs and International Cooperation of the Italian Republic, 2021. https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberspace.pdf

Ministry of Foreign Affairs and Trade of New Zealand. The Application of International Law to State Activity in Cyberspace. Ministry of Foreign Affairs and Trade of New Zealand, 2020. https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf

Ministry of Foreign Affairs of Colombia. Colombia's National Position on the Application of International Law in Cyberspace. Ministry of Foreign Affairs of Colombia, 2025. https://static.wikitide.net/cyberlawwiki/0/0a/Colombia_-_NP_Cyber_PDF_Ingles.pdf

Ministry of Foreign Affairs of Finland. International Law and Cyberspace. Ministry of Foreign Affairs of Finland, 2020. https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727

Ministry of Foreign Affairs of Japan. Basic Position of the Government of Japan on International Law Applicable to Cyber Operations. Ministry of Foreign Affairs of Japan, 2021. https://www.mofa.go.jp/files/100200935.pdf

Ministry of Foreign Affairs of the Czech Republic. Position Paper on the Application of International Law in Cyberspace. Ministry of Foreign Affairs of the Czech Republic, 2024. https://mzv.gov.cz/file/5376858/_20240226___CZ_Position_paper_on_the_application_of_IL_cyberspace.pdf

Ministry of Foreign Affairs of the People's Republic of China. China's Positions on International Rules-Making in Cyberspace. Ministry of Foreign Affairs of the People's Republic of China, 2021. https://www.fmprc.gov.cn/eng/wjb/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/202406/t20240606_11405183.htm

Ministry of Foreign Affairs of the People's Republic of China. China's Views on the Application of the Principle of Sovereignty in Cyberspace. Ministry of Foreign Affairs of the People's Republic of China, 2021. https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

Ministry of Foreign Affairs of the Republic of Poland. The Republic of Poland's Position on the Application of International Law in Cyberspace. Ministry of Foreign Affairs of the Republic of Poland, 2022. https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace

SECURITY COUNCIL RESOLUTIONS AND OTHER DOCUMENTS

United Nations Security Council. Resolution 2341 (S/RES/2341). United Nations Security Council, 2017. https://docs.un.org/en/S/RES/2341(2017)

TREATIES

Charter of the United Nations and Statute of the International Court of Justice. Signed June 26, 1945. 1 U.N.T.S. XVI.

Council of Europe. Convention on Cybercrime (ETS No. 185). Budapest, 23 November 2001. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field. Opened for signature August 12, 1949. 75 U.N.T.S. 31.

Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II). Opened for signature June 8, 1977. 1125 U.N.T.S. 609.

Protocol Additional to the Geneva Conventions of 12 August 1949 and Relating to the Protection of Victims of International Armed Conflicts (Protocol I). Opened for signature June 8, 1977. 1125 U.N.T.S. 3.

Statute of the International Court of Justice. June 26, 1945. 33 U.N.T.S. 993.

Vienna Convention on the Law of Treaties. May 23, 1969. 1155 U.N.T.S. 331.

B. TURKISH SUMMARY / TÜRKÇE ÖZET

Bu tez, modern toplumların işleyişi açısından hayati öneme sahip olan kritik altyapılarım, siber sahada maruz kaldıkları tehditler karşısında uluslararası hukuk tarafından nasıl korunabileceğini incelemektedir. 21.yüzyılın başından itibaren bilgi ve iletişim teknolojilerinde yaşanan devrim niteliğindeki gelişmeler, insanlık tarihinin en büyük dönüşümlerinden biri olan dijitalleşmeyi beraberinde getirmiştir. Başlangıçta sınırlı bir çevrede veri paylaşımı amacıyla kullanılan internet, günümüzde devletlerin, toplumların ve bireylerin varlıklarını sürdürebilmeleri için vazgeçilmez bir ekosistem haline gelen, fiziksel sınırların ötesine geçen, devasa verilerin saniyeler içinde aktarılabildiği ve geleneksel mekân algısını değiştiren siber sahayı doğurmuştur. Siber saha, 21.yüzyılın ikinci yarısındaki ortaya çıkışından bu yana sınırlı bir bilgi paylaşım ağından insan yaşamının hemen hemen her yönünü etkileyen küresel bir beşinci alana dönüşmüştür. Bu alanın sosyal, ekonomik ve politik alanlarla artan entegrasyonu; yapay zekâ, nesnelerin interneti, blok zincir, bulut bilişimi ve kuantum bilişimi gibi yeni teknolojilerle daha da derinleşmekte ve modern toplumların günlük işleyişinin ayrılmaz bir parçası haline gelmektedir. Bu dijital evrim; sosyal, ekonomik ve siyasi alanların siber sahayla derinlemesine bütünleşmesine yol açarak modern toplumların işleyiş biçimini temelden değiştirmiştir. Buna paralel olarak siber saha, toplumun refahı, sağlığı ve devletin temel fonksiyonlarının sürdürülmesi için vazgeçilmez olan enerji, sağlık, ulaşım, finans ve iletişim gibi kritik altyapılarla giderek daha da bütünleşmektedir. Kritik altyapılar, toplumun refahı, sağlıklı işleyişi ve devletin bekası için vazgeçilmez olan hizmetleri sunan stratejik varlıklar ve sistemler bütünü olarak nitelendirilmektedir. Uluslararası hukukta genel kabul görmüş bir kritik altyapı tanımı bulunmamakta, kritik altyapıları tanımlama ve belirleme yetkisi devletlerin takdirine bırakılmaktadır.

Kritik altyapıların siber saha ile bütünleşmesi, bir yandan verimlilik ve işlevsellik sağlarken, diğer yandan bu altyapıları siber operasyonlara karşı son derece kırılgan hale getirmektedir. Siber operasyonlar, artık sadece birer veri hırsızlığı veya sistem

yavaşlatma aracı değil, fiziksel dünyada kitlesel ölümlere, ekonomik çöküşlere ve toplumsal kaosa yol açabilecek kapasiteye sahip stratejik silahlara dönüşmüştür. Nitekim tarihsel süreçte gerçekleşen 2010 Stuxnet saldırısı, 2015 Ukrayna Elektrik Şebekesi saldırısı ve 2021 Colonial Pipeline hadisesi, kritik altyapıların dijital dünyadaki kırılganlığının fiziksel dünyada ne denli yıkıcı sonuçlar doğurabileceğini kanıtlamıştır. Kritik altyapıların birbirine bağlı doğası, bir altyapıda gerçekleşen kesintisinin domino etkisi yaratarak diğer sistemleri de felce uğratması riskini taşımaktadır. Kapsamlı bir uluslararası hukuki rejimin eksikliği ve mevcut kuralların siber sahaya uygulanmasında ortaya çıkan gri alanlar, kritik altyapıları hem devletler hem de devlet dışı aktörler için cazip ve düşük maliyetleri hedefler haline getirmektedir. Bu sebeple, siber sahada uluslararası hukuk kurallarının kapsam ve uygulamasındaki muğlaklıkları gidermek, kritik altyapıların korunması için önem arz etmektedir. Bu bağlamda tez, siber sahanın hukuki statüsü ve uluslararası hukuk kurallarının bu alana uygulanabilirliği üzerinden kritik altyapıların korunmasına yönelik kapsamlı bir analiz sunmaktadır.

Siber sahanın hukuki statüsü üzerindeki tartışmalar, bu sahanın ilk yıllarında bağımsızlık ve anarşi fikirleri etrafında şekillenmiş olsa da yıllar içinde bu görüşler yerini devlet merkezli bir hukuki yapıya bırakmıştır. Yıllar içerisinde siber sahanın hukuki bir boşluk içinde olmadığını, aksine uluslararası hukukun temel kural ve ilkelerinin siber sahada da geçerli olduğu fikri devletlerce genel kabul görmüştür. Bu sebeple tez, siber sahanın bir hukuk boşluğu içinde var olmadığını, aksine mevcut uluslararası hukuk çerçevesi tarafından yönetilen bir alan olduğu temel önermesi üzerine inşa edilmiştir. Bununla birlikte, siber alanın sahip olduğu anomimlik, sınır tanımazlık ve yüksek düzeyli bağımlılık gibi ayrıcı özellikler, başlangıcında fiziki alanlar için yaratılan uluslararası hukuk kurallarının nasıl uygulandığı konusunda ciddi bir yorum boşluğu yaratmaktadır. Bu minvalde tezin temel araştırma sorusu, mevcut uluslararası hukuk kurallarının siber operasyonlara karşı kritik altyapıları korumak için nasıl yorumlanabileceği ve uygulanabileceğidir. Bu kuralların siber sahanın kendine özgü özellikleri nedeniyle yorumlanması ve uygulanmasında çeşitli zorluklar ve görüş ayrılıkları bulunmaktadır. Tez, bu zorlukları ve farklı devlet yaklaşımlarını analiz ederek, uluslararası hukukun siber sahadaki düzenleyici rolünü ortaya koymayı amaçlamaktadır.

Uluslararası hukuk kurallarının siber sahadaki kapsamını netleştirmek; devlet davranışlarının sınırlarını tanımlamak ve sınır aşan siber tehditlerle mücadelede iş birliğini teşvik etmek açısından kritik öneme sahiptir. Bu minvalde, tezde Uluslararası Adalet Divanı Statüsü'nün 38/1.maddesinde uluslararası hukukun birincil kaynakları olarak zikredilen uluslararası andlaşmalar, uluslararası teamül hukuku ve hukukun genel ilkeleri esas alınmış; yargı kararları ve Tallinn Kılavuzu gibi akademik çalışmalar da yardımcı araçlar olarak kullanılmıştır. Siber saha için özel ve kapsamlı bir küresel rejim bulunmadığından ötürü kritik altyapıların korunması Birleşmiş Milletler Şartı ve 1949 Cenevre Sözleşmeleri gibi temel belgelerin evrimsel yorumu yoluyla sağlanmaktadır. Ayrıca, devletlerin sorumlu davranışlarına ilişkin kolektif beklentileri ifade eden ve yumuşak hukuk olarak adlandırılan bağlayıcı olmayan siber normlar, özellikle Birleşmiş Milletler bünyesindeki Hükümet Uzmanları Grubu (GGE) ve Açık Uçlu Çalışma Grubu (OEWG) süreçleri aracılığıyla, bu alanda uluslararası bir mutabakatın kristalleşmesine yardımcı olmaktadır.

Tezin giriş bölümünde siber sahanın uluslararası ilişkilerdeki artan önemi ve kritik altyapılarla olan ilişkisi ele alınmakta; çalışmanın amacı, kapsamı ve araştırma sorusu ortaya konulmaktadır. Bu bağlamda tezin araştırma sorusu, mevcut uluslararası hukuk kurallarının kritik altyapıları siber operasyonlara karşı korumak amacıyla nasıl yorumlanıp uygulanabileceğidir.

Tezin ikinci bölümünde uluslararası hukukun siber sahada uygulanabilirliği ve özellikle devlet yetkisi kavramı incelenmektedir. Bu bölümde ayrıca uluslararası hukukun siber sahada uygulanmasına ilişkin tarihsel süreçteki tartışmalar ve Birleşmiş Milletler başta olmak üzere çeşitli platformlarda yürütülen süreçler anlatılmıştır. Siber sahada uluslararası hukukun uygulanabilirliği, Birleşmiş Milletler nezdindeki GGE ve OEWG süreçlerinde şekillenmiştir. 2013 ve 2015 yılında ortaya çıkan GGE raporları, Birleşmiş Milletler Şartı'nın siber sahaya bütünüyle uygulandığını ve devlet egemenliğinin siber faaliyetler için temel teşkil ettiğini teyit ederek tarihi bir uzlaşma sağlamıştır. Ancak 2017'deki beşinci GGE sürecinin meşru müdafaa hakkı, uluslararası insancıl hukuk ve karşı önlemler konularının siber sahadaki uygulaması ve sınırları konusundaki kutuplaşma nedeniyle başarısızlıkla sonuçlanmıştır. 2021 yılında yayımlanan GGE ve OEWG raporları bu gerilimi yumuşatarak hukukun siber

sahada bir boşluk yaratmadığını yinelemiştir. Bunun yanında, 2015 GGE raporuyla kabul edilen 15 norm, devletlerin siber sahadaki asgari davranış standartlarını ifade etmektedir. Bu normlar hukuken bağlayıcı olmasa da zamana bir *opinio juris* oluşturarak teamül hukuku kuralına dönüşme potansiyeli taşımaktadır. Kritik altyapıların korunması hususu ilgili normlarda önemli bir yer tutmuştur. Bu minvalde 2015 GGE raporuyla ilan edilen f normu devletlerin kritik altyapılara kasten zarar vermemesini, g normu kendi kritik altyapılarını korumak için çerçeveler oluşturmasını ve h normu ise başka bir devletin kritik altyapılarına yönelik saldırıları engellemek için devletler arası iş birliğinin yapılmasını öngörmektedir. Ayrıca, i normu tedarik zinciri güvenliğini, j normu zafiyetlerin bildirilmesini ve k normu acil müdahale ekiplerinin korunmasını düzenleyerek kritik altyapıların korunması konusunda bütüncül bir koruma kalkanı oluşturmayı hedeflemiştir.

Devlet egemenliği, uluslararası hukuk sisteminin temelini oluşturmakta olup, devletlerin kendi sınırları içerisindeki kişi, mal ve olaylar üzerinde düzenleme ve denetim yetkisini ifade etmektedir. Bu çerçevede yetki kavramı yasama, icra ve yargılama yetkisi olmak üzere üç temel kategoriye ayrılmaktadır. Yasama yetkisi, devletin hukuk kuralları koyma gücünü, icra yetkisi devletçe konulan hukuk kurallarını devletin idari veya cevri yollarla uygulama yetkisini ifade ederken yargılama yetkisi de hukuki uyuşmazlıkların mahkemeler eliyle çözülmesini ifade etmektedir. İcra yetkisi, kesin bir şekilde ülkesellik ilkesine bağlıyken ve devletler başka bir devletin rızası olmaksızın yabancı devletlerin topraklarında bu yetkiyi kullanamazken, yasama yetkisinin sınırları daha esnek bir tartışma zeminindedir. Uluslararası Sürekli Adalet Divanı tarafından *Lotus* davasında ortaya konan "serbesiyetçi yaklaşım," devletlerin uluslararası hukuk tarafından açıkça yasaklanmadığı sürece yetkilerini ülke dışındaki kişi ve olaylara genişletebileceğini savunurken günümüz modern uluslararası hukukunda daha çok kabul gören "kısıtlayıcı yaklaşım", devletlerin ancak uluslararası hukukça tanınmış meşru bir dayanak çerçevesinde yetki kullanabileceğini öngörmektedir. Tez, kısıtlayıcı yaklaşımı benimsemekte olup bu doğrultuda devlet yetkisi türlerinin siber saha bağlamında nasıl işlediğini analiz etmektedir.

Uluslararası hukukta yetki kullanımının temel dayanakları mülkilik, şahsilik, koruma ve evrensellik ilkeleridir. Mülkilik ilkesi, devletlerin kendi sınırları içerisinde mutlak yetkiye sahip olduğunu ifade ederken, şahsilik ilkesi devletlerin vatandaşları üzerinde sınır ötesi yetki kullanabilmesini mümkün kılmaktadır. Koruma ilkesi, devletlerin ulusal güvenliklerini tehdit eden eylemler karşısında yetki kullanmalarına olanak tanırken, evrensellik ilkesi belirli ağır suçlar bakımından tüm devletlere yetki tanımaktadır.

Devletler, uluslararası hukukun izin verdiği sınırlar dahilinde yasama, yargı ve icra yetkilerini siber sahada da kullanma hakkına sahiptir. Siber sahadaki yetki iddiaları, mülkilik, şahsilik, koruma ya da evrensellik ilkelerine dayandırılmalıdır. Mülkilik ilkesi uyarınca bir devlet, kendi topraklarında bulunan siber altyapı ve bu altyapıyı kullanan kişiler üzerinde yetkiye sahiptir. Ayrıca, bir siber eylemin etkilerinin bir devletin topraklarında meydana gelmesi durumunda etki doktrini uyarınca da yargı yetkisi tesis edilebilmektedir. Şahsilik ilkesi, devletlerin kendi vatandaşlarının siber faaliyetleri üzerinde, nerede olurlarsa olsunlar yetki sahibi olmalarını sağlamaktadır. Şahsilik ilkesi uyarınca devletler, dünyanın neresinde olursa olsun kendi vatandaşlarının veya kendi ülkesinde kayıtlı tüzel kişilerin gerçekleştirdiği siber eylemler konusunda yetkilidir. Bu bağ, egemen ve tebaa arasındaki karşılıklı hak ve ödevlere dayanmaktadır. Koruma ilkesi, failin uyruğuna ve eylemin gerçekleştirildiği yere bakılmaksızın devletin güvenliği, para birimi veya bankacılık sistemi gibi hayati çıkarlarını tehdit eden siber eylemlere karşı devletin yetki kullanmasına izin verir. Evrensellik ilkesi ise siber sahanın soykırım veya savaş suçları gibi tüm insanlığı ilgilendiren suçların işlenmesinde kullanılması durumunda, failin konumundan bağımsız olarak her devlete yargı yetkisi tanır.

Tezin üçüncü bölümünde kritik altyapının barış zamanında uluslararası hukuk kapsamında nasıl korunabileceğini analiz etmektedir. Bu kapsamda egemenlik, müdahale etmeme, özen yükümlülüğü ve kuvvet kullanma yasağı gibi temel uluslararası hukuk kuralları incelenmektedir.

Egemenlik, devletin kendi toprakları üzerinde münhasır yetkiye sahip olduğunu ifade eder ve siber sahada da tam olarak uygulanabilir bir kuraldır. Egemenliğin siber

sahadaki kapsamı konusunda iki ayrı görüş bulunmaktadır. Bir tarafta egemenliği başlı başına ihlal edilebilir bağımsız bir hukuk kural olarak gören "kuralcı yaklaşım", diğer tarafta ise egemenliği yalnızca müdahale yasağı gibi diğer kuralların temelini oluşturan genel bir ilke olarak kabul eden ve ancak bu kuralların ihlal eşiği aşıldığında ihlalden söz eden "ilkesel yaklaşım" görüşü bulunmaktadır. Tez, egemenliğin sadece betimleyici bir ilke değil, aynı zamanda ihlali hukuki sorumluluk doğuran bağlayıcı bir kural olduğunu savunmaktadır. Egemenlik kuralı uyarınca, bir devletin rızası olmaksızın topraklarındaki dijital sistemlere müdahale edilmesi ve bu müdahalenin fiziksel hasar ya da işlev kaybına yol açması egemenliğin ihlali olarak kabul edilmelidir. Ayrıca, seçim sistemleri veya vergi toplama gibi doğası gereği devlete ait fonksiyonların siber yolla engellenmesi veya gasp edilmesi de egemenliğin ihlalini teşkil eder.

Müdahale etmeme kuralı uyarınca, bir devletin başka bir devletin başka bir devletin egemenlik alanına giren konularda zorlayıcı müdahalede bulunması yasaktır. Bu kural, bir devletin başka bir devletin iç ve dış işlerine siber araçlarla müdahale etmesini yasaklamaktadır. Bir siber operasyonun bu kuralı ihlal etmesi için ilgili siber eylemin münhasıran devletin egemenlik alanına giren bir konuya yönelik olması ve bu eylemin zorlama unsuru içermesi gerekmektedir. Kritik altyapılara yöneltilen siber operasyonlar, doğası gereği devletin temel fonksiyonlarını yerine getirmesini engelleyerek veya devlet iradesini belirli bir yönde zorlayarak bu yasağı ihlal etme potansiyeline sahiptir. Bu çalışma, sağlık hizmetleri, finansal sistemler veya enerji şebekeleri gibi temel kamu hizmetlerini hedef alan siber operasyonların, bir devleti egemen tercihlerinden mahrum bıraktığı için doğası gereği zorlayıcı olduğunu ve bu nedenle müdahale etmeme kuralının bir ihlalini teşkil ettiğini savunmaktadır.

Özel yükümlülüğü ise devletlerin kendi topraklarının ya da kontrolü altındaki altyapıların diğer devletlere zarar verecek şekilde kullanılmasını engelleme yükümlülüğünü ifade etmektedir. Siber sahada bu yükümlülük, bir devletin topraklarında bulunan ağ ve sunuculardan başka bir devletin kritik altyapısına yönelik bir siber operasyon gerçekleştiriliyorsa, toprak sahibi devletin bu durumu öğrendiğinde ya da bilmesi gerektiğinde ilgili eylemi durdurmak için makul önlemleri almasını şart koşar. Atıf sorununun kronik olduğu siber sahada bu yükümlülük, bir

hukuki dengeleyici işlevini görerek, operasyonu durdurmayan veya önlemeyen devletin sorumluluğuna gitmeyi mümkün kılar.

Kuvvet kullanma yasağı, uluslararası hukukun en temel kurallarından biri olup, devletlerin birbirlerine karşı kuvvet kullanmasını yasaklamaktadır. Bu kural kapsamında siber operasyonların fiziksel saldırılarla benzer ölçek ve etkilere sahip olması durumunda bu yasağın ihlal edildiği kabul edilmelidir. Bu analizde benimsenen sonuç odaklı yaklaşım, teknik yöntemden ziyade operasyon tarafından yaratılan etkiye odaklanarak hukukun teknolojik gelişmelere uyum sağlamasını mümkün kılar. Bu bağlamda siber araçlarla gerçekleştirilen bir operasyonun ölçeği ve yarattığı etkiler itibarıyla fiziksel bir saldırıyla aynı sonuçları doğurması durumunda kuvvet kullanma yasağının ihlal edildiği kabul edilmelidir. Öte yandan, bir siber operasyonun kuvvet kullanmanın en ağır çeşidi olan silahlı saldırı eşiğini aşması, hedef devletin meşru müdafaa hakkını doğurarak askeri güçlü karşılık verme yetkisi tanır. Silahlı saldırı eşiği, kuvvet kullanma yasağının ihlalinden daha yüksektir. Tez, kritik altyapılara yönelik siber operasyonların sadece fiziksel yıkım durumunda değil, devletin hayati fonksiyonlarını uzun süreli ve geniş çaplı olarak devre dışı bıraktığı durumların da silahlı saldırı olarak kabul edilmesi gerektiğini, zira modern dünyada böylesi bir durumun fiziksel yıkımdan daha ağır sonuçlara yol açabileceğini vurgulamaktadır.

Tezin dördüncü bölümü silahlı çatışma durumlarında kritik altyapıların korunmasını ele almaktadır. Silahlı çatışma durumlarında kritik altyapıların korunması uluslararası insancıl hukuk tarafından düzenlenir. Uluslararası insancıl hukuk kurallarının uygulanabilmesi için siber operasyonun bir silahlı çatışma bağlamında gerçekleştirilmesi veya tek başına çatışma başlatacak nitelikte olması gerekir. İnsancıl hukuktaki saldırı tanımı, bu çalışmada insancıl amaçlar doğrultusunda geniş şekilde yorumlanmaktadır. Sadece fiziki hasar değiş, bir enerji şebekesi veya su sisteminin işlevselliğini yitirmesi de sivil halk üzerindeki yıkıcı etkileri göz önüne alındığında hukuken bir saldırı olarak kabul edilmelidir. Tez, siber saldırıların da kendi başına saldırı eşiğine ulaşabileceğini gösterdikten sonra uluslararası insancıl hukukun temel kuralları olan ayrım gözetme, orantılılık ve ihtiyat ilkelerinin silahlı çatışma durumlarında kritik altyapıları nasıl koruyabileceğini analiz etmektedir. Bu üç ilke bir bütün olarak, siber sahanın teknik doğasından kaynaklanan riskleri sınırlayan ve kritik

altyapıları silahlı çatışma dönemlerinde koruyan kapsamlı bir hukuki çerçeve sunmaktadır.

Uluslararası insancıl hukukun temel taşlarından birisini teşkil eden ayrım gözetme ilkesi, sivilleri ve sivil nesneleri çatışmaların etkilerinden korumayı amaçlayarak muharip olanlarla olmayanları birbirinden ayırır. Bu minvalde ilke, saldırıların sadece askeri hedeflere yöneltilmesini, sivillerin ve sivil nesnelerin korunmasını emreder. Bu ilke hem uluslararası hem de uluslararası olmayan silahlı çatışmalarda geçerli olan ve ihlali maruz görülemeyecek bir teamül hukuku kuralıdır. Ayrım gözetme ilkesi uyarınca sivillere ve sivil nesnelere yönelik doğrudan saldırı yapılması kesin olarak yasaktır ve bu ilkenin ihlali savaş suçu teşkil etmektedir. Bir nesnenin meşru olarak hedef alınabilir askeri bir hedef sayılabilmesi için doğası, konumu, amacı veya kullanımı yoluyla askeri operasyona etkin bir katkı sağlaması ve imha edilmesinin operasyon anındaki koşullarda kesin bir askeri avantaj kullanımı gerekmektedir. Normalde sivil amaçlara hizmet eden bir nesnenin askeri amaçla kullanıp kullanılmadığı konusunda tereddüte düşüldüğü durumlarda o nesnenin sivil olduğu varsayılmalıdır. Ayrıca, belirli bir askeri hedefi hedef almayan veya etkileri sınırlandırılamayan saldırılar da hukuksuzdur. Bunun yanında uluslararası insancıl hukuk, bazı nesne kategorilerine taşıdıkları önem nedeniyle özel koruma sağlamaktadır. Bu nesneler sırasıyla tıbbi birimler, sivil halkın yaşamını sürdürebilmesi için vazgeçilmez olan nesneler ve tehlikeli unsurları barındıran yapı ve tesislerdir. Ayrım gözetme ilkesi, siber sahada da geçerlidir. Bu doğrultuda siber araçlar ve yöntemler kullanılarak sivillere veya sivil nesnelere doğrudan saldırı düzenlenmesi yasaktır.

Siber sahanın çok yüksek oranda sivil ağlar üzerinden aktığı ve askeri sistemlerin sivil altyapı ile iç içe geçtiği çift kullanımlı bir ortamda bu ilkenin uygulanmasında çeşitli zorluklar yaşanmaktadır. Bunlardan ilki, altyapının büyük oranda çift amaçlı olmasıdır. Bu çalışma, bir altyapının kısmen askeri amaçlarla kullanılmasının tüm ağın hedef alınmasına izin vermediğini, saldırganın sadece ayrılabilir ve spesifik askeri bileşenleri hedeflemekle yükümlü olduğunu savunmaktadır. Diğer bir tartışmalı konu ise verinin nesne statüsüdür. Her ne kadar bazı görüşler verinin somut olmadığından dolayı nesne olarak sayılmaması gerektiğini ileri sürse de giderek artan bir şekilde

dijitalleşen dünyada sivil yaşamın banka kayıtları, sağlık verileri ve seçim kayıtları gibi verilere olan bağımlılığı göz önüne alındığında, verinin insancıl hukuk bağlamında bir nesne olarak kabul edilmesi ve uluslararası insancıl hukukun sunduğu korumadan yararlanması gerektiği sonucuna varılmıştır.

Orantılılık ilkesi, meşru bir askeri bir hedefe yöneltilen operasyonun sivil halk üzerinde yaratacağı zararın elde edilecek somut askeri avantajla kıyaslandığında aşırı olmamasını gerektirmektedir. Bu minvalde orantılılık değerlendirmesi, ilgili operasyonu planlayanların ve yürütenlerin mevcut makul bilgilerin tamamını kullanarak iyi niyet ve özenle yapmaları gereken bir denge analizidir. Sivillerin konumu, kullanılacak araç ve yöntemlerin hassasiyeti ve operasyonun dolaylı etkileri de orantılılık değerlendirmesi sırasında hesaba katılmalıdır. Bunun yanı sıra operasyon sonucunda elde edilmesi beklenen askeri avantaj somut, doğrudan ve algılanabilir olmalı; varsayımsal ya da uzun erimli avantajlar bu kapsamda değerlendirilmemelidir. İlke, çatışmanın tüm taraflarını bağlamaktadır. Siber operasyonlarda sadece ölüme veya fiziksel hasara yol açan eylemler değil, sivil altyapının işlev kaybına uğraması da orantılılık değerlendirmesi kapsamında yer almalıdır. Özellikle kritik altyapıların hedef alınması durumunda, sivil hizmetlerdeki aksamaların yaratacağı zarar beklenilen askeri avantajın önüne geçecektir. Siber sahanın yüksek düzeyde birbiriyle bağlantılı yapısı sebebiyle, bir siber operasyonun doğrudan etkisi ötesindeki tüm öngörülebilir dolaylı zararlar da bu hesaplamaya dahil edilmelidir.

İhtiyat ilkesi ise hem saldırganın hem de savunan tarafın çatışmalarda sivillerin görebileceği zararı asgari seviyeye indirmek için azami gayret göstermelerini zorunlu kılmaktadır. Bu ilke kapsamında, saldıran tarafın uyması gereken aktif önlemler ve savunma tarafının uyması gereken pasif önlemler bulunur. Saldıran taraf, hedefin saldırmanın yasak olduğu sivil bir hedef olup olmadığını doğrulamak için elindeki tüm imkanları kullanmalı, sivillere en az zararlı yöntem ve araçları seçmeli ve gerektiğinde sivilleri korumak için saldırı öncesi etkili uyarılar yapmalıdır. Eğer saldırının orantısız olacağı veya hedefin sivil olduğu anlaşılırsa saldırı iptal edilmeli ya da durdurulmalıdır. Ayrıca, şartlar elverdiği sürece sivil nüfusa saldırı öncesinde etkili ön uyarıda bulunulmalıdır. Saldıran taraf ayrıca benzer bir askeri avantaj sağlayacak hedefler arasından sivillere en az tehlike arz edebi seçmelidir. Savunan taraf ise pasif

önlemler kapsamında askeri ve sivil ağları birbirinden ayırmak ve kritik verileri yedeklemek gibi önlemler almalıdır. İhtiyat ilkesi, kritik altyapıların korunması bağlamında saldıran tarafından hedeflediği altyapının sivil nesne olup olmadığını ya da özel koruma altında olmadığını doğrulamak için en iyi istihbaratı kullanmasını, çift kullanımlı bir altyapının hedef alındığı durumlarda tüm altyapı yerine yalnızca askeri bileşenlerin hedef alınmasını, operasyonun zamanlamasının sivil zararı azaltacak şekilde belirlenmesini, şartlar elverdiği durumlarda internet ya da mesajlaşma uygulamaları gibi kanallarla etkin uyarılar yapılmasını, kritik altyapıların askeri ağ ve altyapılardan ayrılması gibi önlemlerin alınmasını gerektirmektedir.

Sonuç olarak tez, uluslararası hukukun mevcut haliyle kritik altyapıların siber sahada korunması için önemli ve işlevsel bir çerçeve sunduğunu ortaya koymaktadır. Uluslararası hukukun klasik kaynakları olan andlaşmalar, teamül hukuku ve hukukun genel ilkelerinden türeyen türeyen kurallar; siber sahanın anonimlik, sınır tanımazlık ve çok aktörlülük gibi münhasır ve dinamik özelliklerine rağmen uygulanabilirliğini korumakta; Viyana Andlaşmalar Hukuku Sözleşmesi'nin öngördüğü evrimsel yorum yöntemiyle bu yeni sahaya adapte edilebilmektedir. Bu durum, siber sahanın hukuki bir boşluk olmadığı, aksine mevcut hukuk düzeninin kapsamı içimde yer aldığı yönündeki temel önermeyi doğrulamaktadır. Bu bağlamda siber sahada kritik altyapıların korunması, tek bir kurala değil, egemenlikten insancıl hukuka kadar uzanan çok katmanlı bir hukuki çerçeveye dayanmaktadır. Bu çok katmanlı yapı, uluslararası hukukun farklı alanlarının birbirini tamamlayıcı şekilde işleyerek siber tehditlere karşı bütüncül bir koruma sağladığını göstermektedir. Mevcut uluslararası hukuk, dinamik ve evrimsel bir yorumla siber gerçekliklere uyarlandığında, kritik altyapıları korumak için yeterli ve esnek bir zemin sağlamaktadır. Bu bağlamda tez, mevcut hukuk kurallarının uygun yorum ve uygulamalarla siber sahada da etkin bir şekilde kullanılabileceğini savunmaktadır.

Bununla birlikte tez, siber sahanın düzenlenmesinde temel sorunun yeni kuralların eksikliği değil, mevcut kuralların yorumlanması ve uygulanması konusundaki belirsizlikler olduğunu ortaya koymaktadır. Devletler arasında çeşitli kurallar konusunda süregelen görüş ayrılıkları, uluslarasın hukukun uygulanmasında yeknesaklığın sağlanmasını zorlaştırmaktadır. Bu nedenle siber sahada istikrar ve

öngörülebilirliğin arttırılması, büyük ölçüde devletlerin var olan kuralları iyi niyetli, tutarlı ve sorumlu bir şekilde yorumlamalarına bağlıdır. Bu doğrultuda tez, uluslararası hukukun kritik altyapıların korunmasında merkezi bir rol oynamaya devam edeceğini ileri sürmektedir.

C. THESIS PERMISSION FORM / TEZ İZİN FORMU

(Please fill out this form on computer. Double click on the boxes to fill them)

ENSTİTÜ / INSTITUTE

Fen Bilimleri Enstitüsü / Graduate School of Natural and Applied Sciences ☐

Sosyal Bilimler Enstitüsü / Graduate School of Social Sciences ☒

Uygulamalı Matematik Enstitüsü / Graduate School of Applied Mathematics ☐

Enformatik Enstitüsü / Graduate School of Informatics ☐

Deniz Bilimleri Enstitüsü / Graduate School of Marine Sciences ☐

YAZARIN / AUTHOR

Soyadı / Surname : Pur
Adı / Name : Ahmet Semih
Bölümü / Department : Uluslararası İlişkiler / International Relations

TEZİN ADI / TITLE OF THE THESIS (**İngilizce** / English): Legal Protection of Critical Infrastructures in Cyberspace

TEZİN TÜRÜ / DEGREE**:** **Yüksek Lisans** / Master ☒ **Doktora** / PhD ☐

1. **Tezin tamamı dünya çapında erişime açılacaktır. /** Release the entire work immediately for access worldwide. ☒
2. **Tez iki yıl süreyle erişime kapalı olacaktır.** / Secure the entire work for patent and/or proprietary purposes for a period of **two years. *** ☐
3. **Tez altı ay süreyle erişime kapalı olacaktır.** / Secure the entire work for period of **six months**. ***** ☐

***** *Enstitü Yönetim Kurulu kararının basılı kopyası tezle birlikte kütüphaneye teslim edilecektir. / A copy of the decision of the Institute Administrative Committee will be delivered to the library together with the printed thesis.*

Yazarın imzası / Signature ..... **Tarih** / Date .....
(Kütüphaneye teslim ettiğiniz tarih. Elle doldurulacaktır.)
(Library submission date. Please fill out by hand.)

Tezin son sayfasıdır. / This is the last page of the thesis/dissertation.