VILNIUS UNIVERSITY

Alaa
Al Dakour Al Aridi

The Problem of Hybrid War in International Law

DOCTORAL DISSERTATION

Social Sciences,
Law (S 001)

VILNIUS 2022

The dissertation was prepared between 2015 and 2022 at Vilnius University.

Academic supervisor – Prof. Dr. Dainius Žalimas
(Vilnius University, Social Sciences, Law – S 001, from 2015.10.01 till 2019.09.25),
Academic supervisor – Prof. Habil. Dr. Gintaras Švedas
(Vilnius University, Social Sciences, Law – S 001, from 2019.09.26 till 2022.09.30),
Academic consultant – Doc. Dr. Indrė Isokaitė-Valužė
(Vilnius University, Social Sciences, Law – S 001, from 2019.08.26 till 2022.09.30).

VILNIAUS UNIVERSITETAS

Alaa
Al Dakour Al Aridi

Hibridinio karo problema tarptautinėje teisėje

DAKTARO DISERTACIJA

Socialiniai mokslai,
Teisė (S 001)

VILNIUS 2022

Disertacija buvo rengta 2015 - 2022 metais Vilniaus universitete.

Mokslinis vadovas – prof. dr. Dainius Žalimas
(Vilniaus universitetas, sociainiai mokslai, teisė – S 001, nuo 2015.10.01 iki 2019.09.25),
Mokslinis vadovas – p**rof. habil. dr. Gintaras Švedas**
(Vilniaus universitetas, sociainiai mokslai, teisė – S 001, nuo 2019.09.26 iki 2022.09.30),
Mokslinė konsultantė – doc. dr. Indrė Isokaitė-Valužė
(Vilniaus universitetas, sociainiai mokslai, teisė – S 001, nuo 2019.08.26 iki 2022.09.30).

Content

LIST OF ABBREVIATIONS ---- 7

INTRODUCTION ---- 9

I- **EMERGENCE OF HYBRID WARFARE IN THE EVOLUTION OF ARMED CONFLICTS** ---- 29

1. THE EVOLUTION OF WARFARE FROM CONVENTIONAL TO MODERN ---- 31
   1.1. Sun Tzu's Art of War ---- 33
   1.2. Clausewitz Theory of War ---- 35
   1.3. The Changing Character of Modern Conflicts ---- 37
      1.3.1 Conventional Warfare ---- 38
      1.3.2. The Irregular Warfare/ Asymmetric Warfare ---- 39
2. THE DEVELOPMENT OF THE LEGAL TERMINOLOGY OF ARMED CONFLICTS ---- 41
   2.1. Armed Conflict and the International Humanitarian Law ---- 43
      2.1.1. International Armed Conflict (IAC) ---- 43
      2.1.2. The Predominance of Non-International Armed Conflict (NIAC) ---- 44
3. HYBRID WARFARE: DEFINITIONS AND ELEMENTS ---- 48
   3.1. Overview of Hybrid Warfare ---- 50
   3.2. Challenging Elements and Means of Hybrid Warfare ---- 62
      3.2.1. Non-State Armed Groups As An Element Of Hybrid Warfare ---- 64
      3.2.2. Cyber Operations in Hybrid Context ---- 67
      3.3.3. Lawfare ---- 72

II- **INTERNATIONAL LAW ON THE USE OF FORCE AND HYBRID WARFARE** ---- 78

1. THE USE OF FORCE IN INTERNATIONAL LAW ---- 81
   1.1. The Just War Theory to Modern Jus Ad Bellum ---- 81
      1.1.1. The Prohibition of Unilateral Threat or Use of Force ---- 85
      1.1.2. Article 2(4) of the UN Charter and meaning of "Force" ---- 86
      1.1.3. Aggression and Hybrid Warfare ---- 90
2. EXCEPTIONS TO THE PROHIBITION OF THE USE OF FORCE ---- 100
   2.1. Authorization by the UN Security Council ---- 102
   2.2. The "Trigger" for the Inherent Right of State Self-Defense ---- 104
      2.2.1. The Elements of an Armed Attack ---- 108
      2.2.2. Principles of Necessity and Proportionality in Self-Defense ---- 113
   2.3. Right to Self-Defense against Non-State Actors (NSAs) ---- 118
      2.3.1. Self-Defense against Non-State Actors on the Territory of another State: The Myth of the Unable or Unwilling Standard in the Hybrid Warfare era ---- 124
      2.3.2. Self-Defense against Proxy Armed Groups ---- 132
      2.3.3. The Ambiguity between Use of Force in Self-Defense and Potential Armed Reprised crafter by Hybrid Warfare ---- 136
   2.4. Exceptions Outside of the UN Charter System: Humanitarian Intervention and Responsibility to Protect Doctrine (R2P) ---- 143
      2.4.1. From "Right to Intervene" to "Responsibility to Protect (R2P)" ---- 147
3. LEGAL BASIS OF THE ATTRIBUTION OF INTERNATIONAL RESPONSIBILITY TO A STATE ---- 150
   3.1. Attribution and Hybrid Warfare ---- 152
   3.2. Effective and Overall Control Tests ---- 157
      3.2.1. Effective Control Test ---- 157
      3.2.2. Overall Control Test ---- 162
4. THE PRINCIPLE OF STATE SOVEREIGNTY IN THE ERA OF HYBRID WARFARE ---- 166
   4.1. State Sovereignty under International law ---- 166
      4.1.1. State Sovereignty in Cyber Context ---- 172
      4.1.2. Due Diligence Standard: A Potential Remedy to the Complexity of Cyber Threats ---- 175
   4.2. Legal Nature of the Non-Intervention and Non-Interference Principle and Elements of their Scope ---- 182
      4.2.1. Elements of Coercion ---- 187
      4.2.2. Coercive Intervention in Hybrid Cyberspace ---- 189

III- **INTERNATIONAL HUMANITARIAN LAW AND HYBRID WARFARE** ---- 193

1. INTERNATIONAL HUMANITARIAN LAW: BACKGROUND ---- 198
   1.1. Basic Principles of International Humanitarian Law ---- 201

1.2. Responsibilities and Violations of States under International Humanitarian Law ---------- 204
1.3. The Relationship between IHL and IHRL ---------- 207
2. APPLICABILITY OF JUS IN BELLO TO HYBRID WARFARE ---------- 213
2.1. Armed Conflicts in Theory and Practice under International Humanitarian Law (Classification and Core Elements) ---------- 218
2.1.1. Core Elements of International Armed Conflict ---------- 221
2.1.2. Core Elements of a Non-International Armed Conflict ---------- 229
2.2. Hybrid Warfare and Modern Armed Conflicts ---------- 239
2.2.1. Hybrid International Armed Conflict ---------- 246
2.2.2. Hybrid Non-International Armed Conflict (Cyber and Non-State armed groups) ---------- 251
2.2.3. Hybrid Warfare in a Co-existing Armed Conflict ---------- 263
3. APPLICATION OF PRINCIPLE OF DISTINCTION TO HYBRID WARFARE (CYBER OPERATIONS AND HYBRID NSAS) ---------- 274
3.1. Principle of Distinction ---------- 276
3.1.1. Civilian Objects and Military Objectives in Hybrid Context ---------- 280
3.1.2. Civilians and Combatants ---------- 284

CONCLUSIONS ---------- 298

BIBLIOGRAPHY ---------- 303

List of Abbreviations

AP I: Additional Protocol I to the 1949 Geneva Conventions (1977).
AP II: Additional Protocol II to the 1949 Geneva Conventions (1977).
AP III: Additional Protocol III to the 1949 Geneva Conventions (2005).
CA 2: Common Article 2 to the four 1949 Geneva Conventions.
CA 3: Common Article 3 to the four 1949 Geneva Conventions.
Commentary GC I: Commentary on the Geneva Conventions of 12 August 1949 for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.
Commentary GC II: Commentary on the Geneva Conventions of 12 August 1949 for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea.
Commentary GC III: Commentary on the Geneva Conventions of 12 August 1949 Relative to the Treatment of Prisoners of War.
Commentary GC IV: Commentary on the Geneva Conventions of 12 August 1949 Relative to the Protection of Civilian in Time of War.
DARSIWA: Draft Articles on Responsibility of States for Internationally Wrongful Acts
DDOS: Disturbed Denial of Service.
DPH: Direct Participation in Hostilities
DNR: Donetsk People's Republic (unrecognized proto-state located in the Donbas region of eastern Ukraine).
DOS: Denial of Service.
EU: European Union.
FSB: Russian Federal Security Service.
GA: General Assembly of the United Nations.
GC I: Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field.
GC II: Convention (II) for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members of Armed Forces at Sea.
GC III: Convention (III) Relative to the Treatment of Prisoners of War.
GC IV: Convention (IV) Relative to the Protection of Civilian Persons in Times of War.
GCs: Geneva Conventions of 1949.
IAC: International Armed Conflict.
ICC: International Criminal Court.
ICCPR: International Covenant on Civil and Political Rights.
ICJ: International Court of Justice.
ICRC: International Committee of the Red Cross.
ICTR: International Criminal Tribunal of Rwanda.
ICTY: The International Criminal Tribunal for the Former Yugoslavia.
IHL: International Humanitarian Law.
IHRL: International Human Rights Law.
ILC: International Law Commission.
ISIS: Islamic State of Iraq and Iraq (Also known as Islamic State in Iraq and Levant "ISIL").
LNR: Luhansk People's Republic (unrecognized proto-state located in the Donbas region of Eastern Ukraine).
LOAC: Law of Armed Conflict.
NIAC: Non-International Armed Conflict.
NSA: Non-state actor. (for this thesis NSA means armed groups).
OAS: Organization of American States.
OSCE: Organization for Security and Co-operation in Europe.
R2P: Responsibility to Protect

UN GGE: The United Nations Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of International Security.
UN: United Nations.
UNGA: United Nations General Assembly.
UNIFIL: United Nations Interim Force in Lebanon.
UNSC: United Nations Security Council.
UNSCR: United Nation Security Council Resolution.

Introduction

The extensive effort to regulate the use of force, aggression, and armed conflicts through the mechanism of legal regulations, has resulted in the development of international law throughout treaties, rules, and principles, particularly by the end of the 19th century and the beginning of the 20th century. That was reflected chiefly on the dualist conception of armed force which is rooted in the general prohibition on the resort to armed force articulated in the United Nations Charter 1945 that narrowed the grounds on which subjects of international law may legitimately resort to armed violence, and the principles of International Humanitarian law under the Geneva Conventions 1949 (GCs) and its Additional Protocols (hereinafter AP I and II) that governed the conduct of hostilities. Public International Law is one of the fastest-growing fields, a universal system of rules and principles governing the relationship between public bodies through common instruments such as conventions. Correspondingly, International Law influences NSAs that include individuals, corporations, armed militant groups, and groups that wish to break away from states such as minorities (ethnic, religious, linguistic). The primary form for the creation of public international law is through intergovernmental organizations such as the United Nations (UN) that codifies customary law by the form of international treaties, also it develops, creates, and enforces international law on many levels. Given this, understanding and examining the relationship between war and international law is central to countering past and new threats. An assertion that had been well highlighted by Stephen Neff who considered that: "war and law have always exercised a reciprocal influence upon one another."[1]

In the first place Hugo Grotius' influential work "The Law of War and Peace", set a road map to international law around the existence of two categories he referred to as "War and Peace", wherein there is no intermediate state between the two terms. This dividing line is cardinal to the international legal system where the UN Charter considers that peace is the ruling factor in international relations, while the use of force should be an exception based on cases of self-defense or authorized interventions by the international community through the Security Council. However, there is no immutable and scientific definition for the line of distinction between war and peace, leaving a slit for international law to understand the rules

[1] Neff, S., War and the Law of Nations. Cambridge University Press, Cambridge 2008, p.2.

relevant to the use of force and armed conflicts.[2] Nonetheless, while wars were fought over existential survival, resources, and territory that had to be seized or retained by force[3], a shift in warfare by character and nature starting in late 1980 was recognized by the Fourth Generation Warfare theorists that highlighted such transformation predicting future warfare.[4] This development in warfare has ushered in the ability to fight even without using violence or even physically challenging another nation's sovereignty.[5] Correspondingly, Frank Hoffman's argument[6] about the blending form of warfare in a hybrid form, what is widely known as Hybrid warfare, reflected this gray zone between peace and war.[7] Therefore, Grotius' line of distinction in the era of globalization, technologies, and NSAs, is blurred to the point of indistinction. This requires that the dualist conception of armed force, Jus ad Bellum and Jus in Bello, be addressed based on the situation-specific approach in incidents that are neither considered declared war, nor part of peacetime relations.

For this purpose, discussions over the past two decades focused on the evolution of modern wars and the transformation in means and elements of warfare, mainly through scholars from multiple disciplines who focused their attention on defining and examining hybrid warfare[8]. Hybrid warfare created a challenge to international peace and security, especially in that it consists of multiple elements employed to serve the interest of adversaries, particularly in current conflicts[9]. Hybrid warfare has no universal definition, but its main features are highly relevant due to the legal asymmetry it creates by the combination of traditional means of warfare with non-military means through de-centralized operations. However, it does not exist in a legal vacuum, for instance the principal modern legal source of Jus ad Bellum derives from

---

[2] Berman, N., Privileging Combat? Contemporary Conflict and The Legal Construction of War, Col. J. Trans L. I, 2004, p. 43.
[3] Warren J., Not All Wars are Violent "Identifying Faulty Assumptions for the Information War", Air and Space Power Journal, Winter 2020.
[4] Williamson, S., From Fourth Generation Warfare to Hybrid War, U.S. Army War College, Carlisle Barracks, USAWC Class Of 2009, p. 7.
[5] Warren J., Ibid.
[6] Frank G. Hoffman A Senior Research Fellow with The Institute for National Strategic Studies, and the author of Rise of Hybrid War, Conflict of 21st century in 2007, p. 5. Important to note that while War is used to describe the deliberate use of violence to meet political ends, Warfare Describes the Physical Means of Fighting Wars. See, Footsoldier D., "When is a War Not A War? When Its Hybrid", Think Defense, 16 February 2015.
[7] Footsoldier, D, Ibid. Frank Hoffman, who is widely quoted by scholars with regards to the hybridity of contemporary warfare, stated that "we are entering multiple types of warfare taking a variety of forms".
[8] See for example, Owens, M., Reflection on Future War, Naval War College Review 2008, p.61-76; Glenn, R., All Glory is Fleeting: Insights from the Second Lebanon War, RAND, Santa Monica 2012; Jordan l., Hybrid War: Is the US Army Ready for the Face of 21st Century Warfare, US Army Command and General Staff, 2008.
[9] Al-Aridi, A., How Hybrid is Modern Warfare, Conference Paper at the 5th International Conference of PhD Students and Young Researchers, How Deep is your Law? Brexit, Technologies, Modern Conflicts, Vilnius, April 2017, p. 8.

the UN Charter, in particular Article 2(4) regulating the prohibition on the use of force, also the rules of International Humanitarian law regulating armed conflicts and their fundamental principles, and the role of the general principles of law that may be invoked as supplementary rules of international law where appropriate. Most of the general principles of international law are logical propositions underlying judicial reasoning based on existing international law, such as principles of consent, reciprocity, equality of states, and freedom of the seas. In theory, jus ad Bellum and jus in Bello are two distinct bodies, and while the principles of necessity and proportionality have been core principles of both branches, in jus ad Bellum the two principles are conceived as a legal framework to regulate the execution of military operations, whereby the ICJ in Nicaragua case has confirmed that any measures taken in self-defense must be proportionate and necessary to respond to the attack in question.[10] On the contrary, under jus in Bello, the principles are determined by each military action whereby IHL prohibits attacks that may be expected to cause incidental loss of civilian, life, or injury of civilians, and permits only measures which are necessary to accomplish a legitimate military purpose. On the other hand, both branches of law are vital to address any illegal use of force and war crimes respectively, that is highly relevant to the realities of modern warfare with regards to the lawfulness or legitimacy of conflicts of hybrid nature. It is also a vital step as states tend to expand the limits of jus ad Bellum to include notions such as pre-emptive self-defense, humanitarian interventions, or invoke the right to national or collective self-defense to justify extraterritorial responses to non-state or cyber threats. Nonetheless, both bodies of law are independent, states can violate the jus ad Bellum but at the same time act in full compliance with the jus in Bello and vice versa.

Strict adherence to international law, particularly Jus ad Bellum and Jus in Bello, became more imperative in modern warfare, through which the legal complexity of hybrid warfare is based on the ambiguity and legal asymmetry that such campaigns establish, mainly through cyber operations and the employment of NSAs. In many respects, current use or threat to use force in international relations is generated from armed groups that operate covertly, also the access of such groups to tools that are originally non-military but deployed to conduct attacks, such as cyber-attacks that have a great impact on attributing actions to their perpetrators. So, lack of attribution creates legal gray area intended to mask unlawful activities that can be held

[10] Military and Paramilitary Activities in and against Nicaragua "Nicaragua v. United States", Judgment, 1986 ICJ., 27 June 1986, Rep. 14, Para 176.

legal responsibility under international law. In practice, most cyber operations take place below the threshold of use of force, such operations are low-level intrusions that can cause harm but without physical effects. While there is no doubt that international law, including the principle of sovereignty, applies to such operations yet how the law applies is subject of debate. For a hybrid scenario, the jus ad Bellum is vital for the victim state or alliance to legally justify whether/how they can respond to such threats. Similarly, international humanitarian law requires identifiable parties to the conflict for its rules and principles to be applied effectively. Hybrid adversaries aim to avoid direct attribution and by that impose challenges on the classification of armed conflicts due to the ambiguous identity of its parties. Furthermore, hybrid actors involve civilians in certain operations, mainly in cyberspace that are increasingly substituting kinetic means, and urban warfare that is taking place among the civilian population can blur the line of distinction between combatants and persons protected under its rules. Additionally, several scholars highlighted the challenge of using or misusing the fluidity of law as a means of warfare, or what is so-called Lawfare, a concept that was introduced by US Air Force lawyer Charles Dunlap Jr. in 2001 as the newest feature of the 21st century.[11] Hybrid warfare and its challenging elements are successfully employed in contemporary conflicts. Some of these hybrid means were identified in the conflict in Ukraine that increased its level of intensity after the annexation of Crimea and ongoing hostilities in Eastern Ukraine (the study will focus on the conflict that started in 2014 "Annexation of Crimea and conflict in Eastern Ukraine" and will not discuss the latest events of unprovoked aggression in 2022 unless deemed necessary in some areas, hereinafter Conflict in Ukraine)[12], the building of artificial islands by China to gain more territory through unconventional techniques without provoking a military escalation that might lead to a systemic conflict[13], and cyber-attacks that are occurring on daily basis in armed conflicts and peacetime. These examples reflect the deliberate use of lethal and non-lethal means of hybrid operations that were successfully employed and had a direct impact on the rules of international law. So, addressing the legal aspects of hybrid warfare requires it to be properly situated within the existing regime

[11] Charles, J. Dunlap, USAF: Law and Military Interventions: Preserving Humanitarian Values in 21st conflicts, Paper prepared for the Humanitarian Challenges in Military Intervention Conference, Carr. Ctr. For Human Rights Policy Harvard University, Washington D.C. Nov. 2001.

[12] The conflict in Ukraine can be divided to IAC and NIAC, and was considered one of the examples of Hybrid warfare conducted by Russia and involved the use of conventional and non-conventional means to a single battlefield. See more, Kuzio T. and D'Anieri P., Annexation and Hybrid Warfare in Crimea and Eastern Ukraine, E-Interntational Relations, June 25, 2018. Available at: https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/

[13] Miracola S., Chinese Hybrid Warfare, The Italian Institute for International Political Studies ISPI, 21 December 2018. Available at: https://www.ispionline.it/it/pubblicazione/chinese-hybrid-warfare-21853

governing the use of force in international relations (Jus ad Bellum) and the law regulating the conduct of war (Jus in Bello). As by any legal discussion of the law applicable in various situations (Peacetime, armed conflict) the distinction between Jus ad Bellum and Jus in Bello is vital. It is important to keep in mind that both regimes are independent, in which even illegal use of force by states contrary to Jus ad Bellum will activate the law governing the conduct of hostilities (Jus in Bello). In parallel, States may violate the Jus ad Bellum but at the same time act in full compliance with the Jus in Bello and vice versa.

Relevance and Problem of the Research

Public International Law, the only normative regime that purports to be universal and uniform, is traditionally defined as the law between sovereign states, mainly within the context of the rules and principles governing laws of war, peace, security, and as well the protection of territories. In parallel, hybrid warfare is an evolving concept in contemporary conflicts that provided a perfect conundrum. This type of warfare is a military strategy blending conventional, irregular tactics[14], cyber warfare, terrorism, and criminal behavior within a battlespace to obtain political objectives[15]. Such a strategy of warfare can be tooled by state or/and NSAs to destabilize existing order, embrace stabilization in failing or failed states, and create a transnational threat beyond the territorial borders of its operations. Hybrid warfare succeeds through the ability of hybrid actors to synchronize multiple instruments of power simultaneously and intentionally exploit creativity, ambiguity, non-linearity, and the cognitive elements of warfare[16]. Victim states or group often find their response options limited in the absence of an identifiable author of operations, especially since a variety of NSAs operate in this environment acting as proxies for third States. However, the growing number of NSAs involved in NIACs around the world, also their ability to conduct operations through cyberspace and non-kinetic means. The fusion of these asymmetric types of conflicts with unconventional means requires deeper analysis and examination of the applicable principles and rules.

Given these points, several aspects justify the relevance of such scientific research. First, the understanding of war and peace was challenged during the conflict in Eastern Ukraine creating

[14] Hezbollah proved to be a perfect example of NSA that employed Hybrid Tactics in its conflict with Israel in Southern Lebanon in July 2006; Hoffman, F., Ibid. p. 35.
[15] Munich Security Conference Broadened the Hybrid Concept to Include Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement.
[16] MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, Multinational Capability Development Campaign MDCD, January 2017, p.3.

confusion in classifying the conflict and the applicable law. Where in one sense it was classified as a NIAC regulated by international humanitarian law; on the other hand a proxy conflict pitting two states and turning it to IAC with a broader interference of International Law; or it is a newly emerging type of conflict that internationalizes a NIAC. Moreover, the annexation of Crimea, which is considered a clear violation of international law, has in practice proved the success of hybrid operations in reaching objectives that conventional conflict can reach but with more violence and aggression[17]. Another example is the hybrid activities of China in the South China Sea and its use of technological capabilities to enforce superiority and claim more territories[18]. Under these circumstances and in-between the sovereignty of states protected by international law, and the hybrid threats and means of decentralized behavior, the problem of hybrid warfare in international law comes to light. According to Aurel Sari: "Law and legal consideration are in the heart of the hybrid warfare"[19], especially that the threats imposed by hybrid means in contemporary conflicts are employed to exploit gray areas and fault lines in the law.

Secondly, present-day conflicts are based on States' plausible deniability of their involvement in armed operations or support to non-state armed groups, that in return tend to invest in available technologies, such as cyberspace. These new technologies offer hybrid actors ambiguity and the ability to mask their real identity to avoid any responsibility or retaliation for wrongful acts. International law faces difficulties in responding to these new means and weapons introduced, especially since most of the hybrid operations are of low intensity and therefore below the threshold of armed attacks. Although current Jus ad Bellum, on one hand, is sufficient in addressing the use of force in international relations, however, the nature of hybrid threats raises many challenges. For example, State responsibility for actions of agents of groups attributed to it. Also, the inadequacy of control tests in the context of cyber NSAs. Hybrid adversaries also tend to violate State sovereignty through non-kinetic means, which has been seen through interferences in elections, also the cyber-attacks in its relation to the non-intervention principle has a different understanding when it comes to the targeted sector, that has been reflected in the EU's recent restrictive measures against the cyber-attacks

[17] Russia's annexation of Crimea and its incursion in eastern Ukraine was launched on the pretext of protecting ethnic Russians and speaks in the region. See, Ball J., Russia's Justification for the Annexation of Crimea, Global Security Review, June 10, 2019. Available at: https://globalsecurityreview.com/russias-legal-plausible-justification-for-the-annexation-of-crimea/

[18] Miracola S., Ibid.

[19] Sari. A., Strategy and Security Institute Workshop on Legal aspects of Hybrid Warfare, University of Exeter, 2015. https://law.exeter.ac.uk/newsandevents/newsarchive/articles/strategyandsecurityinstitu.php

that were considered a threat to member states when affecting information systems. So, bearing in mind that States engaged in such operations often rely on sub-state actors or proxy armed groups for kinetic and non-kinetic campaigns, this has created a conundrum regarding their legality to self-defense provisions and the law of armed conflict.

Third, hybrid means that reach the level of armed violence are highly relevant to the application of Jus in Bello in an armed conflict, whether international or non-international. However, the blurring line between IAC and NIACs, combatants and civilians, and the ambiguous status of hybrid actors have theoretical and practical challenges. So, whether the GCs have generally provided sufficient guidelines to define and manage gray zone conflicts due to their low intensity and a high degree of operational covertness, is essential. For example, the role of NSAs or individuals engaging in low-intensity cyber operations against another state, or the fishermen in the South China Sea that engage in covert operations to fulfill political or military objectives, by using propaganda, domestic legal structure, economic pressure, and covert support for NSAs to be more capable. That is also relevant to tasks under the GCs of 1949 and its APs, precisely the protection of non-combatants under the principle of distinction.

Moreover, under international law, the legal terminology of warfare has developed separately under both Jus ad Bellum (use of force, armed attack, and aggression) and Jus in Bello (Geneva Conventions and its Additional protocols that apply to IACs and NIACs), and through the role of the Rome Statute of the ICC that established four core international crimes: genocide, crimes against humanity, war crimes and the crime of aggression. But the new challenges to international law constitute a part of a natural process in which the existing legal framework is tested whether it is found to be ineffective or not, and if so, can international law offer viable options for the lawmaking process to address such aspects. In this context, Outi Korhonen indicated that "hybrid warfare can erase the legal categories of war and peace, state and individuals, aggression and defense"[20]. So although the legal definition of hybrid warfare is due to the constant change of its elements (historical, geographical, and demographical), means (weapons, actors, and technological evolution), and the continuous development of the legal theory surrounding wars in international relations, is not an easy task. However, a

[20] Korhonen, O., Deconstructing the Conflict in Ukraine: The Relevance of International Law to Hybrid States and Wars, German Law Journal 2015, vol. 16, p. 459.

thorough revision and examination of the elements of modern hybrid warfare, and its impact on the existing rules of the Jus ad Bellum and IHL, is highly relevant and essential.

Therefore, the research requires tackling the problems that arise to the applicability of the law on the use of force in International Law and International Humanitarian law to hybrid warfare. Such examination is very advantageous not only for international lawyers or legal experts but also has practical value for policymakers and humanitarians. The importance of examining hybrid warfare in terms of both jus ad bellum and jus in bello is mainly because hybrid warfare, through NSAs and cyber operations, falls in a legal grey area. Therefore, hybrid warfare is relevant with regards the legal challenges it imposes in peacetime and armed conflict situation, taking into account the loopholes that may be exploited by an adversary to maintain such a grey zone. Similarly, the lawful response of the state will depend on the legal framework in times of peace and armed conflict, which in many regards may differ. In addition to that, the legal examination of the hybrid warfare concept has been modest so far, especially since the term can be easily characterized than being defined, whereby definitions and analysis of the concept by scholars, governments, and organizations came as a response to contemporary conflicts, and studies were based on examining the cases based on the interest of parties. So, until there will be common terminology that explains the fusion of different means and methods, that is unlikely to happen, legal scholars should focus on addressing its elements separately.

For this research, the relevancy is based on the following features:

- Hybrid warfare is multi-modal. The multi-modality deployment of capabilities and resources in hybrid warfare creates a problem in attempting to define aggression and enforce its prohibition in modern conflicts[21], that was reflected in Nathan Freier's comprehensive definition of hybrid warfare "an adversary's integration and use of at least two of the following modalities: traditional warfare, catastrophic terrorism, irregular warfare, and disruptive use of technology."[22] On the other hand, the ICJ in the Nicaragua case defined armed attack as "the most-grave form for the

[21] According to Michael Reilly "there is no adequate model or methodology to determine a hybrid threat's center of gravity. The current definition and methods fail to account for the multimodalities, ambiguity, and political constraints presented by hybrid threats." See, Reilly M., Hybrid Threat Center of Gravity Analysis: Taking a Fresh Look at ISIL, National Defense University Press, January 26, 2017. Available at: https://ndupress.ndu.edu/Media/News/Article/1038835/hybrid-threat-center-of-gravity-analysis-taking-a-fresh-look-at-isil/

[22] Freier N., Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context, Strategic Studies Institute, May 2007, pp. 18-19.

use of force"[23], yet the threshold of what would constitute an armed attack is still arguable and is challenged by low-intensity hybrid operations, that is an integral feature of grey zone created by Hybrid adversaries. Nevertheless, the ICJ in both the Oil Platform case (the Islamic Republic of Iran v. United States), and the Armed Activities in Democratic Republic of Congo case accepted that a series of incidents that do not rise to the level of an armed attack when examined separately, cross the threshold level of armed attack when viewed cumulatively are likely to bolster support for this accumulation. However, it could be misused by States to justify the use of force in a broad manner threatening the territorial integrity and principle of non-intervention under international law. So, when examining the challenging elements of hybrid warfare, such as cyber-attacks and non-state armed groups,

- Hybrid warfare is deceptive. In general, UN Charter is sufficient to account for hybrid threats when they resemble traditional military activities, however, problem ascends through covert actions and the ability of an adversary to sustain public deniability of their actions that exploit the weakness of international enforcement regime and the ability of targeted states to respond lawfully without being accused of violating the applicable international norms. In the same manner, intra-state conflicts and proxy involvements are dominant in the international arena, and with little legislation regulating such conflicts, states and NSAs exploit this weakness to internalize matters to their utmost, through which it has been argued that IHL does not regulate all possible situations, including some elements of hybrid warfare. And although the classification of hybrid war is defied by the interplay between both types of conflicts and challenging the IHL's regulatory effectiveness despite that over centuries there were efforts to place rules and limits on the methods and methods of warfare that can be used, the rules enshrined in the treaties and judgments are more designed for conventional means, that makes it difficult to apply to hybrid warfare.
- Hybrid warfare is harmful. It flourishes in defenseless areas of laws and combines the properties of different means creating a legal asymmetry and ability to tackle any attempts to be diagnosed or identified. This has been a challenge to the states that have been endorsing plans to strengthen their legal resilience to a new

[23] Military and Paramilitary Activities in and against Nicaragua, ICJ 1986, Ibid, para 191.

different stage[24]. The challenge is to whether the targeted state is under an armed attack that could trigger self-defense or civil unrest to be dealt with through law enforcement; whether the adversary is a non-state armed group not attributable to any state or proxy actor aimed to conceal any involvement; or whether cyber-attacks originating from the territory of another state holds the host state responsibility for wrongful actions or it is the responsibility of the attacker. The legal gray zone established by hybrid adversaries and strategies leverages ambiguity to create an environment in which targeted parties are unable to make strategic a decision in a timely and confident manner.

- It has been argued that hybrid warfare is not well developed in International Law and remains more relevant in political or military doctrines. At the same time for many authors, it is a non-declared war or a non-recognized international armed conflict simultaneously. Therefore, the rules to regulate such campaigns is the main challenge imposed by hybrid actors, whether state or non-state, that use hybrid campaigns as a method to avoid any responsibility of their actions through exploiting the legal thresholds of an armed attack, intervening through proxy fighters at a low-intensity level of force, playing on the broadness of legal framework to justify actions that lack full evidence of using force. On the other hand, it creates a challenge to the targeted states concerning their ability to respond legally in line with principles of distinction, necessity, and proportionality, or to identify the attacker that skillfully combines and blurs the line between the state of peace and war regime. At the same time, it challenges the rules of engagement in IHL as to whether the adversaries are civilians or combatants (blurring the line of distinction); as to whether the State can divide theatrically and legally the scenarios faced between civil unrest (law enforcement), non-international conflict (common article 3 to the GCs 1949) or international armed conflict (common article 2 to the GCs 1949), and combining the principles of both to a single battlefield. Therefore, ambiguity in conflicts' classification is always expected in the contemporary combat environment (conflicts in Syria, Ukraine, Georgia).

[24] See, the establishment of the European Excellence Centre for Countering Hybrid Threats (Hybrid CoE) in April 2017, an intergovernmental think tank based in Helsinki, that engages in strategic dialogue, research, training, and consultations to illuminate vulnerabilities to hybrid measures and improve resilience against hybrid threats.

For this reason, the analysis of the selected elements and features of the hybrid warfare concept presented in this research will propose certain steps that should be taken into consideration to ensure more efficient compliance with the principles and rules of the applicable laws.

Scientific Novelty and Originality of the Research

When research started on this topic, there was no comprehensive analysis of the relevant laws in their relation to hybrid warfare, especially with regards the applicability of international humanitarian law and the international law on the use of force. Hybrid warfare is a very complex and broad topic to be discussed, first of all, it is a term that is undefined legally, with a wide concept that includes many elements hardly to be framed and interplays between politics and law through a thin line. Most of the non-legal literature has discussed the military and strategic elements of hybrid war, by addressing and examining the developed weapons, actors, and strategies of such conflicts, and how western states and in particular NATO can counter such threats coming from adversaries. Yet, the non-legal literature is very important for analysis, as it gives an overview of the means and elements of hybrid warfare, and proves that there is a big tendency by states to use hybrid tactics in contemporary conflicts, as it was seen to be a successful strategy for both states or NSAs. (Hoffman F.[25], Davis R. J.[26]) have discussed the hybrid warfare mindset that is based on four interacting characteristics: understanding strategic context, a holistic approach to operations, internalization of propensity and potential opportunities, and embracing complexity at the edge of chaos. In addition, (Mazarr M., discussing the Gray Zone established by the new era of conflicts[27]; Brands H.[28] the concept of grey zone; Berzins J.[29] analyzing the Russian warfare; Russia and NATO by Poplin C.[30]; Witts B.[31] general overview of Hybrid warfare).

Also, it was acknowledged that scholars have examined the employment of NSAs to achieve objectives that regular forces have been unwilling or unable to achieve through conventional

[25] Hoffman F., Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, December 2007.
[26] Davis J., The Hybrid Mindset and Operationalizing Innovation: Toward A Theory of Hybrid, School of Advanced Military Studies, United States Army Command and General Staff College Fort Leavenworth, Kansas 2014.
[27] Mazar M., Mastering the Gray Zone: Understanding a Changing Era of Conflict, US Army War College, Strategic Studies Institute, December 2015, pp. 55-67 and 72-74.
[28] Brands H., Paradoxes of The Gray Zone, Foreign Policy Research Institute, February 2016.
[29] Berzins J., The New Generation of Russian Warfare, Aspen Review Central Europe, 2014, Vol. 3.
[30] NATO vs. Russia: How to Counter the Hybrid Warfare Challenge, The National Interest, July 2016.
[31] Wittes B., What is Hybrid Warfare? Lawfare Blog, September 2015.

means (Davis, D., Schlichte, K.[32]; Ahram A.[33] on the role of Paramilitaries), it was also examined why states use non-state armed groups to delegate certain types of violence against civilians (Carey et al[34], Forney, J.,[35]). Several scholars have discussed the evolution of warfare and its legal development with regards to the self-defense against non-state armed groups, without giving bigger attention to hybrid warfare and were argued that it does not create any new challenge (O'Connell M. E.[36]; Murray, W., and Mansour, P.[37]).

Besides, scholars had based their interpretation of such forms of warfare on specific conflicts, despite notable exceptions of a series of articles by Dr. Aurel Sari on hybrid wars and Lawfare[38], where it highlighted legal challenges imposed by selected elements of hybrid warfare. Similarly, the valuable writings of Michael Schmitt and his contribution to Tallinn Manuals with regards to cyber-attacks were reviewed as it was very important in examining whether cyber operations can qualify to a use of force while not unleashing destructive or injurious force, and concluded that ICJ in Nicaragua case confirms that such cyber operations can sometimes amount to a use of force[39]; and Marco Sassoli on the role of non-state armed groups and ways to improve compliance with International Humanitarian Law[40]. Another highly important source of the research, which had an impact on the analysis, is the work of Nels Melzer in explaining the ICRC's approach towards the civilians' direct participation in hostilities through interpretive guidance.[41] Melzer also provided quite interesting work by

---

[32] Schlichte, K., With the State against the State? The Formation of Armed Groups', Contemporary Security Policy 2009, p. 246–64

[33] Ahram, A., Proxy Warriors: The Rise and Fall of State-Sponsored Militias, Stanford, Stanford University Press 2011.

[34] Carey, S., Colaresi,M., and Mitchel, N., Government, Informal Links to Militias, and Accountability, Journal of Conflict Resolution 2015, p. 850–876

[35] Forney, J., Who Can We Trust with a Gun? Information Networks and Adverse Selection in Militia Recruitment, Journal of Conflict Resolution 2015, p. 824–849

[36] O'Connel M.E., What is War? An Investigation in the Wake of 9/11, Martinus Nijhoff/Brill. edited vol. 2012.

[37] Mansoor, P., Introduction, Hybrid Warfare in History, Hybrid Warfare, Fighting Complex Opponents from the Ancient World to the Present, W. Murray and P. Mansoor eds., 2012.

[38] Sari, A., Legal Aspects of Hybrid Warfare, Lawfare Blog 2015; Sari A., Hybrid Law, Complex Battlespaces: What's the Use of a Law of War Manual?, in Michael A. Newton ed., The United States Department of Defense Law of War Manual: Commentary and Critique, 2019,p 403-430 ; see also , Hybrid Warfare, Law and The Fulda Gap, in Christopher Ford and Winston Williams (eds.), Complex Battle Spaces , 2019, p. 161- 190

[39] Schmitt, M., The Law of Cyber Warfare: Quo Vadis? Stanford Law and Policy Review, Vol. 25, p. 279-289, 290-293 with regards to conflict characterization and attacks under jus in bello; see also, Schmitt M., The Law of Cyber Targetting: Tallinn Paper No. 7, Naval War College- Stockton Center for the Study of International Law, January 2015

[40] Sassoli, M. Engaging Non-State Actors: The New Frontier for International Humanitarian Law. In: Exploring Criteria & Conditions for Engaging Armed Non-State Actors to Respect Humanitarian Law and Human Rights Law. Geneva: PSIO, UNIDIR, Geneva Call, 2008. p. 8-12.

[41] See, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, adopted by the Assembly of the ICRC on 26 February 2009; Melzer N., Keeping the Balance between Military Necessity and Humanity: A response to four critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities, International Law and Politics Journal, Vol. 42, 2010.

responding to the critiques of the ICRC's approach. This has been also very relevant for our research to examine the notion of direct participation in hostilities with regards to cyber operations. Though the interpretive guidance did not deal with cyber operations, it was quite informative to reflect the complexity and challenges imposed by such phenomena. However, it was hard to find a comprehensive analysis of the legal framework of hybrid warfare, in particular areas that highlight the confusion created by hybrid adversaries using cyber NSAs that involve civilians.

Therefore, the novelty of this research is to illuminate the legal grey zone imposed by selected hybrid warfare elements from a practical and theoretical perspective. For example, addressing technological features of cyber-attacks and examining them under the relevant rules and principles of international law. This scientific research targets to provide recommendations to deal with possible legal gaps especially in understanding the laws applicable to hybrid warfare under the international law on the use of force and International Humanitarian law, in particular with regards to the fusion of different means such as non-state cyber actors, geographical limitations and State practice (unable or unwilling standard[42], targeting killing, and cyber global battlefield) that examines the cross-cutting issues concerning primary principles of both Jus ad Bellum and Jus in Bello.

The research was structured to allow the reader to understand how the relevant principles and rules can be applied to cases derived from contemporary conflicts and threats. The research can also be a proper basis to continue further research on elements of hybrid warfare that were not included in the analysis, such as cyber operations that do not reach the level of armed attack (espionage, financial crimes), also it is a basis for discussing other principles of IHL such as military necessity and precaution that are highly relevant to hybrid warfare.

Research Methods

The present dissertation employs standard legal analysis in studying primary sources of international law such as treaties, customary international law, general principles of law, judicial decisions, and legal doctrine[43], especially the UN Charter, Geneva Conventions I- IV

[42] Unable or Unwilling Doctrine is generally described as "the right of a victim state to engage in extraterritorial self-defense where the host is either unwilling or unable to take measures to mitigate the threat posed by domestic non-state actors, thereby circumventing the need to obtain consent from the host state". See, Williams G., Piercing the Shield of Sovereignty: An Assessment of the Legal Status of the "Unwilling or Unable" Test, University of New South Wales Law Journal, Vol. 36.2, 2013, pp. 625.

[43] Article 38 (1), statute of the International Court of Justice (ICJ)

and its Protocols I and II that govern armed conflicts both international and non-international. Besides, soft law and scientific literature were carefully consulted in the theoretical dimensions of the research by qualitative means, mainly because hybrid warfare is not subject to specific regulation. Case law in ICJ and relevant decisions play an important role in providing a comprehensive approach to the use of force and self-defense, in particular, Nicaragua v. the USA, Uganda v. DRC, Oil Platforms cases. And most recent ICJ case of "Ukraine v. Russian Federation" in 2017 on the Application of the International Convention for the Suppression of the Financing of Terrorism (ICFST) concerning the ongoing armed conflict in eastern Ukraine, and the International Convention of the Elimination of all Forms of Racial Discrimination (CERD) concerning the situation in Crimea.

A *Historical approach* was applied to analyze the evolution of warfare based on relevant scholars and theorists that contributed directly or indirectly to the modern warfare theories, mainly in highlighting the relationship between the theories of Sun Tzu and Von Clausewitz. Historical approach was applied to cover older and latest sources of literature, and previous and current effective legal acts while addressing the evolution of warfare from conventional to modern conflicts including hybrid warfare to assess and reveal the changes in legal understanding of the use of force in international relations, armed conflict, and its classification and to address the novel challenges of hybrid warfare features to existing laws.

The *comparative method* was used to reveal similarities and differences between the provisions and principles in both Jus ad Bellum and Jus in Bello with regards to Hybrid warfare. This comparative method has allowed for the understanding of the different rules that apply to cyber-attacks and non-state armed groups under different legal regimes. Additionally, it highlighted the main obstacles that can be identified in the classification of armed conflicts and the similarities in certain operations that can be active in both conflicts at the same time, such as the cyber-attacks launched by civilians and geographic limitation of conflicts of hybrid nature.

A *legal dogmatic* method was employed to analyze the established sources of international law to respond to the complex challenges of such forms, especially when dealing with the uncertainties of the applicability of Jus ad Bellum and IHL to hybrid means, particularly while discussing the attribution, state responsibility for wrongful acts, and the principle of distinction between combatants and civilians in the cyber context.

The *Inductive method* was used to identify the rules of law by the observation of their effectiveness in contemporary conflicts particularly the conflict in Ukraine and Syria due to their complex nature that is highly relevant while addressing hybrid warfare in practice.

Logical and Deduction methods were used to come up with recommendations and formulate conclusions for every chapter that served to complement and guide the author's analysis and theories to build up the relationship between hybrid warfare and international law.

Object, Aim, and Tasks of the Research

The *object* of this research is the treaty and customary international law relating to hybrid warfare. The object is therefore revealed through the challenging elements of Hybrid warfare, in particular the role of non-state armed groups and cyber-attacks, concerning the international law on the use of force, and the law of armed conflict.

The *aim* of this research is to analyze hybrid warfare by applying to it the relevant legal framework regulating the use of force in international law and law of armed conflict and to disclose whether contemporary international mechanisms can counter the lacuna from which hybrid warfare benefits the most, by extending the reach of international regulations, especially since hybrid warfare has been used recently in a quite wide sense that encompasses conflict involving the use of force in physical and non-physical use of force such as cyber-attacks. In doing so, certain elements of hybrid warfare and their impact on the applicable laws will be addressed, such as challenges imposed by cyber-attacks and non-state armed groups on the legal basis of State responsibility and principles of state sovereignty, also the impact of these elements on the classification of conflicts and its parties under the law of armed conflict or IHL.

Seeking to implement the aim of the research, it will require taking up the following tasks:

1- To disclose the genesis and development of the hybrid warfare concept, by describing and identifying its main elements that are at the core of the imposed legal challenges.
2- To unfold the developing concept of hybrid warfare and the confusion hybrid adversaries pursue using cyber means and employment of NSAs, by reassessing the international legal framework on the principle of non-use of force and its exceptions, territorial integrity, territorial sovereignty, and non-intervention principle that plays an important part of the international legal order.
3- To examine the capability of the hybrid means and methods in camouflaging the real identity of attackers, and the impact of uncertain attribution in the context of state responsibility for internationally wrongful acts under international law.

4- To identify the legal challenges imposed by hybrid warfare on the classification of armed conflicts and the impact of hybrid means in creating co-existing conflicts in a single battlefield.
5- To reveal the challenges imposed on the principle of distinction under the law of armed conflict and address the cyber means' effect in blurring the line of distinction between civilians taking part in hostilities and combatants.
6- To provide proposals and recommendations for potentially identified legal gaps at the international level to strengthen the legal resilience and help to better understand the application of international law and its ability to tackle the complexity of hybrid warfare in discussed areas.

Structure of the research

From a legal perspective, the research focuses on the warfare activities that establish the complex elements of hybrid campaigns in a very narrow sense, including military means amounting to armed interaction which raises classic questions both as regards the use of force and International Humanitarian Law. Yet, It would be impossible to start solving certain questions surrounding the legal complexity imposed by hybrid warfare and the legal applicability to such form of warfare, without examining, at least briefly, numerous aspects such as just war theory, use of force against NSAs within the targeted state and in the territory of another state, armed aggression, the concept of sovereignty and how it applies to hybrid means, and principles of non-intervention which is the corollary of every state's right to sovereignty, territorial integrity and political independence. And on the other hand, the classification of armed conflicts and basic principles of Jus in Bello, particularly the principle of distinction in contemporary conflicts that involve activities conducted by NSAs and individuals whose actions are not attributable to a state under the international law of attribution.

Therefore, for the sake of in-depth analysis, the research will be limited to the most relevant and problematic elements of Hybrid warfare. This will require unfolding the use of cyber means and the employment of non-state armed groups. The reason why the author of the present dissertation chose these two elements, as determined by the specificity of the main complexities highlighted, such as elements of an armed attack concerning new technologies (Ratione Materie, Personae and Temporis), difficulty of attribution in cyberspace, and control tests (Effective and Overall test), right to self-defense against non-state armed groups operating

from third state territory (proxy or self-motivated armed groups). Similarly, these elements were prioritized due to their direct impact on conflict classification of hybrid nature (IAC, NIAC, mixed conflicts), the parties to a conflict (cyber NSAs, geographic limitation of IHL), and blurring the line of distinction between civilians and combatants and their objects (civilian direct participation in hostilities through cyber means, dual-use infrastructure). Meanwhile, other elements are not less important (terrorism, criminal gangs, private contractors), but their physical participation is not as challenging as the elements highlighted above. Also, certain uses of cyberspace (such as cyber espionage, election interferences, and financial crimes) are excluded from the scope of this thesis, and it will be limited to elements that can potentially reach the threshold of armed attack or violence. Therefore, their examination is not pertinent and would widen the scope of the research.

On the other hand, addressing hybrid warfare in the context of IHL requires examining the rules of GCs and its APs that apply to IAC and NIAC, and determining if these rules can be exploited by hybrid adversaries through the employment of cyber NSAs, also the hybridity of these armed groups in contemporary armed conflicts with the extraterritorial effect of their operations. Similarly, in light of the above, it is important to assess the principles of IHL but due to the limited scope of the dissertation, the author will not examine in detail all principles but to the extent necessary. Therefore, the examination will cover the principle of distinction, particularly civilian direct participation in hostilities. That will require a deep exploration of conventional law, state practice, and case law.

The *structure* of the present dissertation is composed of an introduction, three parts, and conclusions. The structure is organized to facilitate the understanding of the warfare concept and its evolution from conventional to hybrid, the examination of international law and its applicability to hybrid warfare and identifying gaps that could be exploited by adversaries (cyber means, state and non-state armed groups).

Part one provides historical background on the evolution of warfare, precisely in the theories of Sun Tzu the "Art of War" and Carl von Clausewitz "On War", which has been recaptured by modern warfare theorists due to its importance and relevance to contemporary settings. Moreover, the section deals with the development in the legal interpretation and terminology of armed conflict through international documents and scholars' input, particularly in the post-UN Charter era. Whereas, the last section of this chapter focuses on the Hybrid warfare concept, through an overview of literature definitions, means of Hybrid warfare and concludes with describing the challenging features and means of hybrid warfare (non-state armed groups

and cyber operations). On the other hand, from a broader sense to the contemporary conflicts, the instrumentalization of the law (Lawfare) by States, both in international and domestic laws, to legitimize their actions and maintain freedom of maneuver and delegitimizes their adversary's activities and constrains their freedom of maneuver[44], is addressed as part of disclosing the genesis and development of the hybrid warfare concept.

Evaluating the legal development of conflicts and emerging elements introduced by hybrid warfare, the author argues that the discussed concept is not a new form of warfare and rather it has roots in the old theories of Sun Tzu and Von Clausewitz. Nonetheless, hybrid warfare falls short of all classic categorizations of conflicts, and rather it combines their distinct features in a single form creating a legal gray area. Consequently, certain challenges face the legal order due to the complexity of actors and new technologies, mainly because these elements rely on deniability and the tendency to avoid attribution.

Part two examines the applicability of Jus ad Bellum to the challenging elements of hybrid warfare. It observes the activities that violate the peace regime and threaten international security, also explores lawful use of force in the context of the UN Charter. Given that, the first section tests the theoretical bedrock on the prohibition of the use of force in international law to some of the most complex characters and means of Hybrid warfare (Cyber, Non-state armed groups). The analysis focuses on the means that could amount to the use of force in terms of armed aggression, the threshold of an armed attack, and the right to self-defense. In doing so, the required elements of armed attack (material and actor elements), principles of necessity and proportionality in self-defense, and the right to use force against NSAs operating from the territory of another state are evaluated. especially regarding the attribution test of effective and overall control in which it was noticed that more restrictive requirements that cover low-scale attacks are required. Also, this part of the research examines the ambiguity of attribution and its tests (effective and overall) that were found as inadequate in certain areas and reveals the complexity of cyber-attacks on State sovereignty and responsibility for wrongful acts. This part also analyses the Due Diligence rule as a potential remedy in the use of force against cyber-attacks.

Part three examines the Law of Armed Conflict or IHL concerning hybrid warfare. This part focuses on the general understanding of the Geneva Conventions and its additional protocols, classification of armed conflicts, and the parties of the conflict. First, as hybrid warfare blurs

[44] See, Dr. Sari A., Dear Geneva: Let's Talk Hybrid Warfare. A Reality Check, Conference Presentation at Geneva Centre for Security policy (GCSP), 2019.

the line of distinction between war and peace, it also confuses the classification of the conflict itself and the parties involved. So, the first section describes IAC and NIACs, and evaluate the distinction between the rules that apply to each type of conflict (mainly common article 2 and 3 to the GCs of 1949). Also, it addresses the challenges that arise from the employment of cyber NSAs and the geographic limitations of IHL in NIACs. This part of the research also examines contemporary co-existing armed conflicts (conflict in Syria as an example) that combine both IAC and NIAC to a single battlefield, and assess whether applicable rules are sufficient in addressing the complexity of hybrid means and methods, or eradicating the distinction between the rules that apply to each conflict would be advantageous to avoid such confusion.

Besides, the third part covers the principle of distinction which is a cornerstone for IHL. It mainly examines the distinction between civilian objects and military objectives, particularly in cyber operations, the legal challenges that arise from blurring the line of distinction between combatants and civilians taking direct part in hostilities (DPH) and evaluates the three cumulative elements for DPH (harm threshold, direct causation, and belligerent nexus) and the additional element of continuous combat function. This section of the research intensely focuses on cyber operations by civilian hackers and their ambiguous status in contemporary conflicts. This dissertation is finalized with conclusions.

Main Statements to be Defended

1. Hybrid warfare relies heavily on a combination of traditional means of warfare with modern technology and decentralized operations (Cyber operations, non-state armed groups, and Lawfare, etc.). The multi-modality of capabilities and resources creates legal asymmetry and exploits legal uncertainty in the current international law.

2. The international law regulating the use of force in international relations can deal with threats emerging from Hybrid warfare. However, deniability and lack of attribution, in addition to the higher threshold for establishing “effective or overall control” over hybrid actors, particularly in cyberspace, is eroding the norm of state responsibility for wrongful actions. The due diligence rule provides good practice in developing a preventive remedy and reduces the issues associated with the attribution due to the complex nature of cyber operations and the

role of non-state armed groups, the lack of a comprehensive approach in dealing with such operations, and the absence of a clear de minimis threshold.

3. Principles of non-intervention and non-interference are well established under international law to tackle the complexity of hybrid warfare. Yet, the ambiguity of hybrid operations that vary in their intensity create a legal challenge when examining coercive elements and left with no agreement on the criteria for certain elements (application of pressure, benefit for perpetrating party).

4. International Humanitarian Law can address the complexity of hybrid warfare, as it is designed through its two main sources the Geneva law as a body of rules which protect victims of armed conflicts, and the Hague law that consists of provisions that regulate the conduct of hostilities in armed conflicts and provides a clear distinction between international armed conflicts and non-international armed conflicts. As Hybrid adversaries tend to deny any involvement in a conflict, the legal regulation of non-international armed conflict applies in most scenarios that involve non-state armed groups, since the threshold for the applicability of international armed conflict is deliberately low. The co-existence of the two types of conflicts to a single battlefield is the dominant feature of modern hybrid warfare. The geographic limitation of non-international armed conflict must be defined precisely under the international humanitarian law upon the rise of cyber operations conducted from territories not involved in the conflict. All the previous loopholes allow certain justifications such as targeted killings and the “unable or unwilling” doctrine to be enforced by States, bringing a higher risk of global battlefields and its impact on international security and peace.

5. Hybrid warfare blurs the distinction between civilians, combatants, and their objects (civilian objects and military objectives), which is a fundamental principle of international humanitarian law. Therefore, the cyber-infrastructure of dual-use nature must be treated as civilian infrastructure even when used to conduct cyber operations, which will alleviate the complexities of distinction, particularly in the cyber-sphere. Also, the notion of direct participation in hostilities is not settled and does not sufficiently deal with the challenges of cyber operations in the hybrid warfare era, particularly regarding Direct causation, the threshold of harm, and the notion of continuous combat function.

I- The Emergence of Hybrid Warfare in the Evolution of Armed Conflicts

Traditionally, wars were waged between sovereign states and were regarded as the continuation of politics[45]. Today most armed conflicts are not only between states, but also other groups are significant combatants, where conflicts arise between internationally recognized governments and NSAs. The realist theory inspired by Thomas Hobbes considered that: "There is always a war of everyone against everyone", portraying that war as a natural condition to anarchy[46]. Firstly, the terminology could be puzzling especially regarding the terms "War" and "Warfare". The former is a state of political being or a condition, while warfare generally describes the methods or actions used to prosecute a war. Commonly said, one of the core characteristics of warfare, is the continuous development of new methods and means of conflicts to overwhelm adversaries with unexpected abilities. This is confirmed and recognized by Article 36(1) of the Additional Protocol to the Geneva Conventions[47] which states the following: "In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a high contracting party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by the Protocol or by any other rule of international law applicable to the high contracting party"[48]. Under international law, the term armed conflict has developed with the evolution of its means, as well as the involvement of non-state armed groups and the rapid evolution of modern technologies. This development has led to, a series of definitions drafted by scholars, a change in the legal understanding, the terminology of war, and the international law's categorization of armed conflicts. This development has evolved during the era of new forms of warfare by an obvious change in nature and character, from conventional to modern conflicts in the mid of the 20th century and the beginning of the 21st century.

Therefore, for this chapter, the first part examines the evolution of warfare and the theories that have a direct or indirect impact on the modern nature of the conflict, in particular, the Sun Tzu's theory on Art of War, which is perhaps the oldest and one of the most widely read classics of military strategy introduced 2500 years ago and providing a unique insight into modern

[45] Quenivet N. and Shah-Davis S., International Law and Armed Conflict, Challenges in the 21st Century, T.M.C Asser Press, Hague 2010, p. 3.
[46] Thomas Hobbes, Leviathan, I00, 1651, Michael Oakeshott eds., Collier 1962.
[47] Wolf Von Heinegg, Robert Frau and Tassilo Singer, Dehumanization of Warfare "Legal Implications of New Weapon Technology" Springer International Publishing, 2018, p.1
[48] Protocol Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, art. 36/1.

conflicts, quoting Sun Tzu's famous statement: "to subdue the enemy without fighting is the supreme excellence".[49] Also, Von Clausewitz's theory of war constituted war as the continuation of politics by other means[50]. Clausewitz wrote his seminal work "On War" in an era dominated by inter-states conflicts, which explains his state-centric approach to conflicts. Moreover, the chapter will highlight theories of Hugo Grotius that has much to say about the dividing line between war and peace and its impact on the development of the legal regime applicable to armed conflicts and peace resolution throughout history, nonetheless is highly challenged in modern conflicts as such dividing line is not acknowledged practically by states and NSAs.

Further, the second part unfolds the shift from conventional to modern warfare, the involvement of irregular proxy warriors, and the employment of new technologies, by highlighting the challenges that face the existing international norms governed by treaties and customary international law. The St. Petersburg Declaration 1868 which has the force of law, confirms customary rule to which the use of arms, projectiles and material of a nature to cause unnecessary suffering is prohibited. The international community intended to regulate new technology of warfare. St. Petersburg Declaration framed the usage of weaponry for any future development by stating that: "The only legitimate object which states should endeavor to accomplish during war is to weaken the military forces of the enemy."[51] In this case, analyzing the changing characteristics of modern armed conflict and their development in contemporary battlefields from regular to irregular wars that include the hybridization of warfare following the UN Charter era, will be essential.

Also, it discusses the development of the legal interpretation of armed conflicts by highlighting the evolution of its legal terminology from war to armed conflict, and the classification of the latter by relevant legal concepts mainly IHL, that drew a line of distinction between international and non-international armed conflicts, which was later challenged by the use of irregular means of war precisely hybrid warfare means.

The third part of this chapter will discuss the definition of Hybrid warfare, by an overview of previous literature and the scholars' understanding and definitions of this term. Then the study

[49] Sun Tzu, The Art of War, The Book of Lord Shang, Wordsworth Editions Limited (1998), p. 25.
[50] Carl von Clausewitz, On War, M. Howard and Paret, P. (eds.), Princeton University Press 1976.
[51] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight (hereinafter the 1868 Saint Petersburg Declaration), Saint Petersburg, 11 December 1868. The Declaration of Saint Petersburg is the first formal agreement prohibiting the use of certain weapons)

will examine the ongoing debate about the novelty of hybrid warfare whether it is considered a new phenomenon or not. Admittedly, the term has no consistent definition so far, it could include irregular, conventional tactics in the battlespace, and non-military means for strategic objectives[52]. And finally, the chapter highlights the challenging elements of hybrid warfare that the present dissertation analyzes under applicable laws

1. The Evolution of Warfare from Conventional to Modern

Warfare refers to the common activities and characteristics of types of war, or of wars in general[53]. Some scholars see war as a universal and ancestral aspect of human nature, while others consider war a result of specific socio-cultural or ecological circumstances. Marven Friend, for example, defines war aims as "The desired territorial economic, military or other benefits expected following successful conclusion". The multiformity of the phenomenon 'war" makes its definition extremely difficult[54]. For instance, Hugo Grotius defined war as: "the condition of those contending by force, viewed simply as such". While the Russian proposal, that was submitted to the Brussels conference 1874 defines international war as "A condition of an open struggle between two independent states and between their organized and armed forces"[55]. This definition applies more to war as de facto rather than to war as de jure or a state of war. It is important to differentiate between the two concepts, as numerous armed conflicts involve widespread hostilities but were not considered wars in the formal sense, such as the British attack on the Danish fleet in 1801 and 1807, by which the Secretary-General of the League of Nations in 1927 considered, from a legal point of view, that the state of war between two states depends upon their intention and not upon the nature of their acts[56].

To demonstrate, before the 20th century, the debate was on drawing a distinction between just and unjust wars, by which the requirement of valid justification for the lawful war was reflected in the Christianity and was elaborated by St. Augustine in the 4th century, who despite his beliefs that Christians should be pacifists, made an exception for fight defensively or in the defense of innocents. The latter has strongly influenced medieval scholastics such as St. Thomas Aquinas and continued to develop until the 16th century by the Spanish jurists such as

[52] This understanding is echoed in the Wales Summit Declaration issued by the head of States and governments of the member countries of NATO on September 5, 2014.
[53] Warfare, Cambridge Dictionary, Retrieved 1, August 2016.
[54] I. Paenson, Manual of The Terminology of The Law of Armed Conflicts and of International Humanitarian Organizations, Bruylant Nijhoff, 1989, P. 2
[55] P.S. Romashkin "Prestuplenie Protiv Mira I Chelovechestva" Moscow, 1967, p.84
[56] Ibid. p. 4.

F. De Vitoria and D. De Soto[57]. Just war has developed and influenced later the right to resort to use force or jus ad Bellum. In the 19th century, there has been a legal development through a historical process of overcoming the moral theological approach of just war (Bellum Justum)[58]. That was spotted by the behavior of the European states that loosened their moral bond criteria for the interest of the sovereign right to go to war. As a result, Wilhelm G. Greeve wrote: "Whenever the problem of war was seriously discussed from an international law perspective, the principle of the freedom to wage war emerged."[59] The uncertainty of war and peace in the 19th century is nonetheless reflected in nowadays conflicts influencing both political practice and the legal doctrine, as to whether preventing and humanizing the conflicts or accepting war as a political instrument[60]. Modern conflicts and their means can be understood by examining them to older theories. For example, Immanuel Kant rejected the inhumanity of wars and their sufferings. In his proposal on "Perpetual Peace", he demanded complete legalization and instrumentalization of national and international law to evade wars, refusing by that the notion of a right to go to war, but instead endorsed the legal prohibition of the latter (jus contra Bellum)[61]. On the other hand, Georg Hegel agrees with Kant on the horrors of wars, nevertheless rejects the universal perpetual peace project and the binding power of the international law, conversely, he stressed the certainty of state sovereignty, as for Hegel war is right to states and legitimate mechanism for dispute settlement[62]. However, for the interest of this chapter and to relate previous theories to contemporary conflicts of hybrid nature, the influential work of Sun Tzu on "the Art of War" and Carl Von Clausewitz on "On War" who considered "war a clash between major interests that are resolved by bloodshed and that is the only way it differs from other conflicts"[63], are remarkable in the way they contribute to this matter. Also, an analysis of the context of war is essential to understand the evolution of theories of warfare, of which hybrid warfare is one of the most recent[64].

---

[57] I. Paenson, Manual of The Terminology of The Law of Armed Conflicts and Of International Humanitarian Organizations, Bruylant Nijhoff, 1989, p.8

[58] Simon, H., The Myth of Liberum Jus ad Bellum: Justifying War in the 19th-century Legal theory and Political practice, The European Journal of International Law, Vol. 29 no. 1, Oxford University Press 2018, p. 114.

[59] Grewe, W.G. The Epochs of International Law, translated and revised by Michael Byers, 2000.

[60] Simon, H. Ibid. p. 118

[61] Cf. Habermas, 'Kant's Idea of Perpetual Peace, with the Benefit of Two Hundred Years' Hindsight', Edited by J. Bohman and M. Lutz-Bachmann, Perpetual Peace: Essays on Kant's Cosmopolitan Ideal, 1997, p. 113.

[62] Simon, H. ibid. p. 118

[63] C. Von Clausewitz, On War, Edited and Translated by M. Howard and P. Paret, 1976, p.75

[64] Amos C. Fox, Hybrid Warfare: The 21st Century Russian Way of Warfare, School of Advanced Military Studies, United States Army Command and General Staff College Fort Leavenworth, Kansas, 2017, p. 10.

1.1. Sun Tzu's Art of War

Sun Tzu's book presents itself as a collection of sayings by Master Sun or else known as Sun Tzu, a General and military advisor at times of ruthless struggles between rival kingdoms decimated China's population. Therefore, countering the slaughter was by developing strategic thought that placed a premium on victory through psychological advantage and preached the avoidance of direct conflict. Sun Tzu stresses the unorthodox or indirect approach as an element of psychology in warfare that was employed by Chi Minh and Vo Nguyen in the Vietnam War that relied on indirect attack and psychological combat against France and later the USA, which had its impact on the USA's frustration in the Asian wars according to Henry Kissinger. [65]

To illustrate, for Sun Tzu, the art of warfare is deceit and the highest excellence in the war was not in winning every battle, but in subduing the enemy's force without having to engage it in battle[66]. Strategic Dominance is central in Sun Tzu's treatise when the balance of forces shifts in one's favor, also known as "Shih". His theories merge the military strategy and political domination to achieve victory, as battles have become unnecessary in his opinion. Various theories stressed in the Art of War, have a direct link to modern conflicts, for example winning battles without fighting and overthrowing the enemy state without protracted war.[67] That matches the main aim of hybrid warfare that relies on low-intensity operations that do not cross the threshold of armed attacks or armed conflict. Furthermore, Sun Tzu's hybrid approach is revealed in his understanding that once the interconnectedness of everything in warfare is established, success depends on the accuracy of the strategist's calculus weighing each component's relative importance, therefore war depends on rationality.[68] The hybridity in Sun Tzu's theory is also reflected in writings to "Chi and Cheng", the former is most commonly orthodox or traditional while the latter is unpredictable or unorthodox[69]. In this regard, Sun Tzu promotes the combination of conventional and irregular means in a multimodal and interchangeable manner through which a conventional (chi) force can turn into unconventional (cheng) force, and vice versa depending on the adversary weakness and strength. This strategy

[65] Henry Kissinger, On China, The Penguin Press, New York 2011, Chapter 1.
[66] Sun Tzu, The Art of War, Ibid. 104.
[67] See Sun Tzu, The Art of War, Trans. John Minford, New York: Viking, 2002, p. 3, 14-16
[68] Nicholas Morrow, Sun Tzu, The Art of War (500-300 B.C.), John Hopkins University SAIS, Classics of Strategy and Diplomacy, November 24,2015.
[69] Macdonald Ch., The Science of War: Sun Tzu's Art of War re-translated and re-considered, Earnshaw Books Ltd, ed.2017, p. 33

can also be understood as an interrelated use of military and non-military means, in other words, hybrid warfare.

Additionally, for Tzu, victory is not the main objective of armed forces, but it is achieving the political objective that the military clash was intended to secure, by which everything is connected and not isolated in a military or strategic contest, from weather, diplomacy, historic perceptions, and the intangibles of surprise and morale. The main objective is observing the adversary, defining it carefully, then striking the enemy's weakest point[70]. Therefore, the art of war theory articulates a doctrine less of territorial conquest than of psychological dominance which addresses the necessity to correctly grasp and evaluate the intentions, traits, and patterns of the enemy's decision-maker[71]. Sun Tzu has devoted the whole chapter to espionage, as a tool to gather intelligence about one's adversary and considered it an important tool available to political and military leaders which is why he emphasizes "the need for meticulous intelligence-related preparations before the outbreak of war and preceding each campaign and battle".[72] So in his understanding of the dynamic world, he describes how there is nothing constant or predictable in warfare.

To sum up, the analyzed context of Sun Tzu's writings proves the role of hybridity within his strategic understanding of waging wars. This has been explained at the operational level through the convergence of conventional and non-conventional means, like irregular warfare and compound warfare. The fusion element of different means to a single battlefield (Chi and Cheng) lies in the core of hybrid warfare and Tzu's theory. Additionally, the importance of military and non-military means based on ambiguity and deniability are equally found in Sun Tzu's Dialectic of harmony and chaos (Ho and Luan) that highlighted the importance of military actions combined with non-military means such as diplomacy economic pressure, or deception[73], by creating uncertainty and confusion to the adversary with regards the deposition of forces, military plans and intent or division of alliances. Therefore, most of Sun Tzu's ideas can be recognized in contemporary state-led hybrid warfare. Nonetheless, nowadays it is seen to be more complex and potent because it includes novel irregular and technological methods along with tools of political warfare that are generally available for States.

---

[70] Joseph Needham and Robin D. S. Yates, Science and Civilization in China, Vol. 5, Part 6: "Military Technology Missiles and Sieges", Cambridge University Press, Cambridge 1994, p. 33–35, 67–79.
[71] Yuen D., "Deciphering Sun Tzu", Comparative Strategy 2008, vol. 27, p. 190.
[72] Handel M., Masters of War: Classical Strategic Thought, London Routledge 2001, p. 177
[73] See examples, O'Dowd E. and Waldron A., Ibid. p. 27

1.2. Clausewitz Theory of War

On the other hand, Western strategists are heavily influenced by the theories of the Prussian soldier-scholar Carl Von Clausewitz that were based on the experience of Napoleonic wars, and his statement was developed based on the Driefontein Consolidated Gold Mines vs Janson case[74]. Clausewitz's observation of armed conflict is related to violence or resort to force by one of the parties, as his notion of war is the need for violence delivered through combat to be for a political or policy purpose. Violence as a fundamental criterion of war in Clausewitz's sense is not applicable in modern conflicts, as many means of armed attacks or conflicts could not be considered violence, however, can fit in the context of war. In this matter, non-violent means had no attention in Clausewitz's On War theory, for his definition is combat-centric, especially since non-violent means had been central in various types of conflicts from the cold war to the hybrid warfare conducted in Ukraine and other states[75]. Besides, violence can be delivered by organized groups such as criminals or drug gangs that can conduct activities reaching the intensity of violence, however, their actions cannot be considered as engagement in armed conflict but are dealt with by law enforcement.

Clausewitz's description of the war between only states has been criticized by theorists of the 21st century, such as Can Creveld that considered: "Organized violence should be called war if waged by the state, for the state or against the state."[76] The military campaigns that Clausewitz was familiar with, were between states and their armed forces with civilians largely uninvolved in the hostilities, in which it can be labeled as regular war. On the contrary, contemporary conflicts affect civilians directly even if they were not involved in the hostilities, even more than combatants who are legitimate targets in armed conflicts. Such conflicts are described as Irregular wars involving non-state armed groups such as the conflict in Syria (Hezbollah, PKK, ISIS, Ahrar AL Sham, and many others), same in Ukraine (Little Green Men) irregular paramilitary forces with pro-Russian agenda. That is what labeled the hypothesis of Clausewitz as state-centric and applicable to regular warfare, but difficult to apply to armed conflicts conducted by rebellion, insurgency, and criminal activities.

---

[74] I.A Shearer,Ibid.
[75] Simpson, E., Clausewitz's Theory of War and Victory in Contemporary Conflict, Exploring War's Character, and Nature, 2018, P.11.
[76] Van Creveld, M., The Transformation of War. London 1991, Brassey, p.36

One of the crucial statements of Von Clausewitz in "on War", was his dismissal of international law as being considered irrelevant[77], which further implies that the type of war he is dealing with is interstate. However, such a statement is not surprising due to Clausewitz's state-centric forms of understanding wars, and it also reflects the classification of war at times the idea of a state of war necessitated a declaration of war between sovereign states or in other words the regular war[78]. Yet, Clausewitz recognized the changing and evolving nature of wars considering that it has always been a "chameleon" that is ever-changing, adapting to new circumstances and camouflaging itself in international relations, national security, and political rhetoric. So, Clausewitz acknowledges the development in means of warfare, but he does not consider that it creates any change to the concept of war or its nature. It is important to note that hybrid warfare is a derivative of the Clausewitzian notion, that war is a continuation of politics by other means. This is highly relevant to the argument that hybrid warfare is not new but goes back to the discussed theories.

In addition, Clausewitz ignored the importance of how the parties themselves represent the conflict for whether a conflict counts as a war or not. So, one of the most important contextual parameters concerning whether a conflict can be classified as war or not is how the parties to the conflict represent it[79]. This can be classified as a perspective-dependent feature of modern conflicts too, including hybrid warfare, through which understanding different views of the parties involved in the ambiguous situation is critical, providing insights into each party's level of commitment and how far each may be willing to go in pursuing their objectives[80].

To summarize, Clausewitz considered that warfare is violent with an instrumental character in reaching political goals and that wars are wars no matter what might develop in the future. This had a great impact on the notion of conventional warfare. Even though Clausewitz took a war for granted, liberal lawyers like Caspar Bluntschli (co-founder of the Institut de Droit International) and Prof. Henry Bonflis believed in the possibility of international peace through law and were in favor of legal prohibition of war[81]. The theory of international peace was also

[77] Simpson, E., Ibid. p. 12
[78] The Swiss International Lawyer Emer De Vattel (1714–67), Changed the Latin Bellum Solemne (Formal War) in the Work of Hugo Grotius (1583–1645), Into the French Guerre en Forme (War in Due Form), Which he also called Guerre Règlée (Regulated or Regular War). See, Emer De Vattel, Le Droit De Gens, Ou, Principes De La Loi Naturelle, Appliqués À La Conduit Et Aux Affaires Des Nations Et Des Souverains, Buffalo, New York, W. S. Hein, 1995, p. 507.
[79] Almang J., War, Vagueness and Hybrid war, Journal of Defence Studies, 2019.
[80] Kapusta Ph., Ibid., p. 4.
[81] Simon, H. Ibid. p. 120.

faced by criticism of the liberal theories that considered it impossible and unthinkable. Those who opposed the theory of legal prohibition of war supported the legitimacy of wars as an honorable and important procedure of international relations.

To conclude, the relevance of the two theories presented by Sun Tzu and Clausewitz are solid to contemporary conflicts, though it varies due to the framework of both. The Art of War is devoted to the strategies of actual fighting and the role of military operations with diplomacy is broader than the framework of On War that is concerned with the art of waging war and considers that war begins when diplomacy has failed. On one hand, Clausewitz's ideas about hybrid nature of warfare that was described war as a chameleon, and on the other hand Sun Tzu's strategic dimensions of war and thoughts on intelligence in asymmetrical wars, both explained the dynamics of all types of contemporary conflicts, including its hybrid nature. And despite the assertion by Clausewitz that the laws of war are hardly worth mentioning, they remain the most reliable answer to the opposing tensions of the necessities of war in modern times.

1.3. The Changing Character of Modern Conflicts

Analyzing contemporary conflicts, particularly in the Middle East after the Arab Spring, Eastern Ukraine and the Annexation of Crimea, armed conflict in South Lebanon, sophisticated cyber-attacks such as Stuxnet and the attack that targeted Estonia, the conflict in Abkhazia and Russian interference in Georgia, in addition to the ongoing conflict in Yemen that has different factors to address as to whether it is considered a NIAC or IAC, is important to understand the modern conflicts and their complexity. All the previous examples sum up that modern conflicts are no longer the same, new means blended with old methods of warfare highlighting a shift by character, nature and creating a challenge to international peace and security[82]. Modern conflicts no longer apply regular and irregular forces in different areas of the conflict as separate efforts, rather combine them in a single domain. Wars that were traditionally between armed forces of established states, fighting for clear political and strategic objectives with armed forces overtly identified by their uniforms and guided by ethical codes of honor that regulate combat[83], are shifting by the increasing level of participation of new entities that are no longer limited to States. That is creating a legal misperception and complexities to the

[82] Al Aridi, A., How Hybrid Is Modern Warfare? Conference Paper at the 5th International Conference of PhD Students and Young Researchers, International Network of Doctoral Studies in Law, Vilnius 27-28 April 2017, p.8

[83] Ignatieff, M., The Warrior's Honor: Ethic War and Modern Conscience, Holt Paper Backs, New York 1998.

principles of IHL and the International Law on the use of force. Wars in the line with Carl von Clausewitz's military theory have been waged between states in conformity with international humanitarian law, while for instance today's example of the western war against Islamic State, is an asymmetrical conflict, facing an insurgency and hybrid armed group using guerrilla tactics and other non-military means such as propaganda and phycological warfare to avoid any army-to-army confrontation.[84]

The development of IHL after Henry Dunant's experience in the battle of Solferino in 1859, which witnessed dramatic suffering of injured, led to the adoption of the Geneva Law dealing with the treatment of war's victims, and the Hague law regulating weapons and methods of warfare. However, the time of traditional battles between opposing sides lined up in squares and columns in a battlefield, where troops use to be sure who and where their enemies were, is no longer the fashion. Modern conflicts that have proliferated in the last two decades are not state-centric anymore. Now battlefields include NSAs that include gangs, criminal organizations, radicals, or cyber hackers. Such new forms of warfare were introduced by the fourth-generation warfare theorists[85]. Modern conflicts are contention between two or more states through their armed forces and international law currently recognizes two disparate types of conflict, interstate (between two states or more) and intrastate (NIAC). Eventually, a decline in the number and intensity of inter-state conflicts was noticed in comparison with the rise of intra-state or internal conflicts presenting the predominant facade of modern conflicts. Therefore, our legal understanding and professional lexicon should evolve parallel to the evolution of warfare.

1.3.1 Conventional Warfare

Warfare can be presented in various forms; it reflects the political will through the use of military forces specifically tailored to apply state-sponsored violence and operate decisively against adversaries as well as a fight by convention[86]. Conventional warfare is the use of

[84] Rudderhof, R., From Classic Wars to Hybrid Warfare, Peace Palace Library, July 27, 2017. https://www.peacepalacelibrary.nl/2017/07/from-classic-wars-to-hybrid-warfare/

[85] Hammes, T.X., The Sling and The Stone: On War in the 21st Century, St. Paul: MN Zenith Press, 2004, p. 321. Hammes defined Fourth Generation Warfare as "evolved from upheaval, unfamiliar with conventional definitions of warfare, blurred lines between war and peacetime, have no fronts and battlefield, wiping out the exact distinction between civilians and soldiers, fighting actors may be nonstarters as well as states, a kind of warfare that classical guerrilla and terrorist operations are revised and modernized of."

[86] Langford, I. Finding Balance between the Conventional and Unconventional in Future Warfare, The Strategy Bridge, 4 December 2018 https://thestrategybridge.org/the-bridge/2018/12/4/finding-balance-between-the-conventional-and-unconventional-in-future-warfare.

traditional means to wage war, a form of warfare between states that employs direct military confrontation to defeat an adversary's armed forces, destroy an adversary's war-making capacity, or seize or retain territory to force a change in an adversary's government or policies. The first and second World Wars, the Korean war and the Desert Storm, are examples of conventional battles between States with uniformed forces under strict hierarchical military command and following a military strategy to fight clear and present military targets with the conformity of international humanitarian law, jus ad Bellum and other rules[87]. Such wars used to end with either total victory, unconditional capitulation, or a peace treaty. However, contemporary conflicts and the engagement of hybrid non-state armed groups or proxy fighters keep the conflict ongoing, and any total victory in the conventional sense of battles would be an illusion. Also, conventional warfare takes place in the physical world and has tangible effects recognizable to all parties. While nowadays conflicts with cyber dimensions, are intangible yet have a direct kinetic effect[88]. So, what distinguishes modern conflicts from conventional ones is the growing influence of NSAs, the tools available to them, and the velocity of change[89].

The regulation of warfare by international law was conventionally a set of distinction rules. The right to use force (jus ad Bellum) was determined by the absence or presence of an actual armed attack, and the regulation of hostilities in the law of armed conflict (jus in Bello), which is based on the principles of distinction between combatant and non-combatants (non-military targets)[90]. And the most prominent distinction was between Jus ad Bellum and Jus in Bello, where in the latter, the aggressor (including an aggressor occupant) enjoyed equal privileges during combat as the victim.

1.3.2. The Irregular Warfare/ Asymmetric Warfare

Unconventional warfare that emerged in the late 1980s, is the use of irregular methods to counter the traditional advantage of stronger opponents and rather favors indirect and asymmetric warfare approaches. The unconventional forces are not equally articulated with no clear policies, resources, and defense portfolio as conventional ones[91]. While the law of armed

[87] Ridderhof, R., From Classic Wars to Hybrid Warfare, Ibid.
[88] Hayatli Z., Cyber Warfare in International Law, the New Jurist 2018.
[89] Kapusta Ph., United States Special Operations Command, White paper: The Gray Zone, September 9, 2015, p. 5.
[90] Benvenisti, E., The Law on Asymmetric Warfare, Martinus Nijhoff Publishers, 2010, p. 933.
[91] Langford, I., Ibid.

conflicts was designed to deal with parties engaged in a states-centric type of warfare, an asymmetric engagement which is mainly between belligerents of unequal military power and strategies is different. The Joint Publication 1-02 of the U.S. Department of Defense has defined irregular warfare as "a violent struggle among state and NSAs for legitimacy and influence over the relevant population. Irregular warfare favors indirect and asymmetric approaches, though it may employ the full range of military and other capacities, to erode an adversary's power, influence, and will."[92] Such tactics are employed by Jihadis using insurgencies, hit and run guerrilla tactics, to avoid confrontation with conventional troops. The latter concept is part of hybrid warfare that is based mainly on the simultaneous use of traditional and irregular military means, its main aim is to subjugate power rather than focus solely on gaining military victories.

The legitimacy of warfare was framed through international treaties based on moral and humanitarian principles. The 1907 Hague Regulations criminalized the behavior of the dominant powers in the 17th and 18th centuries that used irregular troops to exploit civilians, an attempt to make wars more humane, and such attempt depended strongly on the political interest of these powers that suffered from the irregular militias[93]. Though Irregular and asymmetric war (often known by Fourth Generation war "4GW") is considered an element of hybrid warfare and used by some for referring to the latter, there is a difference between both. Irregular warfare is between parties whose military power and strategy are not equal. Hybrid warfare has both state and non-state features, hybrid armed groups can change simultaneously from irregular forces to state forces, a combination that creates a challenge to what legal model applies to it. That is the reason why some authors proposed to divide the conflict in Ukraine, into two different legal precedents: Internal armed conflict (Ukraine v. Donetsk People's Republic (DNR) / Luhansk People's Republic (LNR) and International armed conflict (Ukraine v. Russia)[94]. Otherwise, if combined it will bring to light the first complexity of hybrid war, which is the complexity of classifying an armed conflict in a single battlefield.

[92] Joint Publication 1-02, Department of Defense: Dictionary of Military and Associated Terms, 8 November 2010 (Amended through 15 February 2016). See also, Joint Operating Concept, Irregular Warfare, Ibid. p. 9.
[93] Watkin, K., Warriors Without Rights? Combatants, Unprivileged Belligerents, and the Struggle Over Legitimacy. Harvard University Program on Humanitarian Policy and Conflict Research Occasional Papers, 2005. p.20.
[94] Vlasiuk V., Hybrid War, International Law and Eastern Ukraine, European Political and Law Discourse, Vol. 2, Issue 4, 2015, p. 16.

2. The Development of the Legal Terminology of Armed Conflicts

Under international law, there is no binding definition of "War", especially as the law has evolved in new directions after WWII giving the way to the notion of "Force (UN Charter) and Armed Conflict (Geneva Conventions)"[95]. In the period following the peace of Westphalia and till the end of WW II, the international law of war applied only to conflicts between states[96], while internal conflicts were not treated as real wars in the strict sense of international law interpretation to wars.[97] However, the understanding of war as a condition that can occur only between states has lost its potency. For example, common article 3 of the Geneva Conventions 1949 has assured the recognition of belligerency and that certain fundamental norms of the law of war to conflicts involve NSAs for the subsequent evolution of the law of NIACs[98]. In addition, article 2(1) of the GCs introduced the notion of armed conflict, thereby expanding the application of IHL and making it less dependent on the formalism attached to the notion of declared war. GCs in this sense have played a major role in shaping the "armed conflict" notion that also covers any sort of foreign military occupation, even if such occupation does not meet with armed opposition during or after the invasion.

The importance of the shift in terminology goes back to the times before the Geneva conventions, where "war" was considered a state opposed to the state of peace. The 1907 Hague convention III states that "a formal declaration of war is required to apply the law of war in the relation between two parties". Historically, the declaration of wars was state-centric and any other resort to force without the state's authority would be considered as an act of lawlessness[99]. That has allowed the states to avoid their commitment to such laws, by simply not declaring war. The change in the legal interpretation of armed conflicts had a positive impact on the behavior of states and non-state armed groups, that will be held responsible for their hostile actions even with no formal declaration of war.

[95] Sari, A., Hybrid Warfare, Law, and the Fulda Gap, Complex Battle Spaces, The Law of Armed Conflict and the Dynamics of Modern Warfare, Lieber Series, Volume I, Ed. Christopher Ford and Winston Williams, Oxford university Press 2019, p. 177.
[96] Bartels, R., Timelines, Borderlines and Conflicts, International review of the Red Cross, 2009, p. 35-44.
[97] Akande, D., Classification of Armed Conflicts: Relevant Legal Concepts, Oxford University Press, 2012, p. 31-32
[98] Sari, A. Ibid. p 177
[99] Brunne, J., The Meaning of Armed Conflict and the Jus ad Bellum, Martinus Nijhoff Publishers, 2012, p. 45.

In addition, based on the work of the International Law Association[100], it became clear that the international community has a definition and it no longer uses the term "War" but rather "Armed conflict". A situation that may be treated for purposes of international law as armed conflict is not a matter that a national leader may simply decide at his discretion, it is not a political question or policy issue, it is a legal question of the greatest importance that can be distinguished from peace where human rights and other laws prevail[101]. Similarly, international lawyers have abandoned using the term war and replaced it with armed conflict. That could be explained in line with Greenwood's statement that "there could be a war without fighting and fighting without war."[102] Most of the conflicts after WW II were addressed as armed conflicts. For example, the British Lord Privy Seal of 1 November 1956 stated: "Her majesty's Government do not regard to their present action in the Suez Canal as constituting war, there is no state of war, but there is a state of conflict."[103] Nowadays, formally declared wars are rare in international relations, however, neither a formal declaration of war nor the formal recognition of a state of war is necessary for an armed conflict to occur or for IHL to be triggered[104]. Under Jus Ad Bellum, the terms "war" and "armed attack" are of particular significance. The former in classic pre-charter was the international law term to describe the situation of armed conflict between states. But as the current United Nations Charter prohibits all use of force except in self-defense or with Security Council authorization, governments and jurists began to abandon the use of the term "war". Interestingly, States have lost their grip on the monopoly over violence, by which the number of inter-state conflicts has declined, while the number of NIACs and internal unrests has considerably increased. In the same sense, many NIACs have been internationalized by the intervention of other States in support of one or more of the warring parties, at the same time technological developments have rendered contemporary conflicts more asymmetrical.

[100] The International Law Association, founded in Brussels in 1873, its main objective under its constitution is to study, clarify and development of international law, both public and private, and the furtherance of international understanding and respect for international law. The ILA executive council tasked its committee on the Use of Force with reporting on the definition of war in international law. See, Mary Ellen O'Connell, What is War? An Investigation in the Wake of 9/11, International Humanitarian Law Series, Martinus Nijhoff Publishers, Boston 2012, p. 8-9

[101] Mary Ellen O'Connell (ed.), What is War? An Investigation in the Wake of 9/11, Ibid., p.9

[102] Ch. Greenwood, The Law of War (IHL), MD Evans Ed., International Law, First Edition, Oxford 2003, p. 791-792

[103] I.A. Shearer, Staeke's International Law, Butterworths, II edition 1994, p.478

[104] Articles 2 and 3 of the Geneva Conventions 1949.

2.1. Armed Conflict and the International Humanitarian Law

Jus in Bello or the law of Armed conflict (LOAC)[105], is applicable in situations of armed conflicts. So, the question that rises, when a situation is considered an armed conflict? And what are the types of such conflicts? In this matter, the LOAC distinguishes between two types of conflicts, International Armed Conflict (IAC) and non-International Armed Conflict (NIAC). And while the four Geneva conventions 1949 used both terms, war and armed conflict, it indicated that armed conflict comprises war, but is of a broader scope.[106] Similarly, civil wars were substituted by NIACs, by which inclusion of Common Article 3 to the GCs of 1949 was one of the reasons for using the term "Armed Conflict" rather than "War"[107].

2.1.1. International Armed Conflict (IAC)

International Humanitarian law did not clearly define the IAC, where such conflict is derived from the common article 2 of the GCs 1949, which voices the application of the convention to armed conflict even if the state of war is not recognized by one of the parties[108]. The article states that "the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the high contracting parties even if the state of war is not recognized by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance."[109]

Under the IHL, IAC requires opposition of high contracting parties, in other meaning a conflict between the legal armed forces of two different states, even if one party of the conflict does not recognize the government of the adverse party or no formal declaration of war noticed[110], and it makes no difference how long the conflict lasts or how much slaughter takes place[111]. Moreover, according to the ICRC, neither the duration nor the intensity plays a role in blocking the applicability of IHL to such conflicts[112]. Also, it is important to bear in mind

[105] Law of armed conflict (LOAC) and International Humanitarian Law (IHL) are used interchangeably.
[106] Elizabeth Mikos-Skuza, Ibid. p. 23.
[107] Ibid. p. 25
[108] Greenwood, Ch. Ibid. p.47.
[109] Geneva Conventions (I, IV) 1949, Application the convention, Ch. 1, Common Article 2.
[110] Ibid.
[111] Commentary to the third Geneva Convention, J. Pictet ed., ICRC, 1960, p.23.
[112] Jean Pictet ed., 1952, ICRC commentary to Article 2 of the first Geneva Convention, p. 23, See also Yves Sandoz et Al. ed. 1987, the ICRC Commentary to Article 1 of Additional Protocol I.

that armed conflict can arise where a state uses unilateral armed force against another State even if the latter does not or cannot respond by military means. Moreover, AP I extended the definition of the IAC to cover armed conflicts to fight against colonial domination, alien occupation, or racist regime in the exercise of their right to self-determination or what is called wars of national liberation.[113]

Furthermore, the ICTY in the Tadic case, considered that "an armed conflict exists whenever there is resort to armed force between states[114]". State practice proved that IAC is hardly concluded by a peace treaty, and the end of such conflict stays foggy even with ceasefire agreements that give a de facto situation to have the effect of permanent termination of hostilities. But the ICTY in Tadic Case opined that "IHL continues to be applied in IACs until a general conclusion of peace has been reached[115]". So, as the IHL applicability is seized with the end of IACs, yet according to the 32nd ICRC international conference, this issue is still complex and vague, and the ICRC believes that hostilities must end with a degree of stability and permanence for the termination of an IAC.

2.1.2. The Predominance of Non-International Armed Conflict (NIAC)

Internal Armed conflicts are mainly the use of force within the boundary of one state, with the involvement of one or more-armed groups and the government forces, or between those armed groups. According to Bert Roling ", the laws of war derive their authority, during a war, from the threat of reprisals, prosecution, and punishment after the war."[116] In this matter, conventional law applicable to domestic armed conflicts before the adoption of the Statute of the International Criminal Tribunal for Rwanda did not establish individual criminal responsibility for war crimes committed in such conflicts accompanied by a lack of enforcement mechanism[117]. Nonetheless, NIACs are often called internal armed conflict or traditionally "civil wars". Historically such Intra-state violence can be three types: First is

[113]Additional Protocol to the Geneva Conventions of 12 August 1949 and relating to the protection of Victims of International Armed Conflicts (Protocol I), Article 1(4), 8 June 1977.
[114]ICTY, The Prosecutor v. Dusko Tadic, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, para. 70.
[115] ICRC, 32nd International Conference of the Red Cross and Red Crescent, Ibid. p .9.
[116] Roling B., Criminal Responsibilities for violations of the law of war, 1976, Revue Belge de Droit International, p. 10.
[117] Eve La Haye, Ibid, p.1.

"rebellion" which is involved in limited duration violence and can rapidly be suppressed by police with no need to involve military units[118]. Second is "Insurgents" involved serious violence with extended duration and geographical scope and a larger number of insurgents that the government could not suppress, yet no rights or obligations were given to this type except for reasons of humanity and economic interest[119]. The third type is "belligerency" which requires the existence of a de facto political organization sufficient in character, resources, and population, with the ability to discharge state responsibilities and duties and act in the rules and customs of war. Belligerents were recognized by the parent state which led to the regulation of violence by laws of war[120].

For the applicability of IHL to NIAC, two main legal sources are relevant, Common Article 3 of the GCs 1949 and Article 1 of the AP II. The former has defined NIAC as armed conflict occurring in one of the High Contracting Parties. In other words, it is a conflict between government forces and non-governmental armed groups or between those groups in the territory of one of the parties to the convention[121]. And as the four Geneva conventions are universally ratified, the high contracting parties' requirement has lost its cardinality.[122] In the same manner, the factual scenarios of NIACs are evolving and have become more complex in a contemporary scenery.[123] In this matter, Common article 3 of the GC 1949 states that "each party to this conflict of non-international character shall be bound to the provisions of the article by humanly treating any person that is not part of hostilities or not anymore active without any discrimination, as well wounded and sick shall be collected and cared for. Moreover, it requests the parties to the conflict to bring into force through special agreements all or part of other provisions of the present Convention."[124]

Above all, according to article 1 of AP II, more restrictive requirements have been assigned to NIAC by stating that "a NIAC is in which takes place in the territory of a High Contracting

[118] RA Falk, Janus Tormented: The International law of Internal War, International Aspect of Civil Strife, Princeton University Press, 1964, p 185.
[119] A. Cullen, The Concept of Non-International Armed Conflict in International Humanitarian Law, Cambridge University Press 2010, p. 11-12.
[120] Sandesh Sivakumaran, the Law of non-International Armed Conflict, OUP Oxford, 2012, p.10-11.
[121] Although not spelled out in the text, it has always been assumed that the provision applies to hostilities between government forces and one or more-armed groups as well as those between two or more such groups, see Commentary to Article 1 of APII.
[122] How is the Term Armed conflict defined by International Humanitarian Law? ICRC Opinion paper, March 2008, p.3.
[123] ICRC, International Humanitarian Law and the challenges of contemporary armed conflicts: Report, October 2011
[124] ICRC, Common article 3 of the Geneva Conventions, 12 August 1949, p.24.

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 and to implement this Protocol"[125]. So, territorial control by the dissident armed group is required. But such a requirement applies only to the second protocol as a supplementary rule to common article 3, so it does not extend to cover in general NIACs[126]. Therefore, even if the level of violence may be high in some situations, NIAC does not occur unless there is an organized armed group involved.

It is important to differentiate between NIAC and less serious forms of violence that are not considered armed conflict and are governed by IHRL rather than IHL, such as internal disturbance, tensions, riots, or acts of banditry[127]. Such acts do not reach a certain level of confrontation to be considered an armed conflict, hence not bound by IHL. Nevertheless, they do not fall in a legal vacuum, so Criminal law and human rights law will guarantee that forcible actions by states remain within reasonable bounds. According to the definition of NIACs international case law, this level of confrontation requires two criteria according to the ICTY in the *Tadic case* that required the following:

- Firstly, the hostilities must reach a minimum level of intensity. This may be the case for example, when the hostilities are collective or when the government is obliged to use military force against the insurgents, instead of mere police forces[128]". The ICTY considered the level of intensity requires the following factors: "The gravity of attacks and their recurrence; the temporal and territorial expansion of violence and the collective character of hostilities; whether various parties were able to operate from territory under their control; an increase in the number of government forces; the mobilization of volunteers and the distribution and type of weapons among both parties to the conflict; the displacement of a large number of people owing to the conflict; and whether the conflict is subject to any relevant scrutiny or action by the UN Security Council.[129]"
- Secondly, NSAs involved in the conflict must be considered as "parties to the conflict", meaning that they possess organized armed forces. This means that these

[125] Additional Protocol II, art. 1, para. 1.
[126] How is the Term Armed conflict defined by International Humanitarian Law? , Ibid. p.4.
[127] Additional Protocol II, Article 1-2.
[128] ICTY, The Prosecutor v. Fatmir Limaj, Judgment, IT-03- 66-T, 30 November 2005, para. 135-170.
[129] Arimatsu L. and Choudhury M., The Legal Classification of the armed Conflicts in Syria, Yemen and Libya, Chatham House, March 2014, p 4.

forces have to be under a certain command structure and have the capacity to sustain military operations[130]". And according to the ICTY, such conflict must be protracted armed violence between governmental and organized armed groups (OAG) or between such groups.[131]

Several treaty provisions of the law of NIACs have been regarded as declaratory to the Customary International Law. For example, common article 3 of the GCs 1949 expresses minimum rules applicable to international and NIACs according to the ICJ in the *Nicaragua case 1986*[132]. Therefore, such a treaty is always binding to the contracting states, but also the declaratory standard of such provisions to international customary law, makes it binding to non-contracting states too. In this matter, in the *Delalic et al. Case of 1998*, the Trial Chamber of the ICTY stated the following:

- "While in 1949 the insertion of a provision concerning internal armed conflicts into the Geneva Conventions may have been innovative, there can be no question that the protections and prohibitions enunciated in that provision have come to form part of customary international law." [133]

Moreover, the ICTY in the *Limaj case* when the trial chamber had to determine if the conflict between the Kosovo Liberation Army (KLA) and the governmental forces during the conflict in Kosovo in 1998 can fall under the application of common article 3 of the GCs 1949, the argument if such conflict can be considered an armed conflict was discussed[134]. The trial in reviewing whether such conflict amounted to protracted violence concluded that "it is a periodic armed clash occurring virtually continuously at intervals averaging three to seven days over widespread and expanding the geographic area." [135] Therefore, the *Limaj Case* gives an excellent illustration that the tribunal shall consider all facts before it can conclude if a situation does reach the level of an armed conflict.

Most of the conflicts nowadays are NIACs, which are subject to few treaty rules compared to IACs.[136] While common Article 3 of the GCs 1949 is regularly applied, it is not restrictive.

---

[130] Ibid. p. 94-134.
[131] ICTY, The Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, IT-94-1-A, 2 October 1995, para.70
[132] Case concerning Military and Paramilitary Activities in and against Nicaragua/USA 1986, ICJ Rep.14, 114.
[133] Prosecutor v. Delalic' et al., ICTY, Trial Chamber, 1988, para. 301.
[134] Eva La Haye, Ibid. p.11-12.
[135] ICTY, Limaj Trial, para 168.
[136] The treaties apply to non-international armed conflicts, namely the Convention on Certain Conventional Weapons, as amended, the Statute of the International Criminal Court, the Ottawa Convention banning anti-personnel landmines, the Chemical Weapons Convention, the Hague Convention for the Protection of Cultural

Discussions about when a NIAC comes to an end were also vital, where the 32nd international conference of ICRC has concluded that: "according to the ICRC experience in this matter the NIAC comes to an end when the complete cessation of hostilities between parties occur with absence of real risk or their resumption.".[137] Nevertheless, no clear definition of NIACs was settled by treaty or case laws. However, the level of organization of armed group and the intensity of armed hostilities seems to be the commonly accepted criteria to distinguish such conflicts from other cases of violence or disturbances in international law.

To summarize, the key distinction between NIAC and IAC is the quality of parties involved, and the main obstacle is that in many cases foreign intervention, NSAs, and cyber hackers, cause a multiplication of identity of actors involved which makes the classification of the armed conflict a complex issue, especially when the third parties do not admit their involvement in a conflict. As can be noticed, hybrid warfare elements are quite challenging to the classification of armed conflict as they possibly do not fit into any of the classifications or definitions dealing with the legality of warfare under international law. This is expected since hybrid warfare is tailored to multiple means and methods adopted for the achievement of military and political objectives. Contemporary conflicts are more of mix status nature of low intensity[138], that is due to the fusion of different means of warfare that complicates the understanding of conflicts, use of force, the borderline between peace and wartime, also between NIAC and IAC. In recent years, the use of hybrid tactics has increased in speed, scale, and intensity. So, to unfold the complexity of hybrid warfare, the research makes a comparative overview of the definitions of hybrid warfare, the legal challenges it imposes, and the selected elements that are relevant to this dissertation, mainly cyber-attacks and NSAs.

3. Hybrid Warfare: Definitions and Elements

Hybrid warfare and the emerging role of new actors having the ability to destabilize an order in any state, combined with other non-kinetic means, has attracted the attention of policymakers and security analysts, especially that the 20th century conflicts proved the

Property and its Second Protocol and, as already mentioned, Additional Protocol II and Article 3 common to the four Geneva Conventions. See. Jean Marie Henckaerts and Louise Doswald-Beck, Ibid., p. XXXIV.

[137] ICRC, 32nd International Conference of the Red Cross and Red Crescent, Ibid. p .11.

[138] The shooting down of the U.S. military drone and the alleged US cyber attack response have raised important issues related to the classification of armed conflicts of whether small-scale attack could be considered an IAC, is still controversial. See, Hrnjas, M., The United States of America and the Islamic Republic of Iran: An International Armed Conflict of Low Intensity, The Geneva Academy a Joint Center of The Graduate Insitute Geneva and University of Geneva, December 2019, p.5.

developing multi-modal features starting from the 9/11 attacks, the conflict in Ukraine, and the emergence of ISIS.[139]

Hybrid warfare (hereinafter HW) unlike compound warfare which involves a degree of strategic coordination between regular and irregular forces, suggests cooperation and coordination at all levels: strategic, operational, and tactical. It is also typified by cooperation between a politically motivated force and other groups engaged in criminal activity, hence the hybrid description of the conflict[140]. Compound warfare is a theory developed by Thomas Huber in 1996, by which he defines it as "the simultaneous use of regular or main force and irregular or guerrilla forces against an enemy, by which the operator increases his military leverage by applying both conventional and unconventional force at the same time."[141] HW is not only limited to military means of warfare, but extends to other means of non-military nature, and it is not necessarily a new form of war, however its notion has the potential to change future conceptualization of conflicts that do not fit in the categorization under the Jus ad Bellum and Jus in Bello. Therefore, it is commonly heard that the term HW is used to describe the complexities of the modern battlefield by which it is an overlapping of conventional and asymmetric tactics in an armed conflict.

HW has been defined and analyzed based on certain conflicts or operations that occurred recently and involved a hybrid concept. For instance, Frank Hoffman defined HW based on armed conflict between Hezbollah and Israel in Lebanon in 2006, same did McCuen that based his definition on the conflicts in Iraq and Afghanistan. In the same manner, the discussions within military planning strategic circles particularly in NATO focused on hybrid warfare in Ukraine after the annexation of Crimea by Russia.[142] The European Union has also focused on the hybrid warfare concept and its emergence in the aftermath of the conflict in Ukraine after

[139] Bachmann, S. and Mosquera A., Hybrid Warfare as Lawfare: Towards a Comprehensive Legal Approach, In: Cusumano E., Corbe M. (ed.) A Civil-Military Response to Hybrid Threats, Palgrave Macmillan, Cham 2018, p. 66

[140] F. Hoffman, The Rise of Hybrid Wars and F. Hoffman, Hybrid Warfare and Challenges (2009) 52 Joint Force Quarterly 34-48. See Also N. Freier, The Defense Identity Crisis: It's Hybrid World (2009) 39 (3) Parameters 81-94.

[141] Huber, Th., Compound Warfare: That Fatal Knot, U.S. Army Command and General Staff College Press, Fort Leavenworth, Kansas 2002, p.1-2

[142] Hybrid Warfare: NATO's New Strategic Challenge, Defence and Security Committee, NATO Parliamentary Assembly, 10 October 2015. See also, Countering Russia's Hybrid Threats: An Update, Committee on the Civil Dimension of Security, NATO Parliamentary Assembly, 1 October 2018.

the annexation of Crimea in 2014[143], and the rise of the Islamic State in Iraq and Syria[144]. In this sense, Damien Van Puyvelde notes "In practice, any threat can be hybrid if it is not limited to a single form and dimension of warfare. When any threat or use of force is defined as a hybrid, the term loses its value and confuses instead of clarifying the reality of modern warfare"[145]. Therefore, defining HW is relevant and important to determine how states distinguish it from other threats and how to respond to it. And from an international law perspective, it is important to identify the means and methods used in such warfare. Most international lawyers agree on the importance of such effort, especially with the increase of the use of the HW term in modern battlefields, and with the ongoing debate about the novelty of such forms of warfare and the challenges, they impose on the international legal order.

3.1. Overview of Hybrid Warfare

Hybrid warfare has passed through an evolution in strategic thinking and doctrine, yet scholars' interest from a legal perspective has been modest. Nevertheless, HW plays a role at all levels of warfare but is not equally effective at all levels. Such form has a significant effect in today's conflicts that also became hybrid due to globalization and interconnectivity. The latter had its direct impact on the traditional rules of *Jus Publicum Europaeum*[146], which originated from the Peace of Westphalia in 1648. Those rules established a clear distinction between war and peace, and between legitimate combatants and non-combatants.

To illustrate, HW possesses characteristics of both the special and conventional realms and requires an extreme amount of flexibility to transition operationally and tactically between special and conventional arenas.[147] Nevertheless, it was Frank Hoffman in the aftermath of the Israeli- Hezbollah conflict in 2006, better known as the thirty-three days war, who considered

---

[143] Resolutions 2133 (2016) on "Legal remedies to human rights violations on the Ukrainian territories outside the control of the Ukrainian authorities" and 2132 (2016) on "Political consequences of the conflict in Ukraine" and its Resolution 2198 (2018) and Recommendation 2119 (2018) on "Humanitarian consequences of the war in Ukraine" concerning the military operations in Ukraine.

[144] Resolution 2190 (2016) on "Prosecuting and punishing the crimes against humanity or even possible genocide committed by Daesh".

[145] Chris Tuck, Hybrid War: The Perfect Enemy, Defense in Depth, Research from the Defense Studies Department, King's College London, April 25,2017 Https://Defenceindepth.Co/2017/04/25/Hybrid-War-The-Perfect-Enemy/

[146] The concept of Ius Publicum Europaeum describes the public law of the European legal area that is composed of European Union law and the laws of its Member States as well as other legal sources, such as the law of the Council of Europe.

[147] Mumford, A., McDonald, J., Ambiguous Warfare, Report produced for the DCDC, October 2014. See also, Smith, R., The Utility of Force, The Art of War in the Modern World, Vintage Books, 2007. (In 2005, British General Rupert Smith stated: "War no longer exists… confrontation, conflict, and combat undoubtedly exist all around the world… and states still have armed forces which they use as a symbol of power. Nonetheless, war as cognitively known to most non-combatants, war as a battle in a field between men and machinery, war as a massive deciding event in a dispute in international affairs: such war no longer exists."

that this conflict validated the ability of NSAs to deconstruct the vulnerabilities of western-style military states, and addressed the concept by the following: "Hybrid threats incorporate a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder. Hybrid Wars can be conducted by both states and a variety of NSAs (with or without state sponsorship). These multi-modal activities can be conducted by separate units, or even by the same unit, but are generally operationally and tactically directed and coordinated within the main battlespace to achieve synergistic effects in the physical and psychological dimensions of the conflict."[148] For instance, Hezbollah evolved from a paramilitary resistant movement in the early 1980s to a highly structured and sizeable powerful organization with a large military and political wing recognizing blended irregular tactics and modern weaponry[149]. Hoffman's analysis of the conflict between Hezbollah and the IDF (Israel Defense Forces) considered that Hezbollah had an advantage over Israeli conventional troops by using a mixed form of guerrilla tactics and technology in often densely packed city centers, in addition to the fusion of non-military, political, social, diplomatic, and informational components. However, in the strategic and military practice, such a tactic is not considered new as we have witnessed in history numerous cases by which such tactics have been employed on a battlefield. As well, it does not create a legal challenge to international law as the parties to the conflict and the battlefield are clear and identified. Important to note, that in this conflict the two Security Council resolutions that were adopted, resolution 1697/2006 deploring attacks against the UNIFIL (UN Interim Force in Lebanon) and resolution 1701/2006 that called for a ceasefire and determined its structure, made no reference to the nature of the conflict or to the law which should regulate it[150]. Although, the existence of an IAC is easily recognized due to the parties of the conflict, determining the existence and classification of conflict with a non-state armed group can be difficult[151]. But what is important in Hoffman's analysis of this conflict is addressing the changing nature of military warfare through the involvement of non-state armed groups and its technological capabilities. Hoffman's concept seeks to provide a theoretical framework that

[148] Hoffman F., 'Conflict in The 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies' 2007, p. 8,(Electronic Version) www.Potomacinstitute.Org/Publications/Potomac_Hybridwar_0108.Pdf. , (Last Accessed 29 February 2016). See also, Hoffman F., 'Hybrid Threats: Reconceptualizing The Evolving Character of Modern Conflict', 240 Strategic Forum, 2009, p 1; F.G. Hoffman, 'Hybrid Warfare and Challenges', 52 Joint Forces Quarterly (2009), pp 1–2.
[149] Ridderhof R., Ibid.
[150] Iain Scobbie, Lebanon 2006, International Law and the Classification of Conflicts, Edited by Elizabeth Wilmshurst, Chatham House, Oxford University Press, 2012, p. 398.
[151] Iain Scobbie, Ibid. p. 400-401

enables us to understand contemporary conflicts, his aim is not merely academic but is rather geared towards the formulation of political doctrine.

Modern HW flourished with the growing influence of NSAs, in an attempt of states to avoid direct confrontation or state involvement. However, what might start as low-intensity clashes can shift to conventional conflict. Hybridity expresses the difficulty that instead of separate challenges with fundamentally different approaches, we can expect to face competitors who will employ all forms of war and tactics, perhaps simultaneously. That has been reflected commonly by the writings of Hoffman[152], R. Glenn, and others[153]. In other words, HW is a highly integrated use of diverse use of military and non-military measures to overarching strategic objectives, and its concept was meant to express the idea that symmetrical and asymmetrical forms of warfare are likely to converge rather than just coexist in parallel.

The HW received a substantial amount of criticism, largely because the definition had been comprehended from analyzing and describing the adversaries. In this matter, Mary Ellen O'Connell criticized the novelty of HW and considered that international law can even govern the newest technology of war[154]. O'Connell added that HW became more important after the annexation of Crimea in 2014 and though some of its elements are new, it does not mean that such tactics are novel and it is erroneous to think that international law is out of date or full of gaps concerning new developments.[155] In the same sense, Murray and Mansoor argued that the blending of conventional and unconventional means in a battlefield has been since ancient

[152] Hoffman, F.G., Hybrid vs. compound war. The Janus choice: Defining today's multifaceted conflict. *Armed Forces Journal*, October 2009. Hoffman defines HW as: "any adversary that simultaneously and adaptively employs a fused mix of conventional weapons, irregular tactics, terrorism, and criminal activities in the battlespace to obtain their political objectives."

[153] Anderson K., Explaining Hybrid Warfare in the Annual National Security Conference on February 26-27, 2016 at Duke Law School. Professor Kenneth Anderson noted that: "HW is a term that started to capture the blurring and blending of previously separate categories of conflicts, it is not just categories of conflicts in the military means of waging war, but also adds to it categories civilian in nature such as propaganda, disinformation, cybersecurity, things that we do not traditionally consider as means of war". See also Glenn, R. W. (2009). Thoughts on "Hybrid" Conflict, in: Small Wars Journal, March 2009. R. Glenn considered that "Hybrid threat is any adversary that simultaneously and adaptively employs a tailored mix of conventional, irregular, terrorism and criminal means or activities in the operational battlespace. Rather than a single entity, a hybrid threat or challenge may be comprised of a combination of state and NSAs.

[154] Mary Ellen O'Connell, Myths of Hybrid Warfare, The Centre of Ethical Education in the Armed Forces, 2015 http://www.ethikundmilitaer.de/en/full-issues/20152-hybrid-warfare/oconnell-myths-of-hybrid-warfare/

[155] Mary Ellen O'Connel, Ibid.

times, providing examples such as the American revolution that had two dimensions of conventional means in the North battle lines and the irregular partisan forces in the south.[156]

Part of the criticism can be agreed on with regards to the novelty of such fusion of means and methods to warfare. For example, The Japanese invasion of Manchuria in 1931 offered some striking parallels with the annexation of Crimea, as Japan by that time denied the existence of war and combined large-scale military operations with non-military means, including instigating civil unrest, organizing armed gangs, and supporting armed separatists.[157] Nonetheless, it is concluded that HW offers certain novelties, particularly in the scale of the use of force and exploitation of such means in modern networked societies, the multimodal character aiming for the strategic and tactical realization of synergy effects in the physical as well as the psychological dimensions of conflict, and the exploitation of modern technology.

3.1.1. Hybrid Warfare in Doctrine

The HW concept had been the core of interest to the political and military circles over the past ten years. This western term of modern conflicts has similar terminologies in the Russian doctrine (Non-Linear or New Generation Warfare) and Chinese doctrine (Unrestricted Warfare). From the Russian perspective, through what is known as the "Gerasimov Doctrine", the modern methods of waging warfare are by the broad use of political, economic, informational, humanitarian, and other non-military means, supplemented by civil disorder among the local population and concealed armed forces.[158] Gerasimov's doctrine was that the conflict of the future will be characterized first and foremost by the lack of clear boundaries or even the blurring of differences between war and peace, ununiformed personnel, and covert operations and that wars will not be declared but will just break out. In this way, the use of direct force may not always or initially be a central element of the conflict, or even not employed at all. The new understanding of warfare, according to Gerasimov Doctrine, is based on in-depth analyses and conclusions from recent conflicts and campaigns. For instance, the alleged use of HW by the Russian Federation in the annexation of the Crimean Peninsula highlights the employment of such tactics through the use of special operations forces, such as the Spetsnaz units (little green men) that seized the governmental building and critical

---

[156] See Peter R. Mansoor, Introduction, Hybrid Warfare in History, Hybrid Warfare, Fighting Complex Opponents from the Ancient World to the Present, W. Murray and P. Mansoor eds., 2012.
[157] Report of the Commission of Inquiry, League of Nations Doc. C.663.M.320, Oct. 1, 1932, para. 66–83.
[158] General Gerasimov's article is available in English from Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," In Moscow's Shadows (blog), 6 July 2014, (accessed 11 December 2015). https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov- doctrine-and-Russian-non-linear-war

infrastructure, supported by a large scale of a disinformation campaign from the Russian government spreading doubt and deniability of the Russian interference in the ongoing conflict.

On the other hand, the unrestricted warfare as an alternative description of HW was underlined in the writings of the Chinese military scholars, where they considered that "If a country is at a military disadvantage, catastrophic and disruptive threats must be employed to target the vulnerabilities of the opponent, by blending economic, financial, telecommunication and network, resource, information and media, and International Law warfare."[159] The western doctrine has also recognized the complexity of HW by which it reflects the contemporary form of guerrilla warfare by employing both modern technology and modern mobilization methods. HW can also be noticed in US military and academic writings who agreed that hybrid threats incorporate a full range of different modes of warfare concluding conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder, conducted by both states and a variety of NSAs.[160]

Besides, recent conflicts Syria, Iraq, and Afghanistan had hybrid elements that caused infringements of international law due to the methods and means used such as cyber, proxy actors, NSAs, state actors, terrorism, unorthodox means of fighting, annexations, and extraterritorial effects undermining blatantly the foundation of States' territorial integrity.

3.1.2. NATO's Narrative of Hybrid Warfare

NATO had much to say about HW, especially in the aftermath of cyber-attacks that targeted Estonia, the rise of the Islamic State and its transnational threat in Syria and Iraq, the annexation of Crimea, and the legal complexities of hybrid threats and soft power in the Arctic region.[161] Therefore, NATO found itself in direct and indirect confrontation with the complexity of HW.

---

[159] Barno, D. and Banshael, N., The Irrelevance of Traditional Warfare? *War on the Rocks*, accessed 2 May 2016.

[160] See for example: Hybrid Warfare according to U.S. Joint Forces Command, Joint Center for Operational Analysis briefing on "Joint Adaptation to Hybrid War" is "Conflict executed by either state and/or non-state threats that employs multiple modes of warfare to include conventional capabilities, irregular tactics, and criminal disorder". While a working definition derived by U.S. Joint Forces Command, Joint Irregular Warfare Center, 2008-2009 defines Hybrid Threat as: "An adversary that simultaneously and adaptively employs some fused combination of (1) political, military, economic, social and information means and (2) conventional, irregular, terrorism and disruptive/criminal conflict methods. It may include a combination of state and non-state actors.". According to U.S. Army Training and Doctrine Command's Operational Environment, 2009-2025 Hybrid Threat is: "A threat that simultaneously employs regular and irregular forces, including terrorist and criminal elements to achieve their objectives using an ever-changing variety of conventional and unconventional tactics to create multiple dilemmas.". See also Department of Defense, Quadrennial Defense Review Report, Washington, DC: Department of Defense, 2010, p. 8, (accessed 4 December 2015).

[161] See more about theats in Arctic, Al-Aridi A., Legal Complexities of Hybrid Threats in the Arctic Region, teise 2019, vol. 112, pp. 107-123.

NATO has considered that the Russian aggressive foreign policy is a breach of the long-standing principles of international law by the illegal annexation of Crimea in 2014. NATO defines HW as "a wide range of overt and covert military, paramilitary and civilian measures employed in a highly integrated design."[162] While a hybrid threat, according to the NATO Military Working Group 2010, is posed by any current or potential adversary including state, non-state, and terrorists, with the ability to simultaneously employ conventional and non-conventional means adaptively in pursuit of their objectives. NATO considers that the concept of HW is not new, but what is new is that it has moved from the operational level, underpinned by new dimensions, such as globalization, complex geostrategic environment, advanced technologies, and information demand.

NATO addressed HW in numerous events, however, one of the definitions of the concept that caught our attention is the following "HW is an amalgam of overt and covert military power; a combination of bullying and subversion along with just a dash of deniability – all intended to make a full-scale response much harder"[163]. This definition reflects the actions occurring especially in the Baltic region, where NATO states and Russia are two power blocks with adjacent and opposite borders. Several incidents in the region have occurred based on subversion below the threshold of an armed attack, yet it could escalate anytime to confrontation. And with regards to the cyber dimension that plays a highly specific role in today's hybrid threats, NATO recognized in July 2016 that cyberspace is a domain of operations in which it must defend itself as effectively as it does in the air, on land, and at the sea. Article 5 is central provision of the NAT and depends on the occurrence of an armed attack to be enforced, it is highly relevant to counter traditional inter-state attack, and with the increase of hybrid threats the NATO stretched Article 5 further in the NATO summit declarations of

[162] An International Research conference for Warrior-Scholars, NATO and the New Ways of Warfare Defeating Hybrid Threats, NATO Defense College, Rome 2015. See also, Anders Fogh Rasmussen, NATO Secretary General, America, Europe and the Pacific, Speech at the Marines' Memorial Club Hotel, San Francisco (July 9, 2014), http://www.nato.int/cps/en/natohq/opinions_111659.htm. In 2018 the NATO Deputy Secretary General Rose Gottemoeller at the Microsoft conference on Countering Hybrid Threats stated that: "For NATO, this is an important new area that is been taken seriously. Cybersecurity is a global issue for our time, we cannot fight the threats with the tools of the past. We must tackle the technological threats. We do not know where the borderline is between war and peace, between crisis and conflict. For almost 70 years NATO has been in the business of security of 30 independent democracies, protection of citizens, and defend the principles of democracy and rule of law. Previously kinetic aggressive actions were usual, but nowadays means of hybrid threats such as cyber-attacks are unpredictable. Three things need to be done: Reaffirming the rule of law, supporting national resilience, and fostering deeper cooperation. NATO acknowledged in 2014 that international law including IHL and UN Charter applies to cyberspace. NATO branded Russia's intervention in Ukraine as an example of hybrid warfare, defining the latter as "a combination of traditional military means and more sophisticated covert operations

[163] Marcus, J., Putin problem gives NATO headache. BBC , 28 April 2016. Available at: http://www.bbc.com/news/world-30273813.

2016 and 2018, and now foresee a possibility that a hybrid attack, in particular cyber attacks, may amount to the use of force, and trigger the activation of article 5.[164] And while hybrid warfare varies in intensity and scale, applying article 5 is relevant to hybrid attacks that reach the level of armed attack articulated in article 51 of the UN Charter, while the situations of less intensity are still covered by non-military measures under article 4 of the NAT.

3.1.3. Hybrid Warfare at EU Level

With the emergence of hybrid threats and its ambiguity since Russia's annexation of Crimea in Ukraine, many international organizations including the EU started defining the phenomenon. The EU's 2016 Joint Communication on the concept of hybrid threat-defined it as a mixture of coercive and subversive activity using conventional and unconventional methods, coordinated by state or NSAs to achieve specific objectives while remaining below the threshold of formally declared warfare.[165] However, formally declared warfare has long become obsolete and irrelevant under current international law, particularly IHL. So this definition has dismissed the fact that Hybrid warfare can still evolve during an armed conflict. Nonetheless, the EU assures the importance of keeping the definition of hybrid threats flexible to respond to their evolving nature. That has been seen through the series of decisions that followed the evolving nature of Hybrid threats in the region. For instance, in response to the Salisbury poisoning of former Russian intelligence agent Sergei Skripal, the European Council on 22 March 2018 agreed that the EU must strengthen its resilience to chemical, biological, radiological, and nuclear threats.[166] Additionally, the European Council agreed on an EU action plan in 2018 to counter disinformation and protect societies from malicious cyber activities and hybrid threats. The legal framework at the European and international level that is composed of many legal instruments and supported by declarations and resolutions, plays an important role in establishing a tighter legal net to counter the new challenges that arise due to the rapid technological development and hybrid means.

On the other hand, the Assembly of the Council of Europe (CoE), not to be confused with the European Council, has acknowledged concerns of nowadays confrontations with the

[164] NATO, Brussels Summit Declaration, para. 21.
[165] European Commission (2016b), Joint Framework on countering hybrid threats: A European Union response, Communication, JOIN (2016) , 6th of April.
[166] European Council meeting (22 March 2018), Conclusions.
https://www.consilium.europa.eu/en/meetings/european-council/2018/03/22

phenomenon of "Hybrid War" that poses a new type of threat based on the fusion of military and non-military means such as cyber-attacks, mass disinformation campaigns, disruption of communications, and many others.[167] The draft resolution of CoE agrees that the main features of this phenomenon are legal asymmetry, by adversaries denying their responsibility for hybrid operations and trying to escape the consequences of their actions. Similarly, according to the European Parliament Research Service (EPRS), A "hybrid threat" is "a phenomenon resulting from convergence and interconnection of different elements, which together form a more complex and multidimensional threat.[168]" Taking into account different levels of intensity of a threat and intentionality of actors involved, the EPRS also defines a "hybrid conflict" and a "hybrid war". Hybrid conflict is "a situation in which parties refrain from the overt use of armed forces against each other, relying instead on a combination of military intimidation (falling short of an attack), exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives." Finally, "hybrid war" is "a situation in which a country resorts to overt use of armed forces against another country or a non-state actor, in addition to a mix of other means (e.g., economic, political, and diplomatic).[169]" Interestingly, according to Aurel Sari, excluding the use of armed force from the definition of hybrid threats, reduces hybridity to a loose synonym of complexity.[170] The concept of "hybrid threats" should be reserved for situations where States or NSAs employ non-violent means of warfare as instruments of warfare by integrating them with the use of armed force or the threat of force. Scholars have not shown much interest in the legal aspects of "hybrid warfare", as most of the legal problems related to this concept – such as violation of territorial integrity, support for separatist movements, or the failure to honor international agreements - are not new. The breadth and fluidity of this concept make it difficult to be legally assessed.

Furthermore, the committee of legal advisors on public international law (CAHDI) opined the same concerns regarding the legal challenges related to HW and hybrid influencing[171]. The committee agreed that relevant national and international legal regimes apply to military and

[167] Council of Europe, Draft Resolution on the Legal Challenges related to the Hybrid War and Human Rights Obligations, Committee on Legal Affairs and Human Rights, As/jur (2018) 07, para 2, p.1. (Draft resolution and recommendation adopted unanimously by the committee on 14 March 2018.)
[168] At a Glance. Understanding Hybrid Threats, European Parliament Research Service (EPRS), June 2015.
[169] Council of Europe, Draft resolution As/Jur (2018) 07, Ibid. para 12, p.6
[170] Sari A., Ibid., pp. 16 and 18.
[171] Opinion of CAHDI on Recommendation 2130 (2018) of the Parliamentary Assembly of the Council of Europe "Legal Challenges Related to Hybrid War and Human Rights Obligations"

non-military means of hybrid war and that each action should be assessed individually according to a relevant legal regime. This could be problematic for states to respond to such acts, as HW means are invested to slow down any response. The committee pointed out some international binding existing legal instruments that address the legal challenges of HW, such as the Convention on Cybercrime, The Council of Europe Convention on Prevention of Terrorism (CETS no. 196), and its protocol.[172] In the same sense, The Food for Thoughts Paper (Countering Hybrid Threats) highlights several important aspects of HW[173]. First, it agrees with previous definitions and characterizations of the term as centrally designed and controlled use of various covert and overt tactics, as well the blending of military and non-military means by applying coercive and subversive methods, supported by insurgents or disguising state to state aggression behind the mantle of humanitarian intervention such as protecting minorities. But adds that the important aspect of those tactics is generating ambiguity both in the affected population under attack and in the larger international community. And that the lack of attribution can paralyze the ability of an opponent to react effectively as it becomes unclear who is behind the attack, limiting the speed and scope of a response to the aggression.

Based on the previous analysis, it is understood that there is little agreement on what the HW concept entails and what are its means. Yet it is commonly agreed on that HW represents the fusion of different means of warfare by employing all dimensions of state and NSAs, blurring the distinction between military and civilians, and fruitfully investing the modern technology and non-military means in the campaign. Also, HW is not limited to the physical battlefield, taking into consideration modes that are considered more conceptual such as economic, social, political, and disinformation. In the context of modern armed conflicts, Hybridization is the coexistence of old and new elements of warfare, derives from clashes between regular national forces and asymmetrical conflicts, between military super technologies and primitive weapons, as well as struggles for territory and resources (in maritime environments and land), disputes over identities and values, in addition to conflicts that arise on ethnic, national, and religious grounds rather than between states[174]. At the operational level, China, for example, has

[172] Ibid., para 4.
[173] European External Action Service, Food-for-Thought Paper "Countering Hybrid Threats", 8887/15, May 13, 2015.
[174] Lewicki, W. Hybrid Warfare in Ukraine- A New Way of Waging War, Articles published at the International Conference: “Hybrid Warfare in Ukraine: Outcomes and Recommendations for Europe and the World”, Piotrkow Trybunalski, Poland 2016, p. 7.

successfully invested its technological capabilities to progressively gain more territories using the so-called "Salami Slicing" strategy, by building artificial islands to gain more influence and maritime zones without military means that might lead to a conventional confrontation[175].

Defining HW in terms of the legal complexities that adversaries tend to craft, will require a different interpretation than the ones examined by military scholars and strategists so far. The modern international law stresses that the use of force is considered illegitimate unless initiated within the very narrow confines of the law; mainly self-defense or acting under the authorization of the UN SC[176]. Thus, states formulated military and political strategies to circumvent the law on the use of force and its exceptions mainly with templates for the legality of conduct such as anticipatory self-defense, protection of citizens of States that are unwilling to exercise its responsibility to protect them by so-called humanitarian interventions and responsibility to protect doctrine.

Within this perspective, HW theory transforms into an inevitable by-product of the legal framework governing international relations and creates legal gray areas of international law that such activities are employed to generate and preserve a legal environment based on a lack of attribution and liability. Consequently, the key aspect of gray zone challenges is that it should be sufficiently ambiguous to leave targeted states unsure of how to respond. That can exploit the legal thresholds and obligations by distorting the law to gain an advantage over the targeted party of a conflict. This could be seen through concealing a non-standard, complex, and indirect involvement in a conflict, using force through proxies, and conducting operations at a level of intensity that circumvents the relevant legal threshold. Such fusion of multimodal dimensions, by which in many cases the opponent is fluid, are employed concurrently and lead to a catastrophic result for the targeted state by undermining its essential features and confusing its ability to adopt permissible responses under the international laws, hence allowing the dissolving of borders between what is permissible and impermissible in an armed conflict, whether it is IAC or NIAC or both at the same time. That establishes an asymmetric legal environment where states that continue to abide by the law are placed at a competitive disadvantage against adversaries that exploit legal ambiguities and violate the rules of international law.

[175] Miracola, S. Ibid.
[176] Dörr, O. Use of Force, Prohibition of. In Max Planck Encyclopedia of Public International Law 2015.

In addition, debates about the novelty of HW also took place at the military level, by which some argue that HW is new and unregulated by international law. Such statements can be seen through the writings of military strategists, that aim to use the complexity of HW to expand the necessity of using force in response to the new threats. For example, the US Army's Field Manual Operations considers that "HW is unregulated and imposes a great threat. The future operational environment will be characterized by hybrid threats through combinations of regular, irregular, terrorist, and criminal groups that decentralize and syndicate against us and possess capabilities previously monopolized by nation-states. These hybrid threats create a more competitive security environment, and it is for these threats we must prepare"[177]. On the other hand, others argue that HW is old and fully regulated by international law, considering that wars have not and will not change.[178] Such arguments can be found in the writings of military historians such as Mansoor and Murray characterizing HW as a "conflict involving a combination of conventional military forces and irregulars which could include both state and non-state actors, aimed at achieving a common political purpose"[179].

Despite the conflicting views about the novelty of HW, in practice at modern non-state armed groups have heavily invested in their hybrid capabilities. For example, ISIS started as a branch of al Qaeda in Iraq by the late Abu Musab al Zarqawi in 2004 and flourished to be what's so-called Caliphate, is just a new Hybrid phenomenon, it is a non-state armed group with a clearly expressed agenda based on religious, ideological, and historical acts aiming to gain political victories[180]. Moreover, it reflects a multinational business, a terroristic group with transnational criminal actions, part of it is a network, part organization, and part movement. But for sure it does not qualify to the statehood level asit does not fulfill the Montevideo criteria[181], nor the doctrine of international recognition. Simply conquering and subjugating people does not necessarily mean an acceptable definition of statehood as it used to be in previous centuries. On the other hand, States have also re-structured their military and para-military forces to fit a hybrid nature. China has relied on the so-called Maritime Militia (Haishang Mingbing or the

[177] "Hybrid Warfare," in: JSOU Report 13–4 (2013), p. 4, quoting Headquarters, Department of the Army, Army Field Manual 3-0: Operations (Washington, DC: Department of the Army, 2011), p. 14.
[178] Peter R. Mansoor, Introduction, Hybrid Warfare in History, Hybrid warfare, fighting complex opponents from the ancient world to the present, (W. Murray and P. Mansoor eds., 2012)
[179] Cf. Salonius-Pasternak, Charly (2015): "Preparing Finland for hybrid warfare," in: FIIA Comment 6/2015.
[180] Al Aridi, A. An Interdisciplinary Approach to Combat ISIS: Legal, Political and Socio-economic, 4th International Conference of PhD Students and Young Researchers, Conference paper, International Network of Doctoral Studies in Law, Vilnius 2016, p. 26
[181] Montevideo Convention on the Rights and Duties of States, signed at the International Conference of American States in Montevideo Uruguay, 26 December 1933, came into force 26 December 1934, Art. 1, 3.

little blue men), those militias are mainly Chinese fishermen or civilians in nature but operate as military personnel in the South China sea depending on the scenario they are confronted with, and attacking other ships transiting or operating in this area[182]. These maritime militias are an extension of the concept of people's war under modern circumstances. Therefore, the blurring line between civilians and combatants, or between fishing boats and naval forces in the case of maritime militias, has a direct impact on the principle of distinction in IHL, the law of the sea, and State responsibility for unlawful acts.

To sum up, international law draws a line of distinction between legal and illegal activities, also between what is legally justified in a battlespace and what is not, in turn to build a predictable interstate relation. Yet, hybrid adversaries tend to use covert activities, supported by the fusion of other military and non-military means to create a legal asymmetry. This means that political objectives can be achieved in more rapid for the targeting party and catastrophic sense to the other party of the conflict or targeted entity by adhering to different levels of intensity and operating in a way that fosters deniability of actions for the perpetrator, to create a legal confusion to the targeted state's response. Then, it is essential to situate hybrid measures within existing law they seek to circumvent.

To conclude, HW crystalizes many legal areas of uncertainty in international law, these areas are known as gray zones. An issue that raises questions about the conditions that trigger the inherent right of State self-defense and for invoking collective self-defense, in addition to the principles of proportionality, necessity, and immediacy of the armed response in self-defense. Particularly, hybrid adversaries tend to avoid a direct confrontation "state-to-state" that leads to an IAC, as this would not serve the political and strategic interest behind such campaigns. Nonetheless, HW is not a new strategic concept, but it provides a relevant and potentially useful analytical framework for assessing the relation between International legal regimes governing the use of force and law of armed conflict to contemporary warfare scenarios, this will highlight the legal challenges modeled by specific threats and adversaries that combine symmetrical and asymmetrical methods. As matter of fact, the era of HW has not resulted in significant changes to the law of armed conflict, and the application of law continues to depend on how a conflict is characterized, either IAC or NIAC. However, today's classification is more likely to have characteristics of both types to a single battlefield that includes non-kinetic dimensions, such

[182] Miracola, S. Commentary: Chinese Hybrid Warfare, Italian Institute for International Political Studies, Rome December 2018, https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853

as cyber operations accessed by both civilians and militants. Henceforth, the avoidance of crossing the threshold of armed conflict in both IAC and NIAC will be critical focal points for any hybrid warfare or threat. Therefore, the legal resilience that is decisively challenged by HW operations and fall below or in the gray zone of the threshold of armed conflict, necessitate a clear understanding of how international law applies to modern warfare, rather than entering a dark tunnel of unregulated conflicts that will have horrific results.

3.2. Challenging Elements and Means of Hybrid Warfare

The HW can vary collectively in numerous domains. Initially, the political domain, such as upholding ethnic self-determination over state sovereignty or asserting the supremacy of national laws over international laws; strategically by creating new ethnic realities or claiming the transfer of territories (annexation of Crimea as an example). Also, on a social and cultural level by the exploitation of historical facts and seizure of ethnic minorities. Additionally, the economic and energy domain, such as the destruction of energy infrastructure to justify humanitarian convoys or asserting state sovereignty over energy resources[183], opposing climate change agreements to preserve more access to Arctic resources and untapped fishes in the region. Furthermore, the cyber and military domains combined with intelligence are critical and play an important role in the success of such campaigns. Moreover, as the concept extends to elements of criminality, disinformation, and cyber interference, the distinction between combatants and non-combatants becomes vaguer. For instance, cyber hackers could be seen as immune civilians operating outside of the battlefield making it harder to determine appropriate use of force.[184]

Previously, it was remarked that HW can be characterized easier than being defined. While the legal response against such a form of warfare requires special consideration in the legal domain, it can be seen that the main elements of hybridity which corresponds to an abuse of the defined legal space, can be observed. In practice, hybrid measures are designed to avoid explicit violation of the UN Charter and that can be achieved through an emphasis on covert action as an effective way to exploit the weakness of an international enforcement regime where the status quo is often inaction, particularly in those cases where aggressor states have sown doubt as to attribution or the legality of their behavior[185]. Therefore, a focus is desired on the main

[183] Voyger, M., Ibid.
[184] Watt, K. Ethics and Hybrid War, The Security Distillery, April 2019,
[185] Cantwell, D., Hybrid Warfare: Aggression and Coercion in the Gray Zone, The American Society of International Law, Vol. 21, Issue 14, November 29, 2017

challenges imposed by hybrid campaigns and the features that make such form of warfare successful for the adversary through ambitious features to disorient observers and make it difficult to legally classify the situation, determine the applicable law and assess attribution of responsibility to respond through appropriate legal mechanisms[186]. For instance, lack of attribution that roots from the ambiguity or deniability of actions, also the multi-modality dimensions and simultaneity by either vertical or horizontal escalation by which such fusion of means is employed in highly coordinated and synchronized fashion to create synergistic effects beyond the immediate element of power[187]. Hybrid actors may increase the potency of an operation by intensifying one or more tools (vertical) or by synchronizing multiple tools (horizontal) for a greater combined effect[188]. Also, employing the broadness and fluidity of certain legal rules to justify certain actions that fall in legal gaps manipulated by hybrid adversaries.

The contextual nature and fluidity of HW present concrete challenges. First, the increasingly blurred distinction that the international humanitarian law drew between public and private, state officials and NSAs, combatants and civilians, military and non-military engagement[189]. Secondly, the gray zone by which the hybrid actors operate is an area based on the ambiguity between war and peace challenging the ability of the targeted state to do timely warning and detection given the fact that actions take place in domains traditionally considered outside the realm of war[190]. Thirdly, the recognition of compliance with the new methods of warfare by which certain elements of HW, such as cyber-attacks, espionage, disinformation, lack common interpretation hence puts them under different legal regimes when it comes to judging compliance with international law[191]. And last, the difficulty to detect, attribute and identify the hybrid actors and the response against such threats, which makes it a low-cost and low-risk strategy for aggressors that will be the main feature of future conflicts[192]. Therefore, such features can be fruitfully invested in three central means: Cyber-attacks accompanied by the technological progress that rendered hybrid campaigns more asymmetrical, extensive use or

[186] Uzun, M., Ibid., p. 40-41
[187] Reichborn-Kjennerud, E., Cullen, P., What is Hybrid Warfare? Norwegian Institute of International Affairs, Policy Brief 2016, p. 3
[188] Treverton G., Thvedt A., Chen A., Lee K., and McCue M., Addressing Hybrid Threats, Swedish Defense University and the authors 2018, Ch. IV, p.45.
[189] Korhonen, O., Deconstructing the Conflict in Ukraine: The Relevance of International Law to Hybrid States and Wars, German Law Journal, 2015, Vol. 16, p. 460.
[190] Cullen, P., Hybrid Threats as a New "Wicked Problem" for Early Warning, Strategic Analysis, European Centre of Excellence for Countering Hybrid Threats May 2018, p. 13.
[191] Korhonen, O., Ibid. p. 460.
[192] Deterrence by Punishment as a way of Countering Hybrid-threats: "Why we need to go beyond Resilience in the Gray Zone", MCDC Countering Hybrid Warfare Project, Information note, March 2019, p.2.

threat of use of non-orthodox means, and non-state armed groups (proxies) mainly due to the non-state centric nature of contemporary conflicts where it is challenging and time-consuming to ascribe responsibility for the actions taken; and "Lawfare" by which law itself became an instrument of hostile competition between states, by which one of the legal themes of hybrid warfare is instrumentalizing the law to legitimize the actions of aggressor state or actor and to also delegitimize the actions of the adversary.

Based on what was discussed above, it is noticed that the traditional understanding of Clausewitz that war imbues with unchanging characteristics (violent, instrumental, and political) is to some extent irrelevant, as modern conflicts that are ambiguous in their hybridity are becoming less easily defined and characterized. Therefore, the gray zone between war and peace is the primary characteristic of modern conflicts, by which it seeks to encompass operations that fall short of warfare due to the intensity, legality, and ambiguity. So, for the present research three elements will be addressed and examined due to their ability to collectively merge and impose challenges on contemporary international law. These elements will be non-state armed groups (NSAs), Cyberattacks, and Lawfare.

3.2.1. Non-State Armed Groups As An Element Of Hybrid Warfare

In contemporary conflicts and unrests around the world, the spectrum of new types of NSAs is broad, encompassing a range of identities (paramilitary forces, organized armed groups, militias, urban gangs), motivations, and degree of willingness and ability to observe IHL and other international law standards[193]. The fusion of means used by non-state armed groups and their ability to deploy modern weapon systems (drones, anti-ship missile, and cyber secure communications), that were traditionally beyond the reach of such adversaries, combined with irregular skills to a single battlefield, is one of the core characteristics of such forms of warfare. Besides, the ability to expand the battlefield beyond the purely military realm by using lawfare to make military gains unachievable on the battlefield for their adversary, elements of information warfare[194]. Such hybrid actors present a challenge to the application and compliance of the IHL. Common Article 3 of the GCs regulating NIACs, classifies the parties of a conflict that must demonstrate a certain level of organization regardless of the level of violence demonstrated, this criterion is essential under IHL. Therefore, other groups such as

[193] Kelley M., Challenges to Compliance with International humanitarian Law in the Context of Contemporary Warfare, SIT Graduate Institute, Spring 2013, p. 14.
[194] Reichborn-Kjennerud, E., Cullen, Ibid., p.1-2.

criminal gangs, paramilitary forces, and private contractors, do not meet the organization threshold contributing to the ambiguity of the legal definition of armed conflict under IHL[195].

For instance, ISIS is a violent non-state armed group and a multinational business, a terroristic group with transnational criminal actions[196]. However, ISIS was not the first non-state armed group to develop hybrid capabilities, Hezbollah and Hamas have fruitfully succeeded too in their HW campaigns. Yet, there is a difference between state and non-state hybrid warfare characteristics. Russia's hybrid campaigns in Ukraine entail the composition of different elements to wage war used simultaneously and in a coordinated manner to achieve goals with an aim that such measures would work with no need for an extended or large-scale war at a stake below the threshold of the legal definition of war[197]. Russia's operations have also shown that such an approach can be adopted by states and NSAs too in an asymmetric context, and this is a reflection of Clausewitz's dictum of war as the continuation of politics with other means, by which no official declaration of war and proxy armed groups are to be deployed in Ukraine, making the legal liability a difficult issue.[198] ISIS, on the other hand, is a more complicated entity and has different legal responsibilities, but in contemporary conflicts, both entities have a relation in terms of blending the capabilities and roles to a single battlefield. States rely on proxies for several reasons, mainly proxy have easier access to the communities they are fighting for or on their territory, as they are more accepted than foreign troops rather than promoting their nationalistic backlash that often accompanies foreign interventions.

Also, the proxy groups can limit escalation between states especially when they deny any relation or responsibility for the actions of the proxy fighters or groups. For example, the little green men in Ukraine and its relation with Russia is to an extent, considered a sponsored non-state hybrid group. These entities have robust guerilla hit-and-run tactics for attacking small-scale enemy units and have moved up the spectrum of warfare to develop impressive semi-conventional forces, which have been able to conduct both offensive and defensive operations against seemingly more formidable conventional forces[199]. Another example is the maritime militias particularly based in the South China sea. China has a wide range of territorial claims

---

[195] 31st International Conference of the Red Cross and Red Crescent, ICRC Report 2011: International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, p.8

[196] Aridi A., An Interdisciplinary Approach to Combat ISIS," Legal, Political, and Socio-Economic", Conference paper at the 4th International Conference of PhD Students and Young Researchers, International Network of Doctoral Studies in Law 2016, p. 26.

[197] Hashim A.S., State and Non-State Hybrid Warfare, Oxford research Group, March 2017.

[198] Bachmann S. and Gunneriusson H., Hybrid Wars: The 21st Century's New Threats to Global Peace and Security, Scientia Militaria, South African Journal of Military Studies, Vol. 43, No.1, 2015, pp. 88-89.

[199] Ibid.

in the South China sea that overlays with several regional neighbors, based on a series of large-scale land reclamation projects in the Spratly Islands that included the creation and fortification of artificial islands.[200] China has operated in a gray zone using tactics against the Philippine-held Thitu Island (Pag-Asa Island), also Island building and development of military infrastructure in areas over which they have established control, in addition to cyberwarfare and disinformation campaigns.[201]

The U.S. Center for Strategic and International Studies (CSIS) has published in August 2020 an important report about the U.S. competition with China and Russia, the report used the terms HW/gray zone/ irregular operations to refer to any range of actions from non-violent economic manipulation to low levels of violence using mercenaries.[202] CSIS noted that China, as part of its hybrid coercive operations, uses civilian fishing boats operating in contested waters of the South China Sea as an example of such proxy forces.[203] For example, in April 2012, A Philippine Navy surveillance plane spotted eight Chinese fishing vessels in the disputed Scarborough Shoal. The Fishing vessels were intercepted and found that they were equipped with satellite navigation systems and radio communications, but the Philippines was not able to arrest the fishermen after being blocked by two Chinese marine surveillance ships. An incident was followed by cyber-attacks against the Government of the Philippines and private institutions in the following months.[204] China's maritime militia stands as an important tool that can be less provocative to avoid both international sanctions and maintain regional interest, a core instrument for hybrid adversaries. And in a country, such as China, there is no doubt the actions of these fishermen are imputed to the Chinese government despite their covert and irregular activities that are masked to deny any responsibility or direct involvement in any threat or conflict.

---

[200] Browne A., How China Upstaged U.S. with a " Great Wall of Sand", Wall Street Journal, April 12, 2016, https://www.wsj.com/articles/how-china-upstaged-u-s-with-a-great-wall-of-sand-1460439025

[201] Chorn A. and Michiko M., Maritime Gray Zone Tactics: The Argument for Reviewing the 1951 U.S.-Philippines Mutual Defense Treaty, CSIS, October 2019. https://www.csis.org/maritime-gray-zone-tactics-argument-reviewing-1951-us-philippines-mutual-defense-treaty

[202] Desk W., Explainer: What is Hybrid warfare and how has China used it?, 14 September 2020, https://www.theweek.in/news/world/2020/09/14/explainer-what-is-hybrid-warfare-and-how-has-china-used-it.html

[203] Cordesman A., U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy, Center for Strategic International Studies CSIS, August 2020, pp 18-20

[204] Chorn A. and Michiko M., Ibid.

3.2.2. Cyber Operations in Hybrid Context

Cyber Space is a globally interconnected network of digital information and communication infrastructures, including the internet and telecommunication network. This domain of electromagnetic activity supported by information and communications technologies has a special characteristic[205], by which it is the only domain that is entirely man-made, created, maintained, and operated by public and private stakeholders across the globe, and changes constantly in response to technological innovation[206]. This cyber interconnectivity has extremely useful and promising advantages basically in peacetime in terms of increasing communication and development of economy and social world, however such interconnectivity in wartime or tensions makes it vulnerable because everything can be targeted[207]. Attacks against chemical or nuclear plants or transportation systems are technically possible with huge consequences on population and state infrastructure. The international community tends to understand cyber security in terms of cybercrime or cyber terrorism[208]. This could be seen in the Council of Europe's Cybercrime or so-called Budapest Convention, and another example is the Organization for Security and Cooperation in Europe (OSCE) which published a guide on protecting critical energy infrastructure from terrorist threats originating from cyberspace[209]. Nevertheless, without any concrete treaty framework, it will be hard to establish customary norms specific to the use of cyberspace and modern communications in contemporary conflicts.

However, on the other hand, cyber-attacks were analyzed in the context of international law by studying their impact on the prohibition on the use of force (UN Charter), and their impact as a weapon on regulating armed conflicts under the IHL was addressed in Tallinn Manual. The legality of cyberattacks is generally approached from the prohibition on the use of force under the UN Charter, but many cyber-attacks do not manifest physical damage and are thus not captured by Article 2(4) of the UN Charter. So, Cyber-attacks can be seen as a subset of cyber

---

[205] Butrimas, V. National Security and International Policy Challenges in a Post Stuxnet World, Lithuanian Annual Strategic Review 2013-2014, Vol. 12, De Gruyter Open 2014, p. 11.

[206] Melzer N., Cyber warfare and International Law, UNIDIR Resources 2011, p.5. www.unidir.org

[207] The term "Cyber" is used to refer to the use of computer technology and the internet for operations in the so-called fifth dimension by which "cyber operations", "cyber war" and "cyber-attacks" are examples of such operations depending on their intensity. For more information about the cyber conflict classification, see Schmitt M., Classification of cyber conflict, Journal of Conflicts and Security Law, 2012, p. 245-260.

[208] Butrimas, V. Ibid. p. 12.

[209] Organization for Security and Cooperation in Europe, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyber Space, 2013. See also Butrimas, V. Ibid. p.12

operations employing the hostile use of cyberspace capabilities, by both states and NSAs, to cause damage, destruction, or casualties to achieve military or political objectives[210]. And it is generally accepted that cyber operations may constitute the use of force and potentially trigger the right to self-defense under the UN Charter[211]. Cyber-attacks that do not necessarily violate the non-use of force principle do not mean they are lawful, instead, where such attacks are coercive in nature, they may constitute a violation of the principle of non-intervention that is embedded in customary international law. Yet the degree of intensity that qualifies to a use of force is relatively high, a complex issue that exploits an obscure gray area of international law[212]. Such operations below the threshold of an armed attack or clear use of force are the types of attacks that are more common in current international relations. States in such cases are assessing "scale and effect approach" on a case-by-case basis to determine when a cyber operation that is not part of a broader kinetic attack qualifies as a "use of force" in violation of the UN Charter Article 2(4), a standard that is drawn from the ICJ in the paramilitary activities judgment (para. 195). Some follow the requirements that are also offered in Rule 69 of the Tallinn Manual (the severity of the interference, the immediacy of the cyber operation's effects, and the degree of intrusion), and may add additional ones such as Germany that also considers the degree of organization and coordination of the malicious cyber operation period as one of the requirements.[213] All the above highlights a series of questions related to the classification and identification of cyber-attack as an armed attack, and the applicability of self-defense to cyber operations conducted by NSAs that are easier to camouflage, especially since they require a lower level of structural organization, materials, and human resources, and create a significant challenge to states in spotting and intercepting such attacks compared to their ability to identify and prevent kinetic attacks by similar groups.

An overview of the Tallinn Manual shows the importance of this document, as it involved a group of experts mainly international law scholars and practitioners led by Professor Michael N. Schmitt, the chairman of the international law department of the United States Naval War College. Also, it was observed by NATO, the US Cyber Command, and reviewed by the

[210] Sigholm J., Non-state Actors in Cyberspace Operations, Swedish National Defence College, 2016, p.6.
[211] Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0, Schmitt M. and Vihul edt., prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013, p. 312.
[212] Schmitt, M., Gray Zones in the International Law of Cyberspace, the Yale Journal of International Law, 2017, p. 4-5.
[213] Schmitt M., Germany's Positions on International Law in Cyber Space, Part II, Just Security, March 2021. https://www.justsecurity.org/75278/germanys-positions-on-international-law-in-cyberspace-part-ii/

International Committee of the Red Cross (ICRC) for being the guardian of IHL[214]. The manual distinguished between Jus in Bello that regulates the conduct of hostilities and Jus ad Bellum which regulates the use of force in international law. Following the cyber operations that have risen sharply in the last decade, the cyber domain has become a platform for both conventional warfare, as well as HW, which prompted a group of experts in cyber law to study the existence of a customary international norm based on the principle of sovereignty, which prohibits these minimal uses of force in cyberspace, and codified it in the Tallinn Manuals[215]. Cyberwar and Cyber-attack lack clarity in the terms they are used for, a cyber-attack might lead to an armed conflict and might not, while cyberwar occurs when cyber-attacks reach the threshold of hostilities commonly recognized as an armed conflict by the international community and as defined by international law[216]. According to the Tallinn manual, cyber operations are the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace[217], defining such attacks as: "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects"[218].

Cyberwarfare has been defined broadly by some scholars, for example, Joseph Nye in 2015 includes in his definition all forms of electronic crimes and sabotage through DoS (denial of service) attacks[219]. However, a more restrictive definition must be considered and focus merely on the dual infrastructure and its vulnerability to cyber means, and its impact on the applicability of international law. In this regard, Michael Schmitt's views on cyber operations were essential for unfolding the criteria that should be met for cyber operations to reach the level of armed force. So, what is known as Schmitt criteria categorize the following:

- *"Severity* looks at the scope and intensity of an attack. Analysis under this criterion examines the number of people killed, the size of the area attacked, and the amount of property damage done. The greater the damage, the more powerful the argument becomes for treating the cyber-attack as an armed attack.

[214] The Tallinn Manual is a non-binding document and represents only the opinions of its drafters, however it is the first attempt to tackle cyber warfare from an international law perspective.
[215] Nordstrom C., The Regulation of Cyber Operations Below the Threshold of Article 2(4) of the Charter: An Assessment of Rule 4 of the Tallinn Manual 2.0, Master's Thesis in Public International Law, University of Uppsala, 2019, p. 7-8.
[216] Sigholm J., Ibid. p 7.
[217] Schmitt, M., Tallinn Manual on the International Law applicable to Cyber Warfare, Ibid. p. 258.
[218] Tallinn Manual on the International Law Applicable to Cyber Warfare, NATO Cooperative Cyber Defense Centre of Excellence CCDCOE, Cambridge University Press 2013, Rule 30
[219] Nye, Joseph S., International Norms in cyberspace, Project Syndicate, 11 May 2015.

- *Immediacy* looks at the duration of a cyber-attack, as well as other timing factors. Analysis under this criterion examines the amount of time the cyber-attack lasted and the duration of time that the effects were felt. The longer the duration and effects of an attack, the stronger the argument that it was an armed attack.
- *Directness* looks at the harm caused. If the attack was the proximate cause of the harm, it strengthens the argument that the cyber-attack was an armed attack. If the harm was caused in full or in part by other parallel attacks, the weaker the argument that the cyber-attack was an armed attack.
- *Invasiveness* looks at the locus of the attack. An invasive attack is one that physically crosses state borders, or electronically crosses borders and causes harm within the victim-state. The more invasive the cyber-attack, the more it looks like an armed attack.
- *Measurability* tries to quantify the damage done by the cyber-attack. Quantifiable harm is generally treated more seriously in the international community. The more a state can quantify the harm done to it, the more the cyber-attack looks like an armed attack. Speculative harm generally makes a weak case that a cyber-attack was an armed attack.
- *Presumptive legitimacy* focuses on state practice and the accepted norms of behavior in the international community. Actions may gain legitimacy under the law when the international community accepts certain behavior as legitimate. The less a cyber-attack looks like accepted state practice, the stronger the argument that it is an illegal use of force or an armed attack." [220]

To illustrate, Cyberwarfare can be defined as methods of warfare that rely on information technology to be used in the context of armed conflict. Therefore, an adversary can potentially attack opponents' computer system by infiltrating or manipulating any military or non-military infrastructure that are vital for the latter, which might cause directly or indirectly civilian damage. In other words, Cyberwarfare is a politically motivated attack conducted in cyberspace through cyber means and methods, mainly targeting official websites and networks, disrupting, or disabling essential systems, stealing or altering classified data,and crippling financial systems among many other possibilities[221]. The interconnectivity of the Internet poses a threat to civilian infrastructure. Most military networks rely on civilians, mainly commercial, computer infrastructures, such as undersea fiber optic cables, satellites, routers, or nodes.

[220] Schmitt, M., Cyber operations and the Jus ad bellum revised, vol. 56, Villanova Law Review 2011, pp 576. See also Wingfield T., The Law of Information Conflict: National Security Law in Cyberspace, Ageis Research Corporation, 2000, p. 124-127.
[221] Rouse M., Cyber Warfare, www.techtarget.com , May 2011.

Conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems relying on global positioning system (GPS) satellites, which are also used by the military[222]. Malware as an example, that is slipped into systems to cause disruption and break-down of the power grid, telecommunication and others can come with high costs. Stuxnet malware of 2010 proved that cyber weapons could be offensive too, and with the evolving role of NSAs in the cyber arena, actions can lead to dangerous consequences[223].

Therefore, for cyber-attacks to qualify as an armed attacks they must fit into the kinetic effect of attacks which provides a fruitful basis for analyzing Jus ad Bellum in the context of cyber-attacks. However, considering the physical damage criteria, attacks targeting critical national infrastructure that aim deliberately to destroy or damage objects of strategic values of another state must be dealt with in an expansionist manner to be considered as an armed force even with no physical damage[224]. For instance, most States reject the US position that considers the threshold of an armed attack is identical to that for the use of force, rather they consider that an armed attack is the gravest form of use of force, as viewed by the ICJ in the paramilitary activities judgment.[225] While other states such as France consider that a major attack against their economy would be an armed attack that allows states to enjoy the right to self-defense in cyber-space.

So, cyber warfare is an ideal vehicle for a proxy strategy, given the difficulties in tracing the exact origin of cyber-attacks, this anonymity is one of the main features of HW by which it relies on the fusion of new technology and the society's reliance on a computer network with the ability to avoid clear attribution by using proxies[226]. For instance, NATO allies consider that attacks launched by NSAs even if they are not acting on behalf of the state or with substantial involvement of a state can be treated as justifying a response in self-defense, which is seen as a rejection to the ICJ judges' views in the paramilitary activities case that maintain such response only when NSAs are acting on behalf of a state.[227] Therefore, a deterrent approach in establishing a legal framework through treaties, agreements, and national policy for non-military means is still lacking and left in some areas for the States to decide. That is

[222] ICRC, New Technologies and Warfare, Vol. 94, summer 2012, p. 538
[223] Sehgal, I., Different Forms of Hybrid Warfare, Daily Times, October 11,2018.
[224] Al Aridi, A. The Virtual Trojan Horse in Modern Conflicts, Law, 107, doi:10.15388/Teise.2018.107.11824, p.67
[225] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America), ICJ Rep 14, para 95.
[226] Mumford A., Proxy Warfare and the Future of Conflict, The RUSI Journal 2013, p. 41-42
[227] Schmitt M., Germany's position on International law in Cyber space, Ibid.

the reason various voices called for a digital Geneva Convention that will commit governments to protecting civilians from state-sponsored cyber attacks in times of peace. This initiative was brought by Microsoft president and chief legal officer Brad Smith while addressing RSA security conference in Sand Franciso in 2017.[228] The initiative is an exciting call to action for defining new rights and responsibilities and will certainly need dialogue as it is difficult for international powers to agree on any meaningful standards that would oppose their interest, also some states will not adhere to the treaty to which they agreed, and finally the complexity of attribution as a major factor of non-military means that will make the verification of treaty violation a difficult task.

3.2.3.Lawfare

International law is a distinct system that operates according to its normative logic but intersects with other social systems. It is not considered novel for international law to be an instrument for the promotion of national interest, however, what is new, is the contemporary strategic environment that endorses the use of law as means of conflict and the threat to the integrity of the international legal system by undermining respect for the rule of law in international affairs[229]. And while military operations have to be carried out in compliance with international law, the legality of such operations has brought Lawfare to light. Lawfare, Law encirclement, or legal warfare, a term that is used interchangeably was introduced by US Air Force lawyer Charles Dunlap Jr. in the 2001 essay by asserting that "Lawfare, the use of law as a weapon of war, is the newest feature of 21st century"[230]. It is viewed as a useful tool for both state and NSAs, and consists of characteristics that range from asymmetric warfare using a legal system against an adversary; an instrument of state power; or a strategy that stipulates the engagement of a state in international law. Lawfare aims to create an environment that is based on a lack of a clear classification of the conflict whether IAC or NIAC, the paradigm applicable law and the legal responsibility, and finally the demand for accountability and denial

[228] Transcript of Keynote Address at the RSA Conference 2017 "The Need for a Digital Geneva Convention", Brad Smith , President of Microsoft Corporation, San Franciso , Californa, February 14,2017.
[229] Sari, A. Blurred Lines: Hybrid Threats and the politics of International law, Strategic Analysis, Hybrid COE 2018, p.4.
[230] Dunlap, Charles J. Jr., Colonel, USAF, Law and Military Interventions: Preserving Humanitarian Values In 21st Conflicts, Paper Prepared for The Humanitarian Challenges in Military Intervention Conference, Carr. Ctr. For Human Rights Policy Harvard University, Washington D.C., Nov. 29,2001. Dunlap has addressed the following questions: "Is warfare turning into lawfare? In other words, is international law undercutting the ability of the U.S. to conduct effective military interventions? Is it becoming a vehicle to exploit American values in ways that increase risks to civilians? In short, becoming more of the problem in modern war instead of part of the solution?"

of involvement. For example, Russia with regards to the conflict in Ukraine in 2014 has denied being an active part in the conflict instigating the law to be evaded and misused[231]. So in principle, the tools and means of hybrid warfare are unlimited, and the legal framework of it, also termed as lawfare, is an integrated part of it.

However, Dunlap was not the first to introduce lawfare, rather it goes back four hundred years to Hugo Grotius, to the times where European countries were competing to control seafaring trade routes. Grotius was hired by the Dutch East India Company (DEIC) against the attempts of Portugal to protect the spice trade by deploying its navy to block DEIC access in the Indian Ocean[232]. Grotius was asked to devise a theory "De Jure Praedae" (commentary of Law of Prize) to defend the company and show that war might rightly be waged against, and the prize is taken from the Portuguese on the ground that they wrongfully tried to exclude the Dutch[233]. As a result, Grotius has written his seminal work "Mare Liberum" in 1609, in which his Freedom of Sea theory was adopted by most states in the 1700s by which he used the law to accomplish objectives that Dutch military power could not and thereby solidified the concept of freedom of the seas in modern International Law.

Consequently, international law was developed to prevent violence and endorse negotiations and agreements, therefore it was not intended to be used to justify annexations or invasions the way it is being interpreted by some states. Therefore two bodies of law apply to the use of armed force, Jus ad Bellum and Jus in Bello, both share similar principles such as proportionality and necessity that differ in application, by which under jus ad Bellum the principles requires that any use of force in self-defense must be necessary and proportionate in defeating or deterring an attack by an adversary, while under jus in Bello it requires that armed forces must not attack a target if the expected casualties are excessive concerning the anticipated military advantage gained. So lawfare in modern conflicts is used to mix the status of such principles for strategic and tactical purposes. The fluid interpretation of international law is being used extensively to form a hybrid campaign, and targeted states were not able to be protected by the current legal system that is based on the rule of law.[234] As hybrid threats are designed to exploit gray areas and fault-lines in law, they thrive on legal ambiguity and

---

[231] Bachman, S. and Mosquera A., Lawfare and Hybrid warfare- How Russia is Using the Law as a Weapon, University of Exeter Strategy and Security Institute Workshop 2015, p. 27.

[232] Anand R.P., Maritime Practice in South-East Asia until 1600 A.D. and the Modern Law of the Sea, 30 International and Comp. L.Q., 1981, p. 440-442

[233] Anand R.P., Maritime Practice in South-East Asia until 1600 A.D. and the Modern Law of the Sea, Ibid., p.442

[234] Voyger, M., "Lawfare"- the forgotten element of Russia's hybrid war against the West, 22 December 2018 https://toinformistoinfluence.com/2018/12/22/lawfare-the-forgotten-element-of-russias-hybrid-war-against-the-west/

uncertainty[235], and that lies in the core of lawfare. Such development is due to the asymmetrical warfare replacement to the conventional wars which in turn amended the understanding of certain uses of international law to achieve a military objective, which has an impact on the interpretation of both jus ad Bellum and Jus in Bello, the interpretation of the proportionate and requirements, and impact on the actual conduct of hostilities.[236]

So, lawfare as a component of HW has its impact on international law particularly in the separation between jus in Bello and jus ad Bellum that has been historically emphasized to serve different purposes and results. By which the violation of jus ad Bellum is an unlawful use of force that could constitute a crime of aggression, while violation of jus in Bello could constitute a war crime. Lawfare, as mentioned above, is a tool for both states and NSAs, the latter finds it as an important means, particularly in a disadvantaged position (insurgents, terrorist groups) in an asymmetric conflict. Disadvantaged combatants find refuge in lawfare by not distinguishing themselves from the local population (shifting soldiers and military equipment into civilian neighborhoods, launching rockets from populated areas, employing cyber hackers) to confuse the IHL applicability due to the impact of such actions on the principle of distinction. Lawfare as part of a hybrid campaign that includes NSAs and cyber operations is highly challenging due to its ability to enforce misapplication of the law in conflating jus ad Bellum and Jus in Bello. In this context, Prof. Von Arnauld perfectly noted that: "behind this dazzling concept of hybrid war, lies a combination of open and covert, direct and indirect operations, propaganda and disinformation. As an example, Russia during the conflict in Ukraine has relied on operations of the marked or/and unmarked military forces, support of rebels, classical military actions as well as cyber-attacks and was flanked by propaganda and targeted misinformation at home and abroad.". That will be seen in the distinction and lack of definition of the conflict (IAC, NIAC, civil unrest), the confusion to which is the applicable law and its impact on the fundamental goals of IHL in protecting civilians and those hors de combat, and deniability by which Jus ad Bellum could be evaded or misused to void the inherent principles of international law and reject the validity of treaties.

In practice, States also rely on lawfare, for example, Russian lawfare sponsors what is called the principle of ethnic self-determination to subvert the unity of its target nation and vague

[235] Sari, A. Workshop on Legal aspects of Hybrid Warfare, The University of Exeter's Strategy and Security Institute, 16-17 September 2015.

[236] Blank L., A New Twist on an Old Story: Lawfare and the Mixing of Proportionalities, Case Western Reserve Journal of International Law, 2011, vol. 43, p. 711

cultural concepts, such as "Russkiy Mir" to justify Russia's self-proclaimed right to humanitarian intervention to protect Russian speaker populations[237]. Russia has used the law as means to justify its activities in neighboring countries. For instance, the Constitutional Court of the Russian Federation has issued an opinion on the 19th of March 2014 on the constitutionality of the treaty on the incorporation of Crimea.[238] According to Article 8(1) of the Federal Constitutional Law on the Procedure of Admission to the Russian Federation and Creation of a New Subject of the Russian Federation in its Composition (hereinafter referred to as the Incorporation Law) specifies that the treaty on the admission of a new subject can only be ratified if the constitutional court of the Russian Federation agrees that this treaty complies with the Constitution of the Russian Federation. The court has unanimously approved the constitutionality of this treaty, however, it has ignored whether the treaty complied with the international obligations of the Russian Federation arising out of general international law, in particular non-use of force and non-intervention obligations under international law. Despite the illegality of such treaty and the breach of international obligations that were ignored intentionally by the Constitutional Court of the Russian Federation that contradicted various international resolutions condemning the annexation of Crimea, yet it is a clear example of how States tend to use the law to justify their actions on the international level. Similarly, the amended law grants Russian citizenship based on residency that backs to the USSR and the Russian Empire. A practice that boosts the Russian population in neighboring states such as Georgia and Ukraine and extends the territorial influence to have more superiority in resolving any existing border disputes[239]. Also, as Russian forces moved out of their Sevastopol base on 28 February 2014, no single bullet was shot, and no casualties. Russia considered it a winning card to prove that the population in Crimea wanted to be part of Russia and that Ukraine accepted the Russian annexation in the sense that such acquiescence can create legally binding outcomes[240]. However, if Ukraine has taken no action to counter the insurrection of Ukrainian nationals acting without any external assistance, then the pro-Russian Crimean population would have had a solid claim to lawful secession[241]. But that was not the case, Ukraine's conduct was not acquiescence, and Crimeans had significant Russian influence at every step

[237] Voyger, M. Lawfare- the forgotten element of Russia's hybrid war against the West, Baltic Defense College Tartu Estonia, https://www.integrityinitiative.net/articles/lawfare-forgotten-element-russias-hybrid-war-against-west
[238] Decision No. 6-P of 19 March 2014, Rossiyskaya Gazeta, Federal Issue No. 6335, 19 March 2014.
[239] Voyer, M., Ibid.
[240] C. Macgibbon, The Scope of Acquiescence in International Law, 31 British Yearbook of International Law, 1954, p. 143.
[241] Mary Ellen O'Connell, The Crisis in Ukraine -2014, Ibid. p. 861-862

toward secession. Russia's annexation of Crimea showed that lawfare has been very effective to deny any violations made. The Russian claims of remedial self-determination have been rejected as almost there had been no systematic violent attacks on ethnic Russians before the annexation or invasion[242], while the sponsoring of the militia groups in eastern Ukraine to launch attacks on behalf of Russia, was more difficult to prove.

Similarly, China has issued "The Political Work Guidelines of the People's Liberation Army (PLA)" in 2003, a new warfare concept for the PLA which is the Three Warfare (in Chinese it is known as "San Zong Zhanfa") to be applied during both peacetime and wartime. This document highlights three main concepts:

- "Public Opinion or Media warfare such as using distorted information spread fake news,
- Psychological warfare refers to the application of military and non-military measures to disrupt adversaries.
- Legal warfare (lawfare), which helps the state to undermine other states' foreign policy goals through the international environments, especially that justifying China's actions in international law and establishing positions in domestic law is an important factor for the PLA."[243]

The legal warfare efforts are designed to establish positions in domestic and international law as a legal basis for military action or as a means of limiting the freedom of action of other nations[244]. According to the Chinese strategy, the legal warfare, Lu Hucheng and Zhang Yucheng of the General Staff Department Political Department considered that it is a special form of military operations to be undertaken in preparation for a conflict. They also consider that legal arguments, propaganda, and international agreements worked in advance as justifying any necessary military actions[245].

---

[242] OSCE (HCNM), Human Rights Assessment Mission in Ukraine, May 2014. "No Increase in the manifestation of intolerance or escalation of violence against the Russian-speaking population was observed in the visited regions." See also Rath B., The Virtues of Bright Lines: Self-Determination, secession, and External Intervention, German Journal of Law 2015, p. 384

[243] PLA Doctrine is contained in combat regulations, which are referred to in open sources but not openly available. Authoritative PLA campaign literature and other sources. It discusse at lenth the operational concept that tell the PLA how to fight and are this clearly representative of doctrine. See more, Kania E., The PLA's Latest Strategic Thinking on the Three Warfare, The Jamestown Foundation, August 2016, Vol. 16, issue 13. Available at: https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares. See also, Burke E., Gunness K., Cooper C. and Cozad M., People's Liberation Army Operational Concepts, RAND Corporatio, Research Report 2020, p. 14-16. Available at: https://www.rand.org/content/dam/rand/pubs/research_reports/RRA300/RRA394-1/RAND_RRA394-1.pdf

[244] See more about Chinese Legal Warfare, Wortzel L., The Chinese People's Liberation Army and Information Warfare, United States Army War College Press, March 2014, pp. 37-42

[245] Le Hucheng and Zhang Yucheng, "The Utility and Position of Legal Warfare in the Preparation for Military Conflict", Liu and Liu, Xin Junshi Geming Yu Fazhi Jianshe 2002, pp. 355-362

To summarize, it is obvious that the employment of lawfare is not limited to the strong or weak states or even NSAs, on the contrary, it has been embraced by both. Such an element of HW may delegitimize international law by undermining its values with relativism and opportunism[246]. This ambiguous situation creates confusion to the applicable law and the legal responsibility of actions, based on the legal uncertainties arising from the vagueness of lawfare, the adversaries (whether state or non-state armed groups) exploit the disadvantages of legal restrictions placed upon the complaint actor leading to the emergence of asymmetric warfare by abusing laws[247]. The use of lawfare that finds its way in HW means, negates the validity of treaties and challenges the inherent principle of international law's *pacta sunt servanda*, by which states and NSAs that are parties to an agreement, interpret and apply its provisions depending on the particular circumstances to benefit from such a deviation[248]. One of the examples that fit in this criterion is the use of civilians as human shields to render military targets immune from attack offers a challenge to the Jus in Bello, mainly the principle of distinction and proportionality. Also, that has a big impact on the separation between the two bodies of law that apply to the use of armed force and that require that applicable laws must assert their validity in the face of HW. None of these instruments are indeed new, however, the changed quality lies rather in their combination and the orchestration in the use of the means. This will have to be considered in the development of a counterstrategy and will indirectly radiate into IHL via the principle of military necessity. Law, however, calls for a differentiated assessment of the individual instruments for which it has established rules to build. So, proponents of lawfare must develop explicit principles that operationalize the idea that any use of law must be consistent with the fundamental norms and values of the legal system, at the national and international level.

[246] Newton, M., Illustrating Illegitimate Lawfare, Case Western Reserve Journal of International Law, 2010, Vol. 43, no. 1, pp. 225-277

[247] Mosquera A. and Bachmann S., Understanding Lawfare in a Hybrid Warfare Context, Articles on NATO Current Challenges, NATO Legal Gazette, October 2016, p. 13-14.

[248] Mosquera A. and Bachmann S., Lawfare in Hybrid Wars: The 21st Century Warfare, Journal of International Humanitarian Legal Studies, Brill-Nijhoff, Vol.7, March 2016.

II- International Law on the Use of Force and Hybrid Warfare

Jus Ad Bellum is the most common Latin term adopted to refer to the international law governing the use of force in international relations. This chapter will consider the primary legal issues under international law on the use of force (Jus ad Bellum) presented by Hybrid warfare. The legal terminology with regards to warfare has developed separately under laws on the use of force and the laws of armed conflict, the following chapter will focus on the concept of the use of force, armed attack, and aggression all of which appear under the UN Charter and relates firmly to modern conflicts.

Firstly, it is important to discuss the nature of the prohibition on the use of force, and then its interpretation and application to HW features that potentially amount to the use of armed force. Under the UN Charter, States have the obligation not to use force in their international relations and to settle any dispute peacefully according to Article 2(4) of the Charter. It constitutes a general prohibition on the threat or use of force and concludes that 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 any other manner inconsistent with the Purposes of the United Nations. This prohibition is discerned as more than mere conventional law or customary international law, it is of jus cogens nature (peremptory norm of international law and considered the highest ethical principles), by which the unconditionality of this norm means that any state practice that constitutes conduct in violation of the article does not change the prohibition but violates it. So, no derogation from these norms is permitted through treaty and customary international law for the creation and modification of its rules.

Nevertheless, the UN Charter provides exceptions to the use of force through self-defense and the authorization of the Security Council to maintain or restore international peace and security. But the legal thresholds stressed out in the UN Charter for such use of force to be considered permissible rely largely on the occurrence of an armed attack, which mainly raises concerns about the abuse of such thresholds by adversaries for their own tactical and strategic advantage. First of all, the force under the prohibition is not limited to the use of kinetic, chemical, biological, or nuclear weaponry, by which the ICJ in its advisory opinion concerning the legality of the threat or use of Nuclear Weapons 1996 noted that the prohibition applies to any use of force regardless of the weapons employed[249]. Nonetheless, the notion of force in the UN

[249] International Court of Justice ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996, p 39; and see also, Ian Brownlie, International Law and the Use of Force by States, 1963, pp. 362, 431.

Charter refers to armed or military force[250], as also explained in paragraph 7 of the preamble that stated: "The goal of the UN is to ensure that by the acceptance of principles and the institutions of methods, the armed force shall not be used."[251], despite some proposals to include economic pressure as a form of force that was rejected[252]. Article 2(4) of the UN Charter is generally expected to cover the use of armed or physical force and extends to the indirect use of force by NSAs.[253]

Alternatively, HW mainly relies on the fusion of conventional military and non-military forces, law enforcement, irregular proxy operations, and cyberattacks that play an important role in keeping operations at a low-intensity level. Accordingly, analyzing the concepts of use of force, interventions, armed attack, self-defense, and an act of aggression in the context of HW is essential especially since modern legal theory aims to achieve sustainable peace in international relations through the respect of law, the peaceful resolution of disputes and praises the existence of de jure and de facto mechanisms of governance both at an institutional level (UN Security Council) and normative level (jus cogens norms). While the Jus ad Bellum regime is foundational to the global order and has been remarkably resilient over time, yet States' practices proved that certain uses of force norms are being compromised, by which the credibility of the entire regime and its ability to regulate contemporary threats and uses of force, has been called into question[254]. Debates are indispensable and positioned around the permissibility of the use of force by states being justified to stop or prevent a humanitarian crisis (Humanitarian intervention which resurged at the end of the 1990s in the context of the Kosovo Intervention and continued to develop in the early 2000s through the responsibility to protect R2P) as a developing exception outside of the Charter. Arguments also highlighted the victim States' right to self-defense that have not suffered from an armed attack (pre-emptive self-defense) but still holds the right to protect its sovereignty from imminent or future operations if the requirements of potential attacks have been met. And finally, the right of self-defense that is exercised in response to armed attacks by NSAs lacking any concrete relation with a State (the US actions in Afghanistan 2001, Intervention against ISIS in Syria, and the

[250] See UN Charter, Chapter VII on the Actions with respect to Threats to the Peace, Breaches of the peace and Acts of Aggression, art. 44.
[251] Dörr O., "Use of Force, Prohibition of", Max Planck Encyclopedia of Public International Law, September 2015, para. 11
[252] ILA's Report on Aggression and the Use of Force, International Law Association, Sydney Conference 2018, p.4.
[253] Nicaragua v. United States of America, Ibid., para. 228
[254] Hakimi M., and Katz-Cogan J., The Two Codes ion the Use of Force, The European Journal of International Law, vol. 27, no. 2, Oxford University Press on behalf of EJIL 2016, p. 257-258

operation by Turkey against the Kurdish rebels in Syria "Operation Olive Branch") by which such operations were targeting NSAs in the territory of other states based on the actions of such armed groups.[255] Therefore, among disputed issues surrounding the right to self-defense codified in article 51 of the UN Charter and regulated in customary international law is the definition of an "armed attack", which according to the ICJ is triggered against either state forces or irregular armed bands sent by a state.

All the previous debates are relevant to scenarios of hybrid attacks blending the role of NSAs of asymmetric nature and using virtual weapons that have significantly influenced the expansion of the legality to use force in international relations[256]. Moreover, it promoted the debates about the uncertainties flowing from international law's legitimating principle concerning response to cyber and NSAs operations. In this matter, General Keith Alexander (the Commander of the U.S Cyber Command) stated: "There is no international consensus on a precise definition of a use of force, in or out of cyberspace. Consequently, individual nations may assert different definitions, and may apply different thresholds for what constitutes a use of force."[257] This reflects the states' uncertainty in practice and response towards operations that can fall below the threshold of armed attacks, and whether such understanding justifies the expansion of the use of force to target cyber operators and NSAs that are covert and tend to mask the identity of the factual perpetrator. Uncertainty is also generated because articles 2(4) and 51 of the UN Charter include different wording of provisions related to self-defense and use of force, by which the latter unlike the former, makes no reference to threats but the actual occurrence of armed attack[258]. Therefore, it is essential to affirm whether Jus ad Bellum governs states' activities in modern conflicts that include the ambiguous features of HW, in particular, the vulnerabilities brought to light by the new technologies that create a new understanding of the rule of non-intervention and states' sovereignty under international law.

---

[255] Peters A., The Turkish Operation in Afrin (Syria) and the Silence of the Lambs, EJIL: Talk, Blog of the European Journal of International Law, January 30, 2018. See also, Mignot-Mahdavi R., On the illegality of the Turkish Offensive in Syria, Asser Institute Center for International and European Law, October 2019. The article highlights a vital issue with regards the silence and the use of force in international law in response to the right to self-defense to justify Turkey's military offensive in Syria

[256] Bachmann S. and Kemp G., "Aggression as Organized Hypocrisy?" – How the War on Terrorism and Hybrid Threats challenge the Nuremberg Legacy, Windsor Yearbook of Access to Justice, Feb. 2012, p.252.

[257] LTG. Keith B. Alexander, Hearings before the Committee on Armed Services, United States Senate, 111th Congress, Second Session April 2010.

[258] Glennon M., The Fog of Law and the Jus Ad Bellum, The Fog of Law Series, Just Security, April 2018.

1. The Use of Force in International Law

1.1. The Just War Theory to Modern Jus Ad Bellum

Historically, the Just War Theory is having a just reason to start a war and is mainly a set of mutually agreed rules of combat. And from a moral perspective, there is a strong presumption against the use of violence and aggression that has its roots in the Christian theology and writings of St. Thomas Aquinas. In the "Summa Theologicae", Aquinas presented the general outline of what becomes the traditional just war theory by highlighting what kind of activities can be permissible (for a Christian) in war[259]. It has been the concern of just war theorists that the lack of rules to war between belligerents should be denounced and rules shall apply equally to all[260]. There are principles for the just war that need to be met. Firstly, having a Just Cause is considered the most important condition of Jus ad Bellum, as it encompasses the basic principles behind the conflict. That was reflected in the preservation of slavery and the spread of liberty, also the protection of innocent life or defending human rights.[261] Secondly, Right Intentions are for the sake of a just cause, as the aim of the use of force must not be to pursue narrowly defined national interests by overwhelming the pretext of fighting aggression, but rather to re-establish a just peace. For instance, Immanuel Kant noted that "possessing good intent constitutes the only condition of moral activity, regardless of the consequences envisioned or caused, and regardless, or even in spite, of any self-interest in the action the agent may have."[262] Kant faced criticism for enhancing the value of self-interest and that acting in proper intent justifies actions that might lead to peace. Nevertheless, this Machiavellian approach in "The Prince" that "the ends justify the means" is not relevant in international relations, as the issue of intentions raises the concern of practicalities as well as consequences, which both should be considered before using any kind of force[263]. Thirdly, Proper Authority by which war must be launched by a correct governing body and public declaration by which war cannot be secret. Additionally, the last resort highlights that all previous conditions must be exhausted with a reasonable chance of success to avoid unnecessary bloodshed, and finally proportionality by which the end is proportional to the means used[264], and be in line with the

[259] Moseley A., "Just War Theory", in the Internet Encyclopedia of Philosophy 2009.
Available at: https://www.iep.utm.edu/justwar/
[260] Ibid.
[261] Cline A., Jus Ad Bellum "Just War theory and the Pursuit of War", Learn Religions, July 2019.
[262] Moseley, A., Ibid.
[263] Ibid.
[264] Moseley, A., Ibid.

magnitude of the initial provocation[265]. The moral justification of this principle overlaps with Jus in Bello, regarding the conditions for how war should be fought. Therefore, with regards to the just cause, a policy of war requires a goal that is proportional to the other principles of it[266].

Bellum Justus or Just War theory was crucial in the pre-Westphalia order in Europe, by which the aim of the war was considered legitimate within the confines of religious natural law to allow establishing and maintaining a universal public order as designated under religion except for cases of self-defense.[267] Although having a just cause is considered the most important condition of just war, yet many scholars and states believe that the only just cause for war is self-defense against aggression targeting the territorial integrity or independence of a state[268]. However, this theory was criticized for being far too narrow and too classic. Some states consider that they have the right to defend themselves from imminent violence even if no actual attack occurred, by which states' pre-emptive strikes in cases of potential threat, are justified.[269] Also, justifications of using force included intervention across national boundaries against oppressive States, by which the legal existence of a governing body in a State does not always guarantee its moral legitimacy (in cases of genocides, massive human rights violations), by which such governments lack moral legitimacy and its political sovereignty and rights to govern are called into doubt[270].

The changing and evolving characters of modern conflicts (asymmetric, NSAs, and technological evolution) have raised concerns that such just war theories are no longer effective and applicable. And although there are viable portions of the collective security approach,

---

[265] Hubert D. and Weiss Th., The Responsibility to Protect: Supplementary Volume to the Report of the International Commission on Intervention and State Sovereignty, International Development Research Centre, Canada 2001, p. 139.

[266] Moseley, A., Ibid. see the following example: "if nation A invades a land belonging to the people of nation B, then B has just cause to take the land back. According to the principle of proportionality, B's counter-attack must not invoke a disproportionate response: it should aim to retrieve its land and not exact further retribution or invade the aggressor's lands, or in graphic terms it should not retaliate with overwhelming force or nuclear weaponry to resolve a small border dispute. That goal may be tempered with attaining assurances that no further invasion will take place, but for B to invade and annex regions of A is nominally a disproportionate response, unless (controversially) that is the only method for securing guarantees of no future reprisals. For B to invade and annex A and then to continue to invade neutral neighboring nations on the grounds that their territory would provide a useful defense against other threats and a putative imbalance of power is even more unsustainable."

[267] Uzun M., Ibid, p. 35.

[268] Green L., The Contemporary Law of Armed Conflict, Juris Publishing 2008, p. 59

[269] Walzer, M., Just and Unjust Wars: A Moral Argument with Historical Illustrations, 4th ed., Basic Books New York 2006, p.85.

[270] Luban D., "Just War and Human Rights" Philosophy and Public Affairs 1980, Vol. 9, No. 2, p. 160-181. See also Walzer M. Ibid. p. 107, stated that: "… governments that engage in massacre are criminal governments, wars of interventions resemble law enforcement or police work".

particularly regarding the UN Charter (state's right to self-defense) or Chapter VII (collective response), yet such responses have limited scope to actions conducted in a blurred manner such as cyber operations below the threshold of an armed attack, non-state armed groups that do not attribute their operations to any state or disguised as civilians, and covertly conducting military operations.

Until the beginning of the 20th century, the use of force by states was considered an acceptable way of settling disputes by which the jus ad Bellum was not limited by legal restrictions as it is today in the UN Charter[271]. The only modest exception being noticed was Article 1 of the Hague Convention respecting the Limitation on the Employment of Force for the Recovery of Contract Debt (Drago-porter Convention 1907) and was subject to the debtor state's having agreed to an arbitral settlement and complying with it[272]. However, following a series of actions by states after WWI, an evolution in the matter of outlawing the use of force has been noticed. First, the Covenant of the League of Nations of 1919 had an important role in setting out the rules prohibiting the use of force in international relations by reducing the armaments to the lowest possible level, and exchanging information as to their existing armaments and their prospects.[273] It stressed that member states shall undertake to respect and preserve the territorial integrity and existing political independence of States, and the role of the Council in advising upon how this obligation shall be fulfilled.[274] The Covenant confirmed that force is a matter of concern to all member states that bound themselves to submit all serious disputes to peaceful settlement by the Council and in no case to resort to war until these procedures had had time to lead to a settlement.[275] Moreover, Article 15(7) of the League Covenant stated that "in case the council failed to adopt a report by unanimous vote, the league members reserved to themselves the right to take such action as they shall consider necessary for the maintenance of right and justice."[276]

Likewise, the General Treaty for Renunciation of War as an Instrument of National Policy (The Briand-Kellogg Pact or Treaty of Paris 1928[277]) concluded that war would no longer be used

[271] Kemp, G. The Shift from Jus Ad Bellum to Jus Contra Bellum: The Prohibition of the Use of Force in Normative and Institutional Perspective. In Individual Criminal Liability for the International Crime of Aggression, Intersentia Publication, 2015, pp. 47-48
[272] Dörr O., "Use of Force, Prohibition of", Ibid. para.4.
[273] League of Nations, Covenant of the League of Nations, 28 April 1919, art. 8-9.
[274] Ibid. art. 10.
[275] Ibid. arts.11,12.
[276] Ibid. art. 15/7
[277] Kellogg- Briand Pact 1928, a treaty between the United States and other Powers providing for the renunciation of war as an instrument of national policy. Signed at Paris, August 27, 1928; ratification advised by the Senate,

as an instrument of national policy or to solve international disputes, outlawing by that the absolute power to resort to war by its prohibition of aggressive war[278]. In Article 1 of the Pact, the states declared that they condemn recourse to war for the solution of international controversies, and renounce it, as an instrument of national policy in their relations with one another[279]. In a related manner, the Stimson Doctrine of 1932 by the Secretary of State Henry Stimson following Japan's actions in Manchuria was issued as a policy of non-recognition of states which was created because of aggression[280]. The Japanese expansion and conquest violated the country's obligation under the Kellog-Briand Pact, the League of Nations Covenant, and the Nine Power Treaty. The principles of this doctrine were used in the Sumner Welles declaration of July 1940 on the non-recognition policy of the Soviet annexation and incorporation of the three Baltic States and were strongly pursued until the restoration of independence of Estonia, Latvia, and Lithuania in August 1991. However, prohibitions focused mainly on war not the use of force, which was later violated by state practice. For example, in the second Sino-Japanese war in 1937, both states considered that their military actions against each other did not amount to war and were not a violation of international law. Therefore, the legal framework that needed a more comprehensive approach to the prohibition on the threat or use of all kinds of military force, found its way in the UN Charter articulating international rules that regulate the use of force in international relations. The Charter articulates the basic principle which is the non-use of force principle under Article 2(4) and exceptions to the basic principle through self-defense under Article 51, and the authorization of the SC under Chapter VII. The Charter was set out to ban the use of force between states by adopting a policy of collective security to be guaranteed by the Security Council, which is responsible for maintaining and restoring international peace and security[281]. Nonetheless, the main example that illustrates the significance of treaty interpretation deals with the meaning of the term "use of force" in the UN Charter's Article 2(4) that aims to limit the circumstances in which states may resort to force as a mean of resolving their differences.

January 16, 1929; ratified by the President, January 17, 1929; instruments of ratification deposited at Washington by the United States of America, Australia, Dominion of Canada, Czechoslovakia, Germany, Great Britain, India, Irish Free State, Italy, New Zealand, and Union of South Africa, March 2, 1929: By Poland, March 26, 1929; by Belgium, March 27 1929; by France, April 22, 1929; by Japan, July 24, 1929; proclaimed, July 24, 1929.

[278] Stahn, C. Jus ad Bellum, Jus in Bello . . . Jus post Bellum: Rethinking the Conception of the Law of Armed Force, European Journal of International Law, Volume 17, Issue 5, 1 November 2006, p. 923

[279] Kellogg- Briand Pact 1928, art I.

[280] The policy was implemented by the US federal government in the form of a note in Jaunary 7, 1932 and sent to the Empire of Japan and the Republic of China. The doctrine aims to not recognize any territorial changes that were excuted by force.

[281] Kretzmer D., The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum, The European Journal of International Law 2013, Vol. 24, p. 241

1.1.1. The Prohibition of Unilateral Threat or Use of Force

The prohibition of the use of force exists under both customary and conventional law (article 2(4) of the UN Charter) and is likely to be presently identical in scope. The ICJ in the Nicaragua case affirmed that when the content of treaty and customary rules are identical, they both continue to exist and apply[282]. In addition, the prohibition on the use of force is considered to be jus cogens defined in 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 and which can be modified only by a subsequent norm of general international law having the same character."[283] The prohibition is still a standstill norm in international relations, and article 2(4) is considered international law's primary analytical tool for evaluating hostile acts. In addition, the content of the prohibition on the use of armed force is tightly linked with the concept of aggression and armed attack. While not every use of force amounts to aggression, which is deemed to be the most serious and dangerous form of illegal use of force according to the concept of aggression defined in the UN General Assembly Resolution on the definition of aggression of 1974.[284]

The World Summit of 2005 confirmed that the UN Charter is sufficient to address the full range of threats to international peace and security[285]. However, after the shift of warfare from conventional to modern, new technologies have been highly recognized such as cyber-attacks and unmanned aerial vehicles (Drones). This was accompanied by the change of international actors that are no longer limited to States but involve NSAs such as terrorist groups, proxy fighters. HW raised challenging uncertainties on the role of international law in governing the new hybrid threats. And an analysis of the legal doctrine reveals different views on the interpretation of the rules governing the use of force between states reflecting different methodological approaches.

---

[282] ICJ, Nicaragua v United States of America, Ibid, Reports 1986, p. 14, paras 174-179.
[283] Vienna Convention on the Law of Treaties, 22 May 1969, Art. 53.
[284] United Nations General Assembly Resolution 3314 (XXIX), A/RES/3314, (UNGAR 3314), 14 December 1974, Article 1.
[285] World Summit Outcome 2005, UNGA res 60/1, 24 October 2005, UN Doc A/Res/60/1, p. 79

1.1.2. Article 2(4) of the UN Charter and meaning of "Force"

The rules of international law on the use of force found in the Charter and customary international law are easy to state but can be difficult to apply in practice. The primary rule of the prohibition on the use or threat of force is affirmed in Article 2(4) of the UN Charter and described as a cornerstone of international law, it directs that all member 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 any other manner inconsistent with the purposes of the United Nations. Debates concerning the interpretation of this article created fundamental division in the international community and evolves on every occasion a new weapon or form of use of force is deployed, that has been noticed in contemporary hybrid campaigns, that requires a better understanding of the foundations and the lex lata (the law as it exists) of the present provisions.

The prohibition on the use of force has been interpreted through different approaches, the narrow and broad prohibition. Proponents of the former consider that since article 2(4) prohibits armed or militarized force, then other forms of force are not prohibited (such as cyber-attacks that cause only economic aggression). John Barkham considers that this narrow take on Article 2(4) is not the intended meaning of "force" but a result of its progressive erosion through years, to appoint where it has been stripped of its meaning by new warfare methods.[286] The latter can be considered armed violence, while other scenarios such as financial regulatory measures, covert economic disruptions, or computer network attacks, may or may not be unlawful under international law of the use of force. On the other hand, according to the proponents of the broad interpretation, force in article 2(4) is not merely armed but can also include threats by economic coercion, missile tests, or military maneuvers couple with a promise to resort to armed force.[287] Such force that more swings towards coercion could conceivably consider the above scenarios as a prohibited force. Advocates for the right to use force for humanitarian reasons have shared this view by stating that humanitarian intervention using force does not compromise territorial integrity and is therefore not prohibited.[288] Nonetheless, a flexible and broad interpretation of Article 2(4) has an impact on expanding the

[286] Barkham J., Information Warfare and International Law on the Use of Force, New York University Journal of International Law and Politics, 2001, p. 109.
[287] Hsiao A., Is China's Policy to Use Force against Taiwan a violation of the Principle of Non-Use of Force under International Law, New England Law Review, 1998, Vol. 32, p. 715.
[288] Valek P., Is Unilateral Humanitarian Intervention Compatible with the UN. Charter?, Michigan Journal of International Law, 2005, vol. 26, p. 1234.

use of force in international relations and thus should not mean the same for the right to self-defense in article 51. The broad interpretation in considering force as coercion or interference aims to expand the coverage of article 2(4) beyond armed force to include violations of sovereign domains such as propaganda, political subversion, or economic disruption. Yet, the dominant view of states has long been that Article 2(4) prohibition of force and the complementary Article 51 right to self-defense apply to military attacks or armed violence.

It has been agreed that the prohibition on the use of force constitutes a peremptory norm by which any existing treaty provisions that conflict with that norm become void and terminated. Similarly, the ILC Draft Articles on State Responsibility provide that States shall cooperate to end through lawful means any serious breach of such peremptory norm nor render aid or assistance in maintaining that situation. Moreover, it was claimed that there is a *de minimis* threshold to which use of force does not fall within the prohibition of Article 2(4). According to the ICJ, it will be necessary to distinguish the gravest forms of the use of force (those constituting an armed attack) from other less grave forms. That was reassured and inferred from the case of Oil Platform by the ICJ that the threshold of gravity is flexible and dependent on the specific circumstances of each case.[289] The court added that "it did not exclude the possibility that the mining of a single military vessel might be sufficient to bring into play the inherent right of self-defense[290]." Therefore, it is understood that such an intensity threshold is not needed or at least is much lower for an act to constitute the use of force.

In other words, while the term "force" is used in Article 2(4) of the UN Charter without defining its content, it is generally accepted that it extends to armed force. This armed force that violates the prohibition on the use of force is not confined to force that is directly against State's territorial integrity or its political independence only, but rather it includes any use of force that is inconsistent with the purposes of the UN Charter, so a comprehensive ban against all uses or threats of force.[291] That highlights the broad scope of Article 2(4) that requires in certain areas a more restrictive interpretation. In doing so a distinctive relationship comes to light between force, armed attack, and aggression.

[289] ICJ, Oil Platform Case, Islamic Republic of Iran v. USA, 6 November 2003, p.51
[290] ICJ, Oil Platform Case, Ibid. 12, para. 72.
[291] Ruys T., The Meaning of Force and the Boundaries of the Jus Ad Bellum- Are "Minimal", Uses of force excluded from UN Charter 2(4), The American Journal of International Law , 2014, p. 12.

In determining the legal rule that applies, the ICJ in the Nicaragua case based its interpretation on the formulations contained in the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States under the UN Charter (The UN General Assembly Resolution 2625)[292]. This Resolution reaffirms the prohibition on the threat or use of force and indicates the notion of force is broader in scope than armed attack and aggression, by which incidents that do not qualify as an act of aggression, may still constitute a use of force. The resolution indicates that:

- "A war of aggression constitutes a crime against peace for which there is responsibility under international law.
- Under the purposes and principles of the UN, States must refrain from propaganda for wars of aggression.
- Every state must refrain from organizing or encouraging the organization of irregular forces or armed bands including mercenaries, for the incursion into the territory of another State
- The 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. The territory of a State shall not be the object of acquisition by another State resulting from the threat or use of force. No territorial acquisition resulting from the threat or use of force shall be recognized as legal".

Therefore, use of force in the context of Article 2(4) covers the direct force (cross border shooting or military incursions), or Indirect force (sponsoring, organizing, assisting, or participating in civil strife or terrorist acts against another state that amount to threat or use of force). In this context, the ICJ in Nicaragua case considered that even minor acts of interstate force fall under the general prohibition of Article 2(4) of the UN Charter, regardless if they qualify as acts of aggression or armed attacks entitling the targeted state to resort to self-defense and an exception to Art. 2(4)[293]. That will be explained in further detail in the upcoming section about the acts of aggression, however, the ICJ's judgment has identified that there are various forms of the use of force, of different degrees of gravity, that violate international law by which not all of them amount to aggression or armed attack. So, this relocates cyber-attacks in a gray area under the UN charter, and neither Opinio Juris nor State practice has provided clear criteria regarding the threshold on which such acts, not causing death and injury, be regarded as

[292] ICJ., Nicaragua vs USA, Ibid. para. 191- 195.
[293] International law Commission, Report of the International Law Commission on the work of its Thirty-second session, 5 May–25 July 1980, Official Records of the General Assembly, Thirty-fifth session, Supplement No. 10, UN document A/35/10, 1980, p. 44

prohibited actions and what would be their degree of gravity. Similarly, the question to what extent cyber operation can qualify as a force within the meaning of this prohibition?. Correspondingly, it is important to note that the term force in the former article does not limit the use of force to kinetic, chemical, biological, or nuclear weaponry. According to the ICJ in its advisory opinion concerning the legality of the threat or use of Nuclear weapons 1996, the prohibition applies to any use of force regardless of the weapons employed[294]. This would certainly include Cyber operations that cause death or injury to a person or destruction of infrastructure. For example, any cyber operation manipulating computer systems and resulting in a meltdown in a nuclear power station, or opening the floodgates of a dam above a densely populated area, or disabling a busy airport's air traffic control during bad weather conditions, each with potentially horrendous consequences in terms of death, injury and destruction[295].

A more conservative opinion was observed by the Eritrea-Ethiopia Claims Commission considering that "the commission is satisfied that minor incidents such as encounters between small infantry units, even those involving the loss of life, were not of a magnitude to constitute an armed attack by either state against the other within the meaning of Article 51 of the UN Charter".[296] This locates an adversary conducting operations below this level of intensity in combination with non-forcible means, in a position where they can achieve incremental gains without the ability of the victim state to trigger self-defense[297]. Nonetheless, not any threat or use of force prohibited by Art. 2(4) of the UN Charter will automatically constitute an armed attack that justifies self-defense under Art. 51 of the UN Charter[298]. Such illegal acts which fall below the threshold of an armed attack are at least in the view of most of the judges in the ICJ considered a breach of the obligation under article 2(4) and customary international law, such as not to intervene in the affairs of another state, not to violate sovereignty or interrupt peaceful commerce and trade. The previous means that the options available for victim states to such illegal acts that fall below the threshold of armed attack are through non-violent countermeasures.

---

[294] International Court of Justice ICJ, Legality of the Threat or Use of Nuclear Weapons, advisory opinion, 1996, p 39; and Ian Brownlie, International Law and the Use of Force by States, 1963, pp. 362, 431.
[295] Nils Melzer, Ibid., p.7.
[296] Reports of International Arbitral Awards, Eritrea-Ethiopia Claims Commission - Partial Award: Jus ad Bellum-Ethiopia's Claims 1-8, December 2005, vol. XXVI, p. 465-466, paras. 11,12.
[297] Sari A., and Lauva A., Hybrid Threats and the United States National Security Strategy: Prevailing in an "Arena of Continuous Competition", Blog of the European Journal of International Law, January 2018.
[298] Albrecht Randelzhofer, "Article 51 UN Charter", in Bruno Simma (ed.), The Charter of the United Nations: A Commentary, vol. I, 2002, p. 790

Moreover, violating the prohibition on the use of force includes military activities held by non-state armed groups.[299] In this matter, the participation in forcible acts committed by mercenaries or rebels can fall under the prohibition, by which states must refrain from organizing or encouraging the organization of irregular forces or armed bands for an incursion into the territory of another state and 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 it involves a threat or use of force[300].

Nonetheless, the UN Charter has narrowed the grounds on which relevant actors of international law may legitimately resort to armed force, the shaping of this distinctive normative feature between jus ad Bellum and Jus in Bello is essential to postulate the principle that all conflicts shall be fought humanely, irrespective of the cause of armed violence[301]. Yet, problems arise with regards to the parameters of the right to use force in self-defense defined in Article 51, especially in the era of HW. Even though hybrid adversaries do not operate in a legal vacuum and domestic and international law norms, including international human rights law, apply to their actions. Yet the hybridization of warfare and the continuous evolution of available technological tools allows adversaries to avoid manifest use of force that would reach the required threshold for triggering the application of the above norms, and creating by that a legal gray area[302].

1.1.3. Aggression and Hybrid Warfare

By the end of the Second World War, the crime of aggression was introduced in the constituent instrument establishing the Nuremberg International Military Tribunal 1945 (IMT 1945) which was also used in the Tokyo Judgment in 1948. However, the members of the international community have not been able to agree upon a legal definition of aggression, yet the judgment of the Nuremberg Tribunal makes it clear that acts of aggression are illegal under international

[299] ICJ, Nicaragua v. United States 1986, Ibid, pp. 202. See also Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v. Uganda), Judgment, 2005 I.C.J. Rep.168 (Dec. 19); Legality of the Use or Threat of Nuclear Weapons, 1996 I.C.J. Rep. 226 (July 8).
[300] ICJ., Armed Activities on the Territory of the Congo (DRC vs Uganda), para 162.
[301] Stahn, C. *Ibid.*, p. 921
[302] Legal Challenges related to the Hybrid War and Human Rights Obligations, Committee on Legal Affairs and Human Rights, Council of Europe, AS/Jur 2018, para.4

law.[303] Even before a legal definition of aggression was formed, the ability of the League of Nations or the UN was not impaired to be able to find that certain states were guilty of acts of aggression[304].

While the UN Charter does not define what constitutes an armed attack or armed aggression, the General Assembly of the United Nations adopted the Resolution 3314 (XXIX) in an attempt to clarify the notion of an armed attack by harkening back to the French language version of the UN Charter which refers to "armed aggression" rather than an "armed attack", and clarifies the legal framework in which the presumed victim state must maneuver when it uses armed forces with the aim of self-preservation[305]. However, this definition created more challenges to what armed aggression and armed attack is, also did not give a concrete clarification on the uncertain issues of Article 51 since it only mentioned the armed form of aggression. Relatively, the definition ruled in the resolution shows a significant resemblance to article 2(4) of the UN Charter with regards to both direct and indirect use of force. While HW requires an aggressor that is willing to violate a state's sovereignty by promoting violence during peacetime has created a new vehicle of aggression[306], however it is important to begin by differentiating between armed aggression and act of aggression that is established in two separate legal regimes and then analyzes whether the complexity of HW is well synchronized by Resolution 3314 that its language does not incorporate cyber weapons. The definition of aggression has created a legal grey zone with regards to cyber-attacks, which some states may consider as a loophole allowing the use of cyberweapons more in contemporary international relations.

- **Act of Aggression and Crime of Aggression**

[303] Piper D., The General Problem of Defining Aggression: The Legal Control of the Use of Force and the Definition of Aggression, Georgia Journal of International and Comparative Law, 1972, Vol. 2, p.2

[304] Ibid. p.2. see Report of the Secretary-General, October 1952, on the Question of Defining Aggression. Criteria applied when a conflict has been accompanied by the use of force, VIII, para. 96. It stated that: "…The League of Assembly made such finding with regard to the Soviet Union's invasion of Finland in 1939." See also, The General Assembly Resolution 498 1951. By which it found that both North Korea and Communist China had committed aggression against South Korea.

[305] Bou-Nader Ph., The Baltic States should adopt the Self-Defense Pinpricks Doctrine: the "accumulation of events" threshold as a deterrent to Russian Hybrid Warfare, Journal on Baltic Security 2018, vol.3, p.14-15

[306] Cantwell, D. Hybrid Warfare: Aggression and Coercion in the Gray Zone, American Society of International Law, Nov. 29, 2017, https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone According to Cantwell : HW created a new form of aggression that was outlawed by Kellog-Briand Pact, enforced by Nuremberg and Tokyo Tribunals, prohibited by UN Charter, reaffirmed in the Kampala amendments with near unanimity endorsed that aggression violates international law by states through its means (non-state armed groups, cyber-attacks) that are also seen as a form of aggression."

The definition of the Act of aggression was adopted by the UNGA Resolution 3314 (XXIX) in 1974 that states: "Aggression is the use of armed force by a State against the sovereignty, territorial integrity or political independence of another State, or in any other manner inconsistent with the Charter of the United Nations, as set out in this Definition."[307]. The definition is broad to fit the prohibition articulated in article 2(4) of the UN Charter and can be seen that it was used as a strategic asset by the state who sought to control it to mobilize it to their benefit against opponents[308]. According to the Resolution, the use of armed force by a state against the sovereignty, territorial integrity, or political independence of another state, regardless of whether or not a declaration of war has been made, are acts of aggression if they include the following:

- "Invasion or attack of the territory of one state by another state, or any military occupation, or any annexation using force on the territory of another state or part thereof.
- The bombardment or the use of any weapons by a state against the territory of another state.
- The blockade of the ports and coasts of a state by the armed forces of another state.
- The attack by the armed forces of a state on the land, sea, air forces, or marine or air fleets of another state.
- The use of the armed forces of one state which are stationed on the territory of another state with the latter's agreement, in contravention of the conditions provided for in the agreement.
- The actions of a state in allowing its territory, which it has placed at the disposal of another state, to be used by the other state for perpetrating an act of aggression against a third state.
- The sending by or on behalf of a state of armed bands or groups, irregular or mercenaries, which carry out against another state acts of an armed force of such gravity as to amount to the acts listed above, or the substantial involvement of a state in such acts."[309]

However, the concept of aggression did not gain much attention in international law in the post-charter era, as much as concepts of "use of force" and "armed attack" did[310]. Likewise, in the case law, by which the ICJ in DRC v. Uganda Judgment excluded any finding of

[307] United Nations General Assembly Resolution 3314 (XXIX), A/RES/3314, (UNGAR 3314), 14 December 1974, Article 1.
[308] United Arab Emirates: A Global Perspective on the Crimes of Aggression, STA Law Firm, 12 March 2019.
[309] United Nations General Assembly Resolution 3314 (XXIX), Ibid. article 3.
[310] ILA Report 2018, Ibid. p. 27

aggression despite the court's findings of a "grave violation of the prohibition of the use of force expressed in Article 2/4 of the Charter, due to its magnitude and duration."[311]

On the other hand, the concept of aggression is regulated by the Rome Statute of the ICC that was established by an international treaty in 2002 as the only permanent court responsible for the pursuit of individual responsibility for fundamental crimes under International criminal law. It has been noted that the crime of aggression means: "the planning, preparation, initiation or execution, by a person in a position effectively to exercise control over or to direct the political or military action of a state, of an act of aggression which by its character, gravity, and scale, constitutes a manifest violation of the Charter of the United Nations."[312] Therefore, the crime of aggression as defined in Article 8 bis, must be committed by a person in a position to direct or control the actions of the state or military. It is also understood that the provision of this article shall apply only to persons in a position effectively to exercise control over or to direct the political or military action of a state[313]. The definition of aggression set in Article 8bis and conditions for the exercise of the ICC jurisdiction (Article 15 bis and 15 ter) was adopted at the Kampala Review Conference on the Rome Statute in June 2010[314], it observed that the purpose of this paragraph is to clarify that the leadership requirement discussed under Article 8 bis (1), applies also when making assessments under Article 25(3)[315]. Nevertheless, ICC's interpretation of the "act of aggression" for Article 8 bis differs from the application of the aggression by the Security Council under Article 39 of the UN Charter. Yet both interpretations are related to states, either by the concept of aggression of unlawful use of force by a state (GAR 1974) or the concept of crimes committed by individuals against the sovereignty of a state (Article 8 bis Rome Statute), by which the criminalization of the unlawful use of force is structurally linked to the use of force by a state. Also, with regards to the Effective control (Article 8 bis/1), it limits the individual liability to the exclusion of individuals who merely influenced policy and highlights the difficulty of extending the crime of aggression to forms of organizations represented by paramilitary or terrorist NSAs.[316]

---

[311] ICJ, DRC v. Uganda, Ibid., at para. 165. In their separate opinions, Judges Elabary, at paras. 9 – 20 and Simma, at para. 3, have criticized the Court for having avoided a finding of aggression.
[312] Rome Statute of the International Criminal Court 1998, United Nations, Treaty Series, vol. 2187, Article 8 bis/1.
[313] Rome Statute, Ibid,, art. 25(3) bis.
[314] Bachmann Sascha-Dominik and Kemp G., Aggression as Organized Hypocrisy? – How the War on Terrorism and Hybrid Threats Challenge the Nuremberg Legacy, Windsor Y B Access Just 32012, p.247
[315] See for e.g., Aronsson-Storrier M., Article 25(3) bis. Commentary on the Law of the International Criminal Court, Case Matrix Network June 30, 2016.
[316] Ambos K., The Crime of Aggression after Kampala, German Yearbook of International Law, vol. 53, p. 492.

Further, the threshold provides a distinction between the crime of aggression for which individuals bear responsibility on the one hand and an act of aggression by a state within the meaning of Article 39 of the UN Charter[317]. This can be seen in both the quantitative dimension of "scale and gravity" ensuring that only very serious unlawful uses of force by states are covered by the definition, and qualitative of the "character" to exclude instances of the use of force that falls in a gray legal area. In the same manner, the act of aggression in the context of Article 42(7) UN Charter, equates the armed attack in the context of Article 51, and it could be seen that the phrase armed aggression echoes the French language version of Article 51 which used the words "agression armée" in place of an armed attack.

To conclude, the threshold requirement under the Rome Statute is considerably narrower than the concept of the act of aggression in Article 39 of the UN Charter. Nonetheless, taking into consideration that contemporary conflicts are not state-centric and that NSAs (armed groups and corporations[318]) are increasingly entangled in armed conflicts globally, the limited nature of liability for the crime of aggression is regrettably inadequate. "Article 8 bis" suffers from several shortcomings that did not take into consideration the modern realities of warfare. First NSAs such as ISIS, Al Qaeda, Boko Haram that are not attributed or fight on behalf of any state, could find impunity for their actions, as the definition of the act of aggression is only relevant for actions of States which is a reflection to GAR 3314 (XXIX) of 1974.[319] Yet it is concluded that any criticism of international law scholars and experts with regards to the rise of two different definitions or interpretations of aggression in international law[320] should not be worrying, as Article 10 of the Statute affirms that no interpretations shall limit in any way the existing or developing rules of international law for purposes other than this statute.

[317] ILA Report 2018, Ibid. p. 28.

[318] Corporations that play a vital role in weapons manufacturing, private security contractors and general corporate action in conflict zones, act independently or in partnership with states in contemporary conflicts. According to Mireille Delmas-Marty, "The relationship between mass atrocities and economic activities was already a live issue at Nuremberg . . . Corporate criminal involvement in international crimes did not end with the Second World War. To the contrary, new developments in the available means of communication in a globalized and more interconnected world create new opportunities, particularly as some transnational corporations wield greater economic power than some states. These corporations have become major players, which have complex relationships with national governments and the local population…. throughout the world corporations are involved in the commission of serious crimes, either directly or as part of a larger group." See, Delmas-Marty M., Ambiguities and Lacunae, The International Criminal Court Ten Years on, Journal of International Criminal Justice, 2013, vol.11, p. 553

[319] Rome Statute, Ibid. Article 8 bis (2) para g.

[320] See comments in the ILA Report 2018, Ibid. p 28-29. (emphasis) "There are concerns about the newer ICC definition eclipsing the wider jus ad bellum definition. On the other hand, some suggest that the prohibition of the use of force will not be weakened and that the amendment to the ICC statute may in practice have a stronger deterrent effect on individuals who direct the affairs of governments."

Therefore, the ICC statute is relevant only to the crime over which ICC will have jurisdiction and by that, it has no impact on the meaning of the act of aggression under Article 39 UN Charter, nor on the prohibition of the use of force under Article 2(4) and customary international law.

- **The Legal Basis of Act of Aggression concerning Cyber Operations**

The definition of aggression was passed by the UN in 1974, at time where cyber-attacks and the role of NSAs in cyberspace were not yet significant threats in international relations compared to their readiness in contemporary conflicts. The definition of aggression expressed in the language of Resolution 3314 has two perspectives. The first considers some acts of aggression are prima facie by the simple use of force in a conflict based on a comparison with previous actions that took place. The second has a more materialistic definition of aggression, such as acts of invasion, bombardment, or blockade.[321]

It is seen that the activities that developed after the resolution, mainly cyber-attacks were not addressed directly in the resolution but concluded that such activities must be equated to physical attacks to understand their impact.[322] This perspective has been reflected in the Tallinn Manual that defined cyber attacks as "cyber operations, both offensive and defensive, which can reasonably cause injury or death to persons or damage or destruction of objects."[323] Cyber-attacks fit in the list of activities provided by Article 3 of the 3314 resolution that can qualify as an act of aggression. For example, such attacks can be employed to target another state through a digital blockade of goods moving out of a port, or even attack the military infrastructure or personnel. Cyber forces can constitute a type of irregular force conducting an attack with effects similar to a conventional force[324], by which the assimilation of some cyber-attacks with armed force allows the UNSC to act under Chapter VII and for States to react in self-defense.[325] But certain features of cyber operations may fall below the resolution's requirement and might allow states to avoid any direct attribution in cyber aggression.

[321] Resolution 3314, Ibid.
[322] Hogan J., The Future of War: Cyber-Attacks and Aggression in International Law, Portland State University 2019, p. 11-12.
[323] Tallinn Manual 2.0, Ibid., Rule 92
[324]Mendoza J., Cyber Attacks and the Legal Justification for an Armed Response, School of Advanced Military Studies, Kansas 2017, p. 18.
[325] Greco G., Cyber-Attacks as Aggression Crimes in Cyberspace in the context of International Criminal Law, European Journal of political Science Studies, 2020, Vol. 4, Issue 1, p. 42

According to Nils Melzer, the prohibition on the use of force in interstate relation cannot be circumvented by the application of non-violent means and methods that has the same impact on international peace and security.[326] One of the examples is the attacks that targeted Estonia that may have shed the light on the potential inadequacy of the current legal definition of aggression concerning cyber warfare. The discussion of what constitutes an armed attack and whether tools of HW and if there is consensus on its threshold will be discussed in the upcoming section. However, the study will briefly come across the cyber-attack against Estonia in 2007 and comment on whether the definition of aggression was legally sufficient.

In this regard, following the Estonian government decision in 2007 to move the Bronze Soldier (also known as the Monument to the Liberators of Tallinn) from the center of Tallinn, outrage from the Russian speakers have erupted because the monument represents to them the USSR's victory over Nazism, while for many Estonians it represents a painful symbol of Soviet oppression. In the aftermath of the incident, Estonia faced a series of DDOS cyber-attacks on banks, government institutions, media outlets, and telecommunication services. As a result, citizens were not able to use cash machines and online banking services, government employees were blocked from the ability to communicate by email, and newspapers were not able to deliver the news. According to Liisa Past, a cyber-defense expert at Estonia's State Information System Authority, cyber aggression is different than kinetic warfare, as it allows to create confusion while staying well below the level of an armed attack.[327] In an attempt to trace the attack, Estonia has considered that it traced back the attacks to Russian IP addresses with no concrete evidence that these attacks were carried out by the Russian government, that in turn denied any involvement and suggesting that the attack was launched by private pro-Russian activists.[328] The incident demonstrated again that attribution may be the primary factor limiting the legal justification for armed response. However, analyzing the attack in the context of Resolution 3314, it can be noted that the requirement of armed invasion, bombardment, or physical damage to the infrastructure was not met. While other requirements such as border crossing or allowing the territory of a state to be used for launching attacks on another state are hardly identified due to the technical complexity and nature of cyber-attacks that can create a

[326] Melzer N., Cyber Warfare and International Law, United Nations Institute for Disarmament Research, 2011, p. 8.
[327] McGuinness D., How a Cyber-attack transformed Estonia, 22 April 2017. https://www.bbc.com/news/39655415
[328] Crandall M., Soft Security Threat and Small States: The case of Estonia, Defense Studies Vol. 14, No. 1, 2014, p. 36.

legal gray area. Respectively, some scholars argue that with no evidence of physical damage or injury and death of persons, such attacks are not considered an act of aggression, while it can violate the concept of Friendly relations articulated under resolution 2625. But the fact that cyber-attacks or the employment of NSAs to mask the operations might not meet the definition of aggression, a gap in international law will be a resort for states and NSAs to conduct further attacks of this nature. However, the study instructs an immediate international effort to restructure the definition of aggression to fit the new technologies and hybrid adversaries, that are mainly NSAs. Finally, a state that is the victim of aggression has the right to self-defense. Acts committed in the exercise of the right to self-determination of peoples, or when peoples are fighting against colonial domination, foreign occupation, or racist regimes are not acts of aggression.[329] Since the traditional understanding of aggression triggered by conventional war is clear-cut military aggression, states waging HW pursue activities that are amenable to non-involvement, non-detection, non-attribution, and plausible denial of responsibility.

Based on the above analysis, it is important to note that the core challenge by HW to the prohibition on the use of force is the ambiguity that it is tailored to make a military response difficult to avoid conventional confrontation by operating below the thresholds of the opponents. Such forms can be achieved by hiding and denying agency through the use of proxies, non-attributable forces, and cyber-attacks. Moreover, various means of HW that do not amount to an armed attack or use of force in its physical form, are crucial to the adversary to achieve the political and strategical outcome or even military objectives. This can be seen in disinformation campaigns that play an important role in the escalation and de-escalation of a situation. On the other hand, it is agreed that cyber-attacks that cause injury or death of persons, even damage or destruction of property violate the prohibition to use force in international relations[330]. Yet cyber operations of NSAs do not violate this prohibition unless they are attributable to a state, by which responding rests with the state rather than on the hybrid actor in question, while cyber operations conducted by states against NSAs may implicate the prohibition as the problem of attribution in such case is beyond questioning[331].

[329] Pietro Verri, Dictionary of The International Law of Armed Conflict, International Committee of the Red Cross, Geneva 1992
[330] Tallinn Manual, para. 8 of commentary to Rule 11.
[331] Schmitt M. and Watts S., Beyond State-Centrism: International Law and Non-state Actors in Cyberspace, journal of Conflict and Security law Published by Oxford University Press 2016, p. 607

Nevertheless, according to Tallinn Manual, certain operations which do not have destructive or injurious consequences would qualify as a use of force[332], mainly due to the applicability of international law, including the principles of state sovereignty, sovereign equality, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States, to cyberspace. Rule 1 of the Tallinn Manual stated that "the sovereignty empowers a state to exercise control over cyberinfrastructure and activities within its territory, and in protecting the cyberinfrastructure at its territory from any attacks."[333] Yet, this principle covers the territory, not the object targeted, so if the computer of a state is targeted on the territory of another state, then the sovereignty of the state where the computer is located will be breached[334]. At the same time, the principle of non-intervention can be violated with any cyber support to groups in other states, such as supplying malware to them by which such acts would qualify as intervention by the sponsoring state.

On the other hand, legal ambiguity that is an inherent feature of every legal system is also considered a core challenge and an opportunity for states and NSAs at the same time. The reason for such uncertainties in law is that the interpretation relies on the political decisions and choices, and as legal texts are often obscure, the competence may be ill-defined, and evolving incidents might not be foreseen by legislators[335]. Similarly, the ambiguity of law has some benefits or deterrence factor such as the threshold that trigger collective self-defense arrangements as found in Article 5 of the North Atlantic Treaty that may cause adversaries to act more carefully[336]

However, such grey areas give hostile actors opportunities to advance their strategic interests by which states may rely on the interplay of legal boundaries to mitigate the impact that international norms may have on their domestic law[337]. The Chinese authorities, for example, have used the law to avoid minor or incremental infractions of the rules such as the Air Defense

---

[332] Ibid., para. 10 of commentary to Rule 11.
[333] Michael Schmitt & Liis Vihul, Ibid, p.60.
[334] Ibid
[335] Sari A., Hybrid Threats and the Law: Concepts, Trends and Implications, Hybrid CoE Trend Report 3, April 2020, p. 17.
[336] Ministry of Defence, Deterrence: The Defence Contribution, JDN 1/19, Development, Concepts and Doctrine Centre, Shrivenham 2019, p. 47.
[337] For example, The Russian government have initiated criminal proceedings against Lithuanian prosecutors, investigators and Judges as an act of retaliation in response to the trial of former Soviet officers and officials on charges of war crimes and crimes against humanity during the transition of Lithuania's independence. Russian by this may misuse the INTERPOL system to seek the international arrest of the Lithuanian prosecutors and judges. See, European Parliament Resolution of 28 November 2019 on recent actions by the Russian Federation against Lithuanian Judges, Prosecutors and Investigators involved in investigating the Tragic events of 13 January 1991 in Vilnius, Doc. 2019/2938 (RSP).

Identification Zone (ADIZ) over the East China Sea established in 2013, by which China relied on the state's right to regulate the entry of aircraft engaged in international air navigation into its territory[338]. However, the ADIZ does not differentiate between aircraft entering the Chinese territory from those that are not, which means that China is capable of using force to interdict any aircraft that does not comply with its enforced rules. China has announced that "Aircraft flying in the East China Sea Air Defense Identification Zone should follow the instructions of the administrative organ ADIZ or the unit authorized by the organ. China's armed forces will adopt defensive emergency measures to respond to aircraft that do not cooperate in the identification or refuse to follow the instructions." [339] The previous statement reflects the lawfare element as a potential hybrid threat used by hostile actors to pursue strategic objectives through legal means and in the legal domain.

The right of individual and collective self-defense applies irrespective of the type of weapon used to conduct an armed attack, what matters is the scale and effect of such attack. Therefore, a hybrid attack that employs a combination of military and non-military instruments triggers the right to self-defense, provided that its scale and effects are comparable to a conventionally armed attack. The hybrid character of HW seeks to achieve objectives through non-military means too, such as the Chinese coast guards and fishing vessels in the South China Sea, by which the Assembly failed to solve the legal complexities of such tactics.[340] Yet, some states, such as Finland, have domestically amended the Territorial Surveillance Act which serves as the legal framework for safeguarding Finland's territorial integrity[341]. The resolution calls on member states to refrain from resorting to hybrid war in international relations and fully respect the provision of international law, particularly the principles of sovereignty, territorial integrity,

[338] Petras Ch., The Law of Air Mobility- The International Legal Principles behind the U.S Mobility Air Forces, Air Force Law Review, 2010, p. 63-64. See also, Convention on International Civil Aviation, Article 11, December 1944, 15 UNTS 295.

[339] Announcement of the Aircraft Identification Rules for the East China Sea Air Defense Identification Zone of the People's Republic of China, 13 November 2013. https://www.chinadaily.com.cn/china/2013-11/23/content_17126618.htm

[340] Sari A., The Council of Europe's Parliamentary Assembly takes on the Legal Challenges of Hybrid Warfare, Lawfare Blog May 2018.

[341] Territorial Surveillance Act of 18.8.2000, Amendment Section 2 5(a), 10.7.2017/502, An earlier version of the act required the Finnish armed forces and border guard to take appropriate steps against unauthorized intrusions by foreign military personnel, units, vehicles, aircrafts and vessels. Section 2 of the law defined foreign "military persons" as armed or unarmed members of national armed forces. In 2017, the law was amended to cover groups that are militarily organized, equipped or armed, and comparable to forces operating on behalf of, for or with the consent of a foreign state, but whose national origin cannot be identified. As a result, the Finnish military authorities are now empowered to take appropriate action against armed formations not wearing regular military uniform or other symbols of nationality. See, Sari A. The Council of Europe's Parliamentary Assembly takes on the Legal Challenges of Hybrid Warfare Ibid.

and inviolability of frontiers, per their object and purpose, by not abusively exploiting perceived loopholes or ambiguities[342].

To illustrate, it is with no doubt that ambiguity is the main characteristic of HW. In the Ukrainian conflict in 2014, both Ukraine and the international community could not understand the real situation because proxy fighters created hesitation for decision-makers that helped Russia to gain the time needed to accomplish its task[343]. The uncertainties of contemporary conflicts and the covert intervention by states against the territorial integrity and independence of other states is a violation of Article 2(4) of the UN Charter on the prohibition of the use of force regardless of the objective pursued by it (protection of nationals, humanitarian intervention). Also, the UNSC was shattered because of the international nature of the conflict, especially since the veto of one of the two world powers in the council's vote lead to ineffective measures of collective security[344]. Therefore, the debate on the prohibition of the use of force and its efficiency has been vital for contemporary threats and the use of force. And for the interest of the current research, the analysis will cover the use of force as self-defense especially against NSAs in the territory of another state (unable or unwilling to counter the threat), also in the territory of the targeted state by NSAs that either attributed to a state or not. And that is with no doubt a challenge for a state if such actions would trigger a non-international armed conflict or a case for law enforcement to deal with. That requires a deep analysis of attribution and state responsibility to such actions too especially in the cyber realm where verifiable attribution is difficult because HW employs instruments across multiple domains that allows a state to stay below both the radar of detection and the threshold for responding under international law.

2. Exceptions to the Prohibition of the Use of Force

While it was explained that Article 2(4) of the UN Charter prohibits the resort to the use or threat of force, one exception to this prohibition is an action taken in self-defense under Article 51 of the UN Charter that primarily visualizes the immediate response, individual or collective, of a state which is the victim of an armed attack. Another exception is under the auspices of a UNSC authorization to use force under Article 42 of the UN Charter that envisages institutional collective security response to the use of force against a state in violation of international peace

[342] Ibid. sec. A. para.10.1
[343] Turkgenci Y., and Sayatt H., "Command and Control", Shifting Paradigm of War: Hybrid Warfare, Turkish National Defense University, Istanbul 2017, p.72
[344] Kress C., On the Principle of Non-Use of Force in Current International Law, Just Security at Reiss Center on Law and Security, New York September 2019.

and security. In addition, States can also give consent to another state to use force in its territory to combat rebel or terrorist actors. Nonetheless, debates are also surrounding the shift in a legal landscape that expands the right to use force by taking measures of self-defense to protect nationals abroad (Russia's operation in Georgia 2008) that is sometimes wrongly referred to as diplomatic protection. under the Draft Articles on Diplomatic Protection 2006 such protection consists of the invocation by a State through diplomatic action or other means of peaceful settlement, so it does not include any actions through military means[345]. In addition, the right to humanitarian interventions (Kosovo Crisis 1999) that has developed significantly and sometimes even classified as the third exception to non-use of force in international relations, especially that the international community proved itself more willing to collectively intervene in other states on humanitarian grounds, or in self-defense against NSAs in the territory of another state.

The law relating to the use of force as a right to self-defense has been a matter of discussion due to the controversial issues relating to its permissibility against NSAs, particularly in the rise of Hybrid means to contemporary conflicts. The increase of inter-state conflicts and the rise of NSAs with access to progressed technologies emphasized the emerging state practice in favor of expanding the authorization of force outside the Charter system. This includes evolving doctrinal deviations such as the "unwilling or unable" test. UN Charter Article 51 provides the trigger for the exercise of the right of self-defense, as in international law is the state's inherent right to use force to protect itself from an armed attack[346]. Given the complicated nature of the topic, it is hard to distinguish between the use of force and armed attack, which creates a gap between Article 2(4) and Article 51 of the UN Charter, especially since all armed attacks are the use of force, but not all uses of force amount to an armed attack[347]. Yoram Dinstein argues that the gap is ought to be quite narrow, and he states that: "Any use of force causing human casualties or serious damage to property constitutes an armed attack."[348] Nonetheless, an armed attack means any use of armed force and does not need to cross some threshold of intensity. Also, although the ICJ has stated that some uses of force

[345] Draft Articles on Diplomatic Protection 2006, Part 1, Article 1, Adopted by the International Law Commission at its 58th session, 2006.
[346] The right of self-defense is a legal notion that has been widely analyzed by relevant legal doctrine and scholars, it has been accepted that the concept is of a customary and treaty norm. See, D.W. Bowett, Self Defense in International Law 1958; J. Zourek, La Notion de Legitime Defense en Droit International 1975; Y. Dinstein, War, Aggression, and Self-defense 2005; J. Green, The International Court of Justice and Self-defense in International Law 2009.
[347] Dinstein Y., Computer Network Attacks and Self-Defense, 2002, p. 163.
[348] Kretzmer D., The Inherent Right to Self-Defense and Proportionality in Jus Ad Bellum, Ibid. p. 243

may not be of sufficient gravity to constitute an armed attack, it is argued that this view has not been generally accepted[349]. The term "force" in Article 2 of the UN Charter is not only confined to the armed force, whereas the notion of armed attack necessarily requires resort to arms, as the general tendency in state practice, embodied in the Friendly Relations Declaration, is to limit its meaning to the military use of force.

The traditional customary law governing self-defense by a state derives from an early diplomatic incident between the USA and the UK over the killing of several US citizens engaged in transporting men and materials from American territory to support rebels in what was then the British colony of Canada[350]. Self-defense is a natural law concept and states have different definitions of how broad this right is, but it is mainly based on direct threat and scopes. Article 51 of the UN Charter states that: "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 UN until the Security Council has taken the measures necessary to maintain international peace and security", the article reflects the customary right of self-defense. [351]

For the present section, the exceptions to the use of force in international relations will include the authorization within the UN Charter (Self-defense and UNSC authorization), and authorizations of force outside the Charter system (Humanitarian interventions, unable or unwilling test). The importance of addressing these issues in the context of HW is highly relevant and important as it will include the challenging elements of HW such as the NSAs and Cyber operations and the impact of these means on the adequacy of the exceptions to the non-use of force norm. That will require highlighting when can a state use force in self-defense, what is the threshold and elements of an armed attack, principles of necessity and proportionality, self-defense against NSA in the territory of another state, also whether Humanitarian intervention and Responsibility to protect have become the new exceptions to the prohibition on the use of force in Article 2(4) of the UN Charter.

2.1. Authorization by the UN Security Council

Generally, the Security Council is authorized to determine the existence of and take necessary action to address any threat to international peace and security as lawful use of force under

[349] Chatham house Principles of International Law on Use of Force is Self-Defense, February 2011.
[350] Clapham A., Brierly's Law of Nations, 7th ed., Oxford University Press, Oxford, 2008, pp. 468–469.
[351] Tallinn Manual, Ibid., Rule 13, p. 54.

international law in the form of genuine world police action. Article 24 of the UN Charter affirms that as an organ of the UN, it is the SC that has the primary responsibility of maintaining international peace, security, and stability. The UNSC plays a major role in global collective security. Article 39 in Chapter VII of the Charter explains when the SC can begin to handle the situation and address it in three scenarios: Threat to the peace, breach of the peace, and acts of aggression[352].

The SC has the upper hand through which the General Assembly (UNGA) cannot take measures that are binding on States or make recommendations on disputes when the SC is discussing it according to article 12 of the UN Charter. So the SC may itself use force under Articles 39 and 42 of Chapter VII, by calling on member states, including regional organizations such as the Organization of American States (OAS), NATO, or Organization of African Unity (OAU) to provide needed military forces.[353] Threat to the peace is not defined anywhere, therefore, it is left to the SC to decide and remedy the situation based on its interpretation, by either non-forceful measures that are articulated in article 41 of the UN Charter[354], or by deploying UN troops against violators of the peace when the SC decided that the non-forceful measures have been/would be inadequate (forceful measures without the consent of the state targeted).[355] Nonetheless, the SC has identified potential or generic threats such as terrorist acts (counter-terrorism Committee guided by the UNSCR 1373 of 2001 and 1646 of 2005), the proliferation of weapons of mass destruction, and the proliferation and illicit trafficking of small arms or light weapons (non-proliferation committee guided by UNSCR 1540 of 2004) under Chapter VII of the UN Charter).

In addition, Article 41 of the Charter, gives the SC the authority to impose measures not involving the use of armed force. These sanctions are tools to apply pressure on a State or entity

---

[352] UN Charter, Chapter VII "Actions with respect to Threats to the Peace, Breaches of the Peace and Acts of Aggression", Article 39 states the following: The Security Council shall determine the existence of any threat to the peace, breach of the peace, or act of aggression and shall make recommendations, or decide what measures shall be taken in accordance with Article 41 and 42, to maintain or restore International peace and security."

[353] Under Article 43, the UN Charter contemplated agreements between the SC and members governing the disposition and use of member forces, but since no agreements have been concluded, member forces have been provided on a voluntary basis. See, Bowet D., International Military Force, Encyclopedia of Public International Law , 1995, p. 1267.

[354] UN Charter, Ibid. Article 41 states that: "The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon Members of the UN to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations."

[355] Ibid., Article 42 states that: "Should the Security Council consider that measures provided for in Article 41 would be inadequate, it may take such actions by air, sea, or land forces as may be necessary to maintain or restore international peace and security. Such actions may include demonstrations, blockade, and other operations by air, sea, or land forces of Members of the United Nations."

to comply with the objectives set by the SC without resorting to the use of force. The range of sanctions has included comprehensive economic and trade sanctions, and more targeted measures such as arms embargoes, travel bans, financial or diplomatic restrictions. These enforcement actions fall short of the use of force and have been acknowledged not to be within the monopoly power of the SC, by which such non-force measures may be imposed unilaterally or collectively by states without SC authorization.[356]

The role of the UNSC was not always effective as the Council has been a captive of the East-West conflict for decades. Although some cases such as, the intervention against Saddam Hussein in 1990, which is known as the first Gulf war, was effective by which the UNSCR 660 in August 1990, stated that "The Security Council determining there is a breach of the peace by the Iraqi invasion of Kuwait", that was followed by UNSCR 678 (29/11/90) that authorized member states cooperating with Kuwait unless Iraq, on or before January 1991, fully implements the foregoing resolutions to use all necessary means to uphold and implement (SC Res. 660) and all subsequent relevant resolutions and to restore international peace and security[357]. Furthermore, UNSC's has a role to authorize the use of force when it comes to protecting a civilian population that has been a victim of genocide, crimes against humanity, and the systemic commission of war crimes in cases where the national government does not fulfill its responsibilities or is itself behind the attacks[358]. Although the state itself is responsible for protecting its people, however, the UN codification of the Responsibility to Protect (R2P) granted the UNSC exclusive control over authorizing the use of force in sovereign states[359]. That will be addressed in further detail when discussing Humanitarian intervention (subsection 2.4).

2.2. The "Trigger" for the Inherent Right of State Self-Defense

The right to individual and collective self-defense is recognized as an exception to the prohibition of the use of force outside the framework of collective security and nothing in state practice has justified use of force due to the state of necessity or right to reprisals, can be

[356] Hickey J., Challenges to Security Council Monopoly Power over the Use of Force in Enforcement Actions: The Case of Regional Organizations, 10 Ius Gentium, 2004, Vol. 75, p. 87-88.
[357] UNSCR 678, Iraq-Kuwait of 29 November 1990.
[358] Kress C., Ibid.
[359] Report of the International Community on Intervention and State Soverignty, transmitted by Letter Dated 26 July 2002 from the Permanent Representative of Canada to the UN addressed to the Secretary General, The Responsibility to Protect, at 49, UN Doc. A/57/303 (2001).

identified today as it used to be prior the UN Charter 1945[360]. Nonetheless, the UN Charter does not explicitly define what does Article 51 include and especially in the context of armed attack and inherent right, yet it is accepted that exercise of the right to self-defense must meet the demands of immediacy, necessity, and proportionality.[361] This article is an exception to article 2(4) which prohibits the use of force, so a state can use force without violating the prohibition when it is a victim of an armed attack that does not require any authorization from SC.

To begin with the question of what might constitute an armed attack, the ICJ in the Nicaragua case stated that the definition of an armed attack must be interpreted with guidance from the definition of aggression[362]. So it applied the definition as a basis for determining what may constitute the threat or use of force and armed attacks, by which several conditions must be met for the use of force in self-defense to be legal, such as the state acting in self-defense must have been the victim of an armed attack, must have declared itself to have been attacked, and must have requested the assistance of the states which come to its aid. Similarly, the ICJ in its 1996 Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons stated that the court cannot lose sight of the fundamental right of every state to survival, and thus its right to resort to self-defense, under article 51 of the Charter, when its survival is at stake only in an extreme circumstance of self-defense.[363] However, the catastrophic scenario of nuclear threats beyond any doubt triggers the right to self-defense.

Challenges arise if such operations generate consequences crossing the armed attack threshold, then the state may find itself the target of forceful cyber or kinetic responses under the law of individual or collective self-defense. According to the ICJ, identifying an armed attack is a question of gravity, by which the 1986 Nicaragua case asserted that the difference between armed attacks and less grave forms of the use of force was one of scale and effects, such as the assistance to rebels in the form of the provision of weapons or logistical or other support. Such actions amount to threat or use of force, or intervention in the internal or external affairs of other states (principle of non-intervention), but does not qualify to an armed attack or armed force[364], and that the armed attack must in itself be contrary to Article 2(4) of the UN Charter. Therefore, it highlights the relationship between the notion of armed attack and the principle

[360] Ibid.
[361] Dinstein, Y., War, Aggression and Self-Defense, Cambridge University Press 2014, 3rd ed. p. 184
[362] General Assembly, 1974, Definition of Aggression, Article 3 (a-g), para 195-199, and 232-233.
[363] ICJ, Legality of the Threat or Use of Nuclear Weapons Advisory Opinion, Reports 1996, para.96-97.
[364] ICJ., Nicaragua vs USA, Ibid., para. 195.

of non-intervention, by which all armed attacks amount to both uses of force and interventions, but not all interventions amount to an armed attack[365]. Yet, where exactly this threshold lies, is the subject of continuing debate, but it is seen to be met when the use of force involves the loss of life or the physical destruction of objects[366]. There is a lack of consensus on whether the force has to meet a threshold of intensity or not. However, the court in the Nicaragua case outlined the nature of the acts which could be treated as an armed attack, by which an armed attack must be understood as including not merely action by regular armed forces across an international border, but also the sending by or on behalf of a state of armed bands, groups, irregulars or mercenaries, which carry out acts of armed force against another State of such gravity as to amount to (inter alia) an actual armed attack conducted by regular forces.

In customary law, the prohibition of armed attacks may apply to the 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 a mere frontier incident had it been carried out by regular armed forces. But the Court does not believe that the concept of armed attack includes not only acts by armed bands where such acts occur on a significant scale but also assistance to rebels in the form of the provision of weapons or logistical or other support.[367] The court's restrictive approach did not consider that actions of assisting irregulars or armed bands in the form of logistical or other support may amount to an armed attack[368]. The court was criticized for excluding mere frontier incidents that involve lethal force and may give rise to the right of self-defense. For instance, in 2006 Israel launched a military campaign against Hezbollah in South Lebanon justifying its inherent right to self-defense due to border incidents. Several states expressed concerns over the proportionality and the nature of Israel's response, yet they agreed that the gravity of the attack is an essential factor in assessing the necessity and proportionality of a forcible response[369]. Israel has argued that the use of force in response to cross-border attacks relied on the accumulation of events theory, by which Israel's permanent representative to the UNSC relied specifically on the right of its country to self-defense under Art. 51 of the Charter in response to the fact that Israeli citizens were subject to deliberate terrorist attacks[370]. This theory deals with low-scale attacks targeting a state and

---

[365] Bou Nader Ph., Ibid. p. 18

[366] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Edited by Schmitt M., 2nd ed., 2017, rule 71, p. 341

[367] ICJ., Nicaragua vs. USA., Ibid. para. 195.

[368] J. Green, The International Court of Justice and Self-defense in International Law, Oregon 2009

[369] ILA Report 2018, Ibid. p. 6. See also different views on this matter, Gray C., International Law and the Use of Force, Oxford University Press 4th ed. Oxford 2018, pp. 177-183

[370] Ronen, Y., "Israel, Hezbollah, and the Second Lebanon War", Yearbook of International Humanitarian Law, vol. 9, 2006, p. 362-372

whether the victim state may defend itself not only against the use of force that triggered a forcible response in self-defense but against the threat arising from accumulative series of events. The accumulation theory did not receive support from the UNSC and it certainly creates more challenges to the justification of the use of force based on the state interpretation of a conflict or threat. Yet, in current state practices, the theory is receiving more acceptance than in past.[371]

The key issue that will be highlighted is what constitutes an armed attack, due to the indistinctness of different terms used in the above documents (armed aggression, use of force, non-intervention). In this matter, the reason for the use of different terms is the international community's intention to distinguish between the "first shot" and the "armed attack" itself.[372] This plays an important role in the contemporary conflicts, particularly in the annexation of Crimea, by which the distinguishing factor between the state of "first shot" and the "aggressor" is vital in cases where a state conducts a campaign to control a territory of another state without the occurrence of an armed fight, by which the targeted state that lost part of its territory, will be under obligation to use armed force (as a first shot) against the aggressor triggering its right to self-defense. In that case, the state that controlled the territory of another state would not be the first to shoot, but it would be the aggressor since it committed the armed attack[373]. It can be concluded that Article 2(4) of the UN Charter prohibits the use of force, which could be excluded if force took the form of armed aggression triggering Article 51 of self-defense. Nevertheless, Hybrid adversaries (e.g. the case of Ukraine and Russia) tend to employ hybrid strategies that are the fact-paced passage from the mere use of force to actual aggression, to suddenly de-escalate the conflict to mere diplomatic and economic pressure. This was seen in the context of incidents that started from the involvement of mercenaries in Eastern Ukraine covertly to the annexation of Crimea overtly, and then the confrontation between Ukraine and Russia in the Azov Sea incident, which was considered by Ukraine as armed aggression by Russia.

Similarly, the ongoing tension between the USA and Iran in the Middle East, by which Iran has heavily invested in expanding its influence in the region through proxy militias (Popular Mobilizations Forces "PMF") that have established the means to survive in the absence of

---

[371] Tams, Ch., "The Use of Force against Terrorists", European journal of International Law EJIL 2009, supra-note 49, p. 388. Christian Tams argues that: "States seem to have shown a new willingness to accept the accumulation of events doctrine which previously had received little support"

[372] Dinstein y., War, Aggression and Self-Defense, 4th ed. Cambridge 2005.

[373] Bou-Nader Ph., Ibid. p.16

effective and trusted formal governance in Iraq and Syria, to avoid any legal attribution and direct responsibility. However, the situation has legally escalated after the assassination of Qassim Soleimani in Iraq (the most prominent military leader figure in Iran and close to the supreme leader Ayatollah Ali Khamenei) that converted the conflict from indirect low-intensity conflict to a confrontation between the two states. The US relied on legal justifications for its actions and to denounce Iran, in which it justified the killing of Soleimani as an exercise of the inherent right to self-defense in response to an escalating series of armed attacks by the Islamic Republic of Iran and its affiliates on US forces in the region[374]. On the other hand, Iran has used the same justification to target US military facilities as a response to the targeting of Soleimani, so the legality of one party's reaction hinges on the illegality of the other party's prior conduct, based on the principle that the right of self-defense is available in response to an unlawful armed attack[375]. Therefore, that highlights the importance of identifying the elements of an armed attack that would trigger a response in self-defense as an exception to the nonuse of force principle.

2.2.1. The Elements of an Armed Attack

Based on the analysis of the previous section, the right to use force in international law is allowed once a state is a victim of an armed attack. Therefore, it has been noticed that three elements are vital to consider whether the act committed is an armed attack. These elements can be summarized as follow:

- **Ratione Materie (Material Element)**

An element that highlights the material aspect of an armed attack by taking into account the following: an act that qualifies as an armed attack according to international law, the gravity of the acts, if such acts must be taken in isolation or aggregated as per the accumulation of events theory, and intent of the aggressor state. This has been reflected in article 3 of the GA Res 3314 (XXIX) on the definition of aggression, and confirmed later by the ICJ (Congo v. Uganda case) considering that the resolution will serve as an authority on the future determination of acts of aggression that constitute an armed attack.[376] While the gravity of the

[374] Letter dated 8 January 2020 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, 9 January 2020, S/2020/20.
[375] Sari A., Hybrid Threats and the Law: Concepts, Trends and Implications, Ibid., p. 12.
[376] ICJ, Congo v Uganda, Ibid. para 146. See also, Legal Consequences of the construction of the wall case, Ibid., para 139.

acts committed is distinguished between the most grave "armed attack" and the less grave act of aggression based on the severity of the act and its effect and damage on the victim state. [377] According to Dinstein, the gravity of the attack is predicated by the consequences that are liable to be produced by the attack rather than the actual casualties inflicted. Therefore, even small-scale attacks can reach the gravity of armed attacks if they would result in or can destroy property or loss of lives.[378]

Another importantly observed argument that had been noticed in opinio Juris is the accumulation of events theory, suggesting that if an act is not of sufficient gravity to qualify an armed attack, but at the same time is part of a series of acts of force directed against a victim state, then the effects caused by the separate incidents in accumulation can reach the gravity threshold of an armed attack. This theory is also known as the "Needle Prick" doctrine, promoted by Israel to justify its campaign against the Palestinian Liberation Organization (PLO) in Lebanon, considers that "each specific act of terrorism or needle prick, may not qualify as an armed attack that entitles the victim state to respond legitimately with armed force. But the totality of the incidents may demonstrate a systematic campaign of minor terrorist activities that do rise to the intolerable level of armed attack."[379] Although Israel's justification was rejected by the UNSC, however, some scholars have considered that this rejection was not addressed to the theory itself but was based upon a disproportionate use of force by Israel in retaliation of the attacks.[380] Similarly, the ICJ has not dismissed or rejected the accumulation theory, rather considered it indirectly in the Nicaragua case when considering if border attacks by Nicaragua into Honduras and Costa Rica could amount to an armed attack and stated that: "very little information is available to the Court as to the circumstances of these incursions or their possible motivations, which renders it difficult to decide whether they may be treated for legal purposes as amounting, singly or collectively, to an armed attack by Nicaragua on either both States."[381] The previous cases are important to consider that this theory could be used to justify the use of force against adversaries if the series of attacks

[377] Nicaragua case (merits) Ibid, para 195.
[378] Ruys T., Armed Attack and Article 51 of the UN Charter: Evolutions in Customary law and Practice, Cambridge University Press, New York, 2013, p. 155.
[379] Menachem Feder N., Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack, New York University Journal of International Law and Politics, 1987, p. 395.
[380] Ruys T., Ibid. p. 169.
[381] ICJ., Nicaragua v. United States case, Ibid., para 231. See also DRC v Uganda case, para 146. (The court considering whether series of attacks could be cumulative in nature, stated that: "even if this series of attacks could be regarded as cumulative in character, they still remained non-attributable to the DRC.") the court's statement did not dismiss the accumulation of events theory but did not confirm it due lack of clear evidence of attribution and not the theory itself.

cumulatively reach the sufficient gravity of the armed attack. And although case law did not confirm its applicability, it did not dismiss it.

Besides, it is required that the attack must be based on hostile intent against the victim state, otherwise, it will be considered a mere frontier incident. This has been confirmed by the ICJ in the Oil Platforms case that stated the following: "there is no evidence that the minelaying alleged to have been carried out by Iran to specifically target the US vessel. Therefore, the attacks could not amount to an armed attack." [382]

- **Ratione Personae (Actor Element)**

The element is also reflected in article 3 of resolution 3314 on the definition of aggression. It mainly states that acts committed by state actors or groups sent by or on behalf of a State constitute an armed attack if these attacks can be attributed to that state.[383] Such involvement can be through armed bands, groups, irregulars, or mercenaries sent by or on behalf of a State that conducts attacks that reach the threshold of an armed attack. This triggers the use of self-defense if there was enough proof of the involvement in these attacks, direct or indirect, to the state in concern.[384] The element also includes substantial involvement, by which the ICJ in the Nicaragua case did not suggest under what circumstances an involvement must be taken to be substantial enough as to amount to an armed attack. However, the court has excluded the mere tolerating of an armed group's presence within a state's territory and required that the assistance must amount to more than assistance to rebels in the form of the provision of weapons or logistical or other support.[385] Nonetheless, the spoofing technique in Cyber-attacks also targets the ratione personae by masking the attribution factor that links such attacks to the actual aggressor.

- **Ratione Temporis**

The element highlights the time required for the use of force in response to an armed attack. It is agreed that self-defense must be triggered in response to an attack that occurred or is imminent. This has been reflected in article 51 of the UN Charter. Therefore, three key points along the timeline of self-defense must be met: the period before an armed attack has occurred,

---

[382] ICJ., Oil Platforms, Islamic Republic of Iran v. United States of America, Judgment 2003, Reports 16, p. 196, para.
[383] Resolution 3314 (XXIX), Ibid. article 3(g).
[384] ICJ., DRC v. Uganda, Ibid. para 146.
[385] Randelzhofer A., Article 51 in Bruno Simma (ed), The Charter of the united Nations: A commentary, Oxford University press, 2002, 2nd edition, p. 788-802.

the period while the attack is ongoing and the period after it has ended. However, this element creates confusion of an ongoing debate regarding the anticipatory self-defense that corresponds with the standard established in the famous 1837 Caroline case.[386] According to the Caroline incident that is often thought of as a seminal international legal episode about anticipatory self-defense "self-defense would be lawful when the necessity of it is instant, overwhelming and leaving no choice of means, and no moment for deliberation." [387] So with regards to the period before an armed attack has occurred, it was argued that any use of force in self-defense against an attack that is not demonstrably imminent, is unlawful by which states will have to refer to the SC or employ non-forcible measures. The "UN High-Level Panel on threats, challenges, and change" stated in 2004 that "a threatened State, according to long-established international law, can take military action as long as the threat is imminent, no other means would deflect it and the action is proportionate."[388] Though the doctrine is not settled to date or enshrined by any case law however it appears to be accepted by a growing number of states. On the other hand, with regards to action taken during an ongoing armed attack, the victim state will have to respond within reasonable temporal proximity to the commencement of the attack, and any overly delayed response will be unlawful. For example, in the case of the Falklands, a period of twenty-three days was accepted period following Argentina's invasion because following the attack there was continued occupation of the islands, which means an ongoing armed attack.[389] And finally, with regards to responding to a terminated armed attack, though in general it is seen to be unlawful based on the basic customary international law requirement that self-defense is lawful only while the armed attack is ongoing.

In the context of the modern world, the line between what is reasonably temporally proximate to the attack and what constitutes a significant amount of time such the attack began, is almost impossible to identify. For example, the difficulty in detecting imminent terrorist attacks or cyber attacks, and the ability to gather all necessary information about it before responding is challenging to the victim state. Additionally, it faces issues with regards to how further can a

---

[386] The Caroline case occurred when British soldiers in Canada crossed the Niagara River to attack and send over Niagara Falls the American steamship Caroline that was assisting Canadian rebels. Britain justified their actions as self defense, but the US Secretary of State Daniel Webster wrote in 1842 that the use of force prior to suffering an attack qualifies as legitimate self-defense only when the need to act is instant overwhelming, and leaving no choice of means, and no moment for deliberation. See Potcovaru A., The International Law of Anticipatory Self-defense and US options in North Korea, 8 August, 2017. https://www.lawfareblog.com/international-law-anticipatory-self-defense-and-us-options-north-korea

[387] Waxman M., The Caroline Affairs in the evolving International Law of Self-Defense, 28 August 2018, https://www.lawfareblog.com/caroline-affair

[388] Potcovaru A., Ibid.

[389] Levitin M., The Law of Force and the Force of Law: Grenada, the Falklands, and Humanitarian Intervention, Harvard International Law Journal, 1986, Vol. 27, pp. 621-638.

state go in its response to eliminate the threat, particularly if waiting for the threats to cross the imminence threshold.

To summarize, the Charter of the UN prohibits the use of force against other states except where the UNSC has authorized the use of force and where a state is exercising its inherent right of individual or collective self-defense when an armed attack has occurred against the victim state, as recognized by Article 51 of the Charter. Under international law, for an act to be considered an armed attack, three elements must be taken into consideration. Firstly, *Ratione Materiae* that requires the existence of an unlawful act of force against a State, meets the required gravity threshold, individually or cumulatively with hostile intent against the victim State. Then, *Ratione Personae* relates to the party that conducted the illegal use of force, whether state or non-state actor. And *Ratione Temporis* is the element that deals with the determination of at what moment in time the use of force may be classified as an armed attack. This element is applicable when an armed attack occurred or the threat is imminent. Also, although article 51 preserves the right to use force if an armed attack has occurred, yet right to self-defense applies if used to avert the threat of an imminent attack, which is so-called anticipatory self-defense. A less restrictive argument by considering that a state must not wait until an armed attack has occurred to launch a legitimate pre-attack strike. That is also confirmed by the UN High-Level Panel on Threats, Challenges and Change, by which a threatened state can take military action as long as the threatened attack is imminent, no other means would deflect it and the action is proportionate.

The problem arises where the threat in question is not imminent but still claimed to be real. For example, the acquisition, with allegedly hostile intent, of nuclear weapons-making capability[390]. The statement was established in the 1837 Caroline case as the use of force before suffering an attack qualifies as legitimate self-defense only when the need to act is instant, overwhelming, and leaving no choice of means, and no moment for deliberation[391]. That also has roots after the attacks on the United States on 11 September 2001 by Al Qaeda, by which it has raised new considerations of pre-emptive self-defense with regards to the use of force to respond to armed attacks. The pre-emptive self-defense doctrine was defined as a claim to

[390] Report of the High-level Panel on Threats, Challenges and Change. A More Secure World: Our Shared Responsibility, UN General Assembly, A/59/565, 2 December 2004, para. 188, p. 54.

[391] Potcovaru A., The International Law of Anticipatory Self-Defense and U.S. Options on North Korea, Lawfare Blog, 8 August 2017. The article also refers to several examples when states cited self-defense to justify a pre-attack strike such as the Cuban Missile Criss, The Six-Day War and Operation Opera (Osirak Bombing) and other cases.

entitlement to use unilaterally, without previous or international authorization, high levels of violence to stop an incipient development that is not yet operational or directly threatening, but that is permitted to mature, could be seen by the potential attacked-state as susceptible to neutralization only at a higher and possible unacceptable cost to itself.[392] The main difference between the doctrine of anticipatory self-defense and pre-emptive self-defense is that the former demands the existence of an imminent attack to be launched, while the latter excludes that condition for the application of the right to self-defense. This doctrine does create broad interpretation and application compared to the traditional concept of the right to self-defense as it lacks proportionate response requirements and does not require imminence of the attack. States may abuse this doctrine in an unrestricted manner to claim the right to self-defense based on their interpretation of potential threat. This proves once more that traditional treaty-based self-defense and customary based anticipatory self-defense have demonstrated some flaws in their ability to protect and prevent states from new manifestations of the use of force, especially with trending issues such as attacks on non-state armed groups and cyber attacks. These issues will be developed further in upcoming sections.

2.2.2. Principles of Necessity and Proportionality in Self-Defense

The use of force in international law that is being justified by self-defense articulated in article 51 of the UN Charter, requires the involvement of fundamental principles (necessity and proportionality) in both jus ad Bellum and Jus in Bello. Although these principles unquestionably are critical to the stability of international relations, they are not identical in effect. International law restricts the use of force by states to situations of absolute necessity that justify only proportional force to counter-attack by an adversary. The principles are intended to limit state resort to force to a measure of last resort (*ultima ratio*) in Jus ad Bellum and are considered the founding principles for appropriate self-defense. Whereas the principle of proportionality under Jus in Bello, which is articulated in Article 51(5)(b) of the AP I, prohibits the attack that causes incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination which would be excessive with the concrete and direct military advantage anticipated.[393]

[392] Reisman W. and Armstrong A., "The Past and Future of the Claim of Pre-emptive Self-Defense", Yale Law School Legal Scholarship Repository, 2006, p. 526.
[393] Study on Customary International Humanitarian Law, Ibid., Rule 14.

While these principles are fundamental in both branches, yet they are not identical in effect. The right to use force in self-defense must adhere to the requirements of necessity and proportionality as a rule of customary international law[394], by which jus ad Bellum restricts resort to force by states to a situation of absolute necessity that justifies only proportional force to return the previously existing state of affairs (*status quo ante*). The principles are measured based on the lawful use of force to serve a legitimate end and they can only be applicable if can be seen as self-defense in response to an armed attack that occurred. Such response has two primary approaches for either halting and repelling an ongoing attack by minimizing the possibilities for lawful recourse to force[395], or halting and repelling but also preventing further attacks which are to be expected under the circumstances[396]. The ICJ in its advisory opinion on the legal consequences of the construction of a wall in the occupied Palestinian territory has considered that Israel cannot rely on a right of self-defense or on a state of necessity in order to preclude the wrongfulness of the construction of the wall. The court accordingly finds that the construction of the wall and its associated regime are contrary to international law.[397] By that, the court has observed that the state of necessity is a ground recognized by customary international law that can only be invoked under strictly defined conditions that must be cumulatively satisfied. Consequently, States' self-defense is strictly limited in the amount of force that may be employed to respond to the threat, as such force must be necessary to meet the threat and restore the status quo ante of security[398]. Therefore, any force that exceeds the limit is considered outside the realm of a legally justified response.

- **Necessity Principle**

Necessity means that states may use force in self-defense when peaceful means have been reasonably exhausted, or if diplomatic means are ineffective.[399] Therefore, the use of military force in self-defense is permissible if an armed attack began or is ongoing, as a necessary measure to intercept or repel an ongoing armed attack. The general rule behind the necessity principle for the use of force once enforced, is that it is presumed that peaceful means failed

[394] ICJ on the Legality of the Threat or Use of Nuclear Weapons, Ibid., para 41; Nicaragua v. USA, Ibid., para 176
[395] For more detailed explanation on this matter, see Kretzmer D., The Inherent Right to Self-Defense and Proportionality in Jus Ad Bellum, European Journal of International Law, 2013.
[396] ILA's Report on Aggression and the Use of Force, Ibid., p. 11
[397] ICJ on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory , Advisory Opinion 2004, para 136.
[398] The term is used in judging criminal sanctions': "The punishment must fit the crime." See Von Hirsch, Proportionality in the Philosophy of Punishment, Crime and Justice 1992, Vol. 16, p.55.
[399] Ruys, T., Armed Attack and Article 51 of the UN Charter, Cambridge University Press 2010, p. 95.

and the UNSC will not or cannot take measures necessary to maintain or restore international peace and security. However, one of the challenges in state behavior appears when states enforce this principle before an attack occurs presuming that the peaceful means will fail, which can be an alerting factor of using unnecessary force in international relations. One of the examples was the Israeli strike on an Iraqi nuclear reactor in 1981, an attack that was unanimously considered by the UNSC as a violation of the UN Charter.[400]

On the other hand, the United States in its dispute with Iran over its nuclear program in 2015, has considered that the use of force was necessary to prevent Iran from fortifying its nuclear facilities if peaceful measures failed.[401] Correspondingly, another challenge is regarding some states' tendency to use military force in self-defense after an armed attack ends if the state determines that further armed attacks are imminent or will occur if not forcibly prevented. For instance, the series of attacks launched by the United States and claimed as self-defense against Iran in 1987 in the aftermath of the missile that struck a Kuwaiti oil tanker and the incident where a US warship struck a mine in international waters by which the US attributed both incidents to Iran, were called by the ICJ as unnecessary use of force based on insufficient evidence that Iran was responsible for the attacks and considered that assuming Iranian responsibility was confirmed, the US attacks on the Iranian Oil complexes were also not necessary to respond to these incidents as there was no evidence that the US complained to Iran of the military activities of the platforms.[402] The former is an additional reference to the states in making reasonable efforts to resolving disputes by peaceful means even if states assume that future armed attacks might be anticipated.

- **Proportionality Principle**

This principle has to be tested based on different situations in which the use of force in self-defense was enforced. First and foremost, this principle involves a quantitative approach by which any use of defensive force must be comparable in its scale and effects to that of the armed attack to which it responds, and it will be judged by whether it was necessary to achieve its ends. So, the force that was not necessary to achieve legitimate ends will be regarded as disproportionate. The ICJ in the Oil Platforms case noted that: "As a response to the mining by an unidentified agency of a single United States warship which was severely damaged but not

[400] UNSC res. 487 of 19 June 1981.
[401] Haque, A., Necessity and Proportionality in International Law (draft), in Larry May (ed), Cambridge Handbook on Just War, 2016, p. 3.
[402] ICJ., Oil Platforms, Islamic Republic of Iran v. United States of America, Judgment 2003, Reports 16, p. 196, para. 76

sunk and without loss of life. The military operations by the United States that destroyed the Salman and Nasr platforms and what followed can be regarded as a proportionate use of force in self-defense." [403] This shows that both principles, necessity, and proportionality, may seem to interplay with regards to whether the restrictions serve to achieve the legitimate ends or whether those ends could be achieved by less restrictive means.

Another approach by the same principle involves a more instrumental way, in which states are required when deciding to use force in self-defense must define the aims of such force and assess the scope of the force and the means necessary to achieve those aims, this will be effective for states that plan to use force to halt or repel an ongoing or initial armed attack. However, it will not appeal to those who believe that force may be used after an armed attack ends to prevent or deter future attacks. Judge Higgins' advisory opinion on the legality of the threat or use of Nuclear weapons case considered that the concept of proportionality in self-defense limits response to what is needed to respond to an attack and not a requirement of symmetry between the mode of the initial attack and the mode of response.[404] The instrumental approach may be seen as inconsistent with the Jus Ad Bellum, as the aim of the modern law of force is not only to protect states from the unlawful force but also to limit any use of force that could cause more casualties, primarily to save succeeding generations from the scourge of war, according to the UN charter preamble.

The principle involves also a third approach, which is weighing or balancing the harm inflicted by defensive force with the harm prevented by the defensive measures. In other words, any necessary use of force in self-defense must guarantee that the operation is considered morally proportionate if it does well more than harm. The ICJ considered this approach to be valuable in its Nuclear Weapons advisory opinion and noted that the extremely strong risk of devastation associated with nuclear weapons may limit the extent to which states can exercise a nuclear response in self-defense under the requirements of proportionality.[405] While assessing this opinion it could be subjected to a narrow proportionality approach as the harm must not be disproportionate to the expected benefits of achieving legitimate ends. Some experts consider this approach irrelevant to jus ad Bellum in particular cases due to disagreements on whether the use of force is proportionate on the legitimate ends of force in the case under discussion.

[403] ICJ, Oil Platforms case, Ibid., at 197-199 para. 77.
[404] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, Dissenting Opinion of Judge Higgins, ICJ Reports 226 (1996), p. 583-4, para.5.
[405] Nuclear Weapons case, Ibid., paras 41-44.

Many examples of such disagreement can be identified in HW means in particular use of force against NSAs and cyber-attacks due to the complexity of such attacks and the amount of time needed to attribute such attacks to a state or adversary. For instance, in the aftermath of the criticism of Israel's use of force in Lebanon in 2006, many states referred to the extensive damage caused to civilians and to infrastructure that was considered disproportionate after measuring the damage caused.[406] Therefore, a combination of approaches to each case can be one of the useful legal tools to assess whether the use of force in self-defense is legitimate.

Respectively, the ICJ in the DRC v Uganda case seemed to combine the instrumental and weighing approach by observing that: " the taking of airports and towns many hundreds of kilometers from Uganda's border would not seem proportionate to the series of transborder attacks it claimed had given rise to the right of self-defense, not to be necessary to that end."[407] Also, according to Judge Kooijmans the actions conducted by Uganda were both unnecessary and disproportionate to the former's professed defensive aim by commenting that:

> "Not by any stretch of the imagination can the occupation of Kisangani airport or any of the subsequent attacks against a great number of Congolese towns and military bases be considered as having been necessitated by the protection of Uganda's security interests. These actions moreover were grossly disproportionate to the professed aim of securing Uganda's border from armed attacks by anti-Ugandan rebel movements." [408]

To conclude, principles of necessity and proportionality are vital for assessing the legitimate use of force in self-defense by minimizing the situations where states resort to force and limiting the disadvantages and consequences of the use of force on international relations and peace. Although these principles and their various approaches, explained above, can be assessed in conventional conflicts or threats between states. However, it is more complex when it involves cyber NSAs as to whether the non-state armed groups may be attributed to the host State or the time needed by the victim states to consider the effects that countermeasures could cause might all affect the ends of the force used, especially that self-defense provisions were drafted for a physical realm far before a scenario of active cyber-defense was foreseen. Therefore, many questions are raised with this regard as to whether the role of NSAs or the

[406] Ronen, Israel, Hizbollah and the Second Lebanon War, 9th Yearbook on International Humanitarian Law, 2006, at 373–374.
[407] Armed Activities on the Territory of the Congo (DRC v Uganda), Judgment 2005, ICJ Reports 163, p. 223, para 147
[408] Ibid. Separate Opinion of Judge Kooijmans, 2005 ICJ Reports 168, p. 306, para 34.

origin of cyber-attacks have attributed a state or not, also whether the desired result of the use of force is to prevent for instance NSAs from attacking again by depending on the instrumental approach or to deter the terrorist from further attacks by which the scale of the armed attack will be relevant in assessing the proportionality of the force used. All these conceivable ends will be fundamental to the legality of the use of force in line with the principles of proportionality and necessity that the study will try to answer in upcoming sections of the thesis.

2.3. Right to Self-Defense against Non-State Actors (NSAs)

The use of force against armed groups is not new but has been modernized after the U.S. operations in Afghanistan following the attacks of 11 September 2001, which led to extraordinary legal attention surrounding its legitimacy and many studies have been made in recent years about extraterritorial use of force against terrorists or other NSAs. Much more debates centered upon the question of whether a State has the right to self-defense in response to attacks or threats generated by such groups located in another State in the absence of attribution of the attack to that State[409]. NSAs' status is regulated through numerous areas of international law and does not constitute a "terra incognita" or undiscovered domain, due to their vital role and involvement in international relations throughout history.[410] Such groups are non-governmental groups that directly or indirectly engage in support of non-governmental combatants in non-international and purely internal conflicts. In the same sense, Cherif Bassiouni identifies the types of such groups as the following:

- "Regularly constituted groups of combatants with a military command structure and a political structure;
- Non-regularly constituted groups of combatants with or without a command structure and with or without a political hierarchical structure;
- Spontaneously gathered groups who engage in combat or who engage in sporadic acts of collective violence with or without a command structure and with or without political leadership;
- Mercenaries acting as an autonomous group or as part of other groups of combatants;

[409] Lubell N., Fragmented Wars, Multi-Territorial Operations against Armed Groups, Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare, Oxford University Press, Lieber Series, 2019, Vol 1, p. 4.
[410] Schreuer C., "The Waning of the Sovereign State: Towards a New Paradigm for International Law?" European Journal of International Law 1993, *p.* 447

- Expatriate volunteers who engage for a while in combat or support of combat operations, either as separate units or as part of duly constituted or ad hoc units."[411]

Moreover, NSAs can be divided into two categories: 1- Peaceful NSAs that abide by international law and include non-governmental organizations, international religious organizations where there is no need to deter such actors. 2- Violent NSAs (VNSAs) include international criminal organizations, terrorist groups rebel groups in which they are the main target of deterrence by states and the international community[412]. VNSAs can be hardly deterred for several reasons, mainly lack a single approach to be applied to them due to their variances (motivation and characteristics, ideology and objectives) as they are composed of distinct factions that have multiple political objectives and moral justification. For instance, Al Qaeda and ISIS, although have a common understanding that the Jihad is a Just War as fighting for a greater cause, yet have a difference in views, strategy, and objectives, by which the latter aimed to create a caliphate and focused in their fight on local enemies, contrary to what Al Qaeda that targeted distant enemies[413].

Besides, claims of legitimacy differ between the two groups, Alia Brahimi considers that: "proper authority in waging Jihad was designed as the decisive test of a conflict's legitimacy."[414] Al Qaeda's quest for legitimacy is visible through the constant invocation of sacred texts, and an attempt to appear as a scholar capable of interpreting Islamic laws. On the other hand, ISIS legitimacy represented by Abu Bakr Al Baghdadi is based on the figure of Mahdi, a historical and spiritual figure dating back from the Abbasid revolution of whom the ISIS leader made many references, while Al Qaeda never dared to suggest that the Mahdi was around the corner.[415] The difference in moral justification proves that these groups are not fighting the same war and this has an impact on their strategies and means to the battlefield. The same is with groups such as Al-Shabab and Boko Haram that witnessed internal disputes among its factions for goals that need to be achieved, and this state of uncertainty about the ideological composition of VNSAs obstructs the ability to adapt a collective response towards such groups[416]. Moreover, challenges arise from the nature of the targeted actor, as most of the

---

[411] Bassiouni Ch., Ibid. p.715-716

[412] Blackburn, A., Brannum, R.K., Turmelle, D.R., Boyette, G.T. and Napolitano, W.M. A National Policy for Deterring the Use of Weapons of Mass Destruction, Air Command and Staff College, Air University, Montgomery 1996.

[413] Fraise Th., Shades of Jihad: Variation of Military Ethics between ISIS and Al Qaeda, Sciences Po Kuwait Program, Fall 2017, p. 3

[414] Brahimi A., Jihad and Just War in the War on Terror, Oxford University Press, New York 2010, p. 318.

[415] Fraise Th., Ibid. p.4

[416] Elbahu R., Deterring Violent Non-State Actors: Dilemmas and implications, Journal of Humanities and Applied Social Science 2017, p. 46-47.

VNSAs do not exercise sovereignty over a territory, but in contrary, they seek to undermine the legitimacy and credibility of the state by threatening its ability to exercise its sovereignty over the territory it controls as it is often easier for a VNSA to deter a state and not the opposite[417]. Such a lack of clear understanding of the nature and objectives of such groups can be a double-edged weapon, as it could be successful to discourage the use of force, but at the same time, it could be the main cause for promoting such use of force.

A legal person is an entity that has duties and rights before the legal system. According to the AP I of the Geneva Conventions of 12 August 1949, armed groups are dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of the territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol, such groups bear responsibility and obligations under international law. That has been confirmed in the Tadić Case that stated "An 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."[418] The legal framework of the use of force generally can be invoked against an aggressor state, and the state practice has proved that invoking self-defense against non-state armed groups is applicable practically. Besides, although the term "State" appears in Article 2(4) of the UN Charter concerning the use of force against the territorial integrity or political independence of another state, such limitation was not included in Article 51 of the Charter[419]. Therefore the former article does not exclude self-defense against attacks generated by NSAs.

Nonetheless, some scholars have referred to the practice in the UNSC in the 1990s as evidence of extension of the prohibition of the use of force within the states[420], and the resolutions that included non-state armed groups with regards to non-international armed conflicts, imposing

[417] Elbahu R., Ibid. p. 47.

[418] ICTY, Judgmenet in Tadic Case, Appeals Chamber 1999, para. 70. See also on Customary Law rules; Convention on the Prevention and Punishment of the Crime of Genocide 1948, 78 UNTS 277, art 4: 'Persons committing genocide or any of the other acts enumerated in article III shall be punished, whether they are constitutionally responsible rulers, public officials or private individuals."

[419] Chen Lung-Chu, An Introduction to Contemporary International Law, Oxford University Press 2000, 2nd ed., p. 25-38.

[420] Cassese A., "Article 51", in J.P. Cot and A. Pellet eds., La Charte des Nations Unies (The United Nation Charter), 3rd edn., 2005, at 133.

obligations of the ceasefire on the parties[421], or the refrain from any use of force[422]. Also, The application of article 51 in response to attacks from nonstate armed groups, has been developed and became practical after 9/11 which was confirmed by the SC resolution 1368(2001) and demonstrated that an attack of terrorists may rise to the level of an armed attack of a State. Therefore, the UNSC has referred to the right to self-defense in such instances.

A most recent example in contemporary conflicts is the Turkish operation "Peace Spring" of October 2019, which was launched against the Kurdish military groups in northeast Syria, and justified under Article 51 of the UN Charter, mainly to counter "an imminent" terrorist threat[423]. Turkey also considered that this operation is essential within the context of the responsibility attributed to member states of the UN in the fight against terrorism through Security Council Resolutions.[424] Turkey in this letter has taken the position of "anticipatory self-defense", by which such right exists if an armed attack against a state is imminent and if the state is faced with a threat of an armed attack which presents a necessity of self-defense, instant, overwhelming, leaving no choice of means and no moments of deliberation[425]. However, attacks against NSAs and whether it justifies a forcible defensive action on the territory of another state is a controversial topic that is rejected by several states and international lawyers, as it broadens the interpretation of the right to self-defense[426]. Therefore, it is still premature to affirm that Article 51 no longer requires any state involvement and could be invoked against any armed attack irrespective of the attacker's character[427]. But at the same time, self-defense following an armed attack by an independent NSA operating from outside the borders has support in a textual reading of Article 51 of the UN Charter, which does not mention the nature of the entity that commits the armed attack, as it deprives the inherent right to self-defense if such right is based on the identity of the attacker rather than the attack itself.[428]

---

[421] SC Res. 849 (1993); SC Res. 858 (1993); SC Res. 1150 (1998); SC Res. 1187 (1998); SC Res. 1225 (1999); SC Res. 1216 (1998); SC Res. 1199 (1998); SC Res. 1584 (2005). For more details and citation see, Corten O., The Law against War: The Prohibition on the Use of Force in Contemporary International Law, Hart Publishing March 2012, at 131.

[422] Corten O., Ibid., para. 24

[423] Letter dated 9 October 2019 from the permanent Representative of Turkey to the United Nations addressed to the President of the Security Council, United Nations Security Council, S/2019/804, p.1. The facts that Turkey refers to in this letter are essentially those: 'In particular, PKK/PYD/YPG units close to Turkish borders in the north-east of Syria, continue to be a source of direct and imminent threat as they opened harassment fire on Turkish border posts, by also using snipers and advanced weaponry such as anti-tank guided missiles.'

[424] Ibid. p. 2. See for example the Security council resolutions [1373(2001), 1645 (2005), 2170 (2014), 2178 (2014), 2249 (2015) and 2254 (2015)] that were referred to in the letter above.

[425] Kretzmer D., Ibid. p. 247,248.

[426] Kreb C., A Collective Failure to Prevent Turkey's Operation "Peace Spring" and NATO's Silence on International Law, Blog of the European Journal of International Law , October 2019.

[427] Lanovoy V., Ibid., p. 573

[428] Greenwood Ch., International Law and the War against Terrorism, International Law Affairs, 2002, Vol. 78, p. 301-307.

This can be verified in the position of the significant number of states that have intervened against ISIS in the Syrian territory and the letters that were sent to the UNSC regarding these actions and providing by that a recognition of self-defense action against an armed group on another State,[429] and most importantly that state practice against NSAs have certainly been recognized subject to core requirements of proportionality and necessity.

In parallel, HW that aim to generate a situation where it is unclear whether a state of war exists- and if it does, who is a combatant and who is not due to the extensive employment of non-state armed groups, it is important to analyze the right to self-defense against such groups especially those not imputed to a state as it is relevant to the general prohibition on the use of force in international relations according to the UN Charter. The complexity of the strategic and legal environment created by such groups in contemporary threats relies upon the blurring character of state and NSAs into one force that is commonly known as a proxy relationship. NSAs have been employed to act clandestinely for objectives that regular forces have been unwilling or unable to achieve as a rational means to govern and control[430]. These proxy forces are part of regular forces but fight for and on behalf of states wishing to alter the strategic outcome of a conflict while remaining external to it[431]. Numerous proxy and state-controlled forces can be identified in the era of the current HW environment, such as Iran's axis of resistance network in the Levant involved in conflicts in Syria, Iraq, Lebanon, and Yemen. Also, one of the examples is the Little green men in Ukraine, is when soldiers without insignia on their green uniforms seized control of Crimea in 2014, Russian officials including the Russian President Vladimir Putin denied that they were Russian troops until a year later, also the Chinese civilian finishing boats in the South China Sea that includes the "Yue Tai Yu Fleet" that their maritime militia status seems apparent from time spent loitering in the waters around Philippine-occupied "Thitu" and "Loaita" Islands[432].

---

[429] See for e.g. Letter from the Charge d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council, UN Doc. S/2015/221, March 31, 2015, that stated the following: "writing to report to the Security Council that Canada is taking necessary and proportionate measures in Syria in support of the collective self-defence of Iraq, in accordance with Article 51 of the Charter of the United Nations."

[430] Davis, D., Non-State Armed Actors, New Imagined Communities and Shifting Patterns of Sovereignty and Insecurity in the Modern World, Contemporary Security Policy, p. 222.

[431] Rauta V., Towards a Typology of Non-State Actors in Hybrid Warfare: Proxy, Auxiliary, Surrogate and Affiliated Forces, Cambridge Review of International Affairs, September 2019, p. 10-11.

[432] Poling, G., Illuminating the South China Sea's Dark Fishing Fleets, January 2019, www.ocean.csis.org.

On the other hand, Auxiliary forces combine regular and irregular forces by which it is not considered part of regular forces but are directly embedded into the structure of fighting operating in collaboration with or alongside regulars or more of supplementary form to the regular forces.[433] For example, during the annexation of Crimea, the formation of Russian special forces and local self-defense militias has played a role as auxiliary forces in the conflict[434]. This explains how hybrid NSAs can mask their operations and relations with other States, a factor that evolves based on the intensity and role in a conflict or internal disturbance. Parallelly, a state before resorting to self-defense must ensure that it meets the criteria of necessity, proportionality, and immanency if applicable, and these requirements may vary depending on whether the acts of such groups were imputed based on direct control or indirect attribution that must be addressed properly to prove the undoubted linkage between NSA and host state for any cross-border operations.

In other words, Article 51 does not limit the potential originator of armed attacks to States[435], while the UN Charter was drafted in a legal surrounding with little awareness towards threats of internationally organized armed groups. Yet, the ICJ has refrained from giving such interpretation[436]. This can be seen in the Oil Platforms Case of 2003 in which the court continued to apply the state-centric concept of armed attack without suggesting any interpretive changes with regards to aggression by NSAs[437]. Attacks launched by non-state armed groups have been largely settled after the UN Security Council recognized that the 9/11 attacks constituted an armed attack justifying the right to self-defense[438]. Alternatively, in the aftermath of the 9/11 attacks, the USA and its allies reincarnated an old doctrine from the pre-UN charter, what is known as the unwilling and unable doctrine, to justify the use of force against non-state armed groups in weak or sympathetic states. The doctrine that is seen as a process of legal change, was used by states to legally justify their right to self-defense under

[433] Rauta V., Ibid. p. 9
[434] Ibid. p.9-10.
[435] Kowalski M., Armed Attack, Non- State Actors and a Quest for the Attribution Standard, polish Yearbook of International Law 2010, Vol. 30, p.119.
[436] Starski P., Right to Self-Defence, Attribution and the Non-State Actor- Birth of the "Unable and Unwilling" Standard, Heidelberg Journal of International Law, Sept. 2015, p. 461.
[437] ICJ, Oil Platforms Case, ICJ Reports 2003, p.161, para. 51. The court has also stated that: "…the evidence indicative of Iranian responsibility for the attack on the Sea Isle City is not sufficient to support the contentions of the United States. The conclusion to which the Court has come […] is thus that the burden of proof of the existence of an armed attack by Iran on the United States […]." See ICJ, Oil Platforms Case 2003, Ibid. para. 61.
[438] Security Council Resolution (S.C. Res.) 1368, September 12, 2001; S.C. Res. 1373, September 28, 2001.

Jus ad Bellum against imminent or actual armed attacks from the territory of another state unable and unwilling to consent to the target state using force[439].

While the lawful use of force is codified to narrow down the state's ability to illegally use force, however, certain activities though not legally accepted or considered as a customary rule, have been practiced by states for more than two decades and could be seen as a misuse of law or instrumentalizing the laws for the interest of the state, or what is so-called Lawfare. States and NSAs employ these legal arguments and process them as tools of hybrid influencing, by which law is one of the domains in which hybrid competition takes place[440]. Such behavior has raised various legal questions about targeted killings and the principle of non-interventions that might have been justified under jus ad Bellum as part of a broader claim of self-defense, yet it has many effects on Jus in Bello (IHL) rationales in defense of the lethal operations against non-state armed groups[441].

Whether the arguments mentioned above are an accepted shift of the traditions of Jus ad Bellum to replace existing law or not, or for being an unwarranted expansion of the long-standing recognized confines of self-defense, is still early to decide. However, such standards are of high importance to contemporary threats concerning the state's responsibility for wrongful acts if they failed to prevent the use of their territory to harm another state. The unable or unwilling standard profoundly alters the nature of the due diligence principle that derives from the principle of sovereignty, allowing more suppleness in the use of force by eliminating the requirement of attribution of the actions of NSAs to a state. That is based on the argument that attribution to the state from whose territory the armed attack being launched, is no longer necessary.

2.3.1. Self-Defense against Non-State Actors on the Territory of another State: The Myth of the Unable or Unwilling Standard in the Hybrid Warfare era

The rise of ambiguous contemporary threats involving armed groups and cyber operations that rely on the ability of adversaries to maintain operations below the threshold of armed attack or even avoid direct attribution has encouraged states to expand the exception of the right to use

[439] Martin C., Challenging and Refining the "Unwilling or Unable Doctrine", Vanderbilt Journal of Transnational Law 2019, Vol.52, p.391
[440] Joint Research Centre and European Centre of Excellence for Countering Hybrid Threats, The Landscape of Hybrid Threats: A Conceptual Model, European Commission, Brussels 2020, section 4.1.9.
[441] Martin C., Ibid. p. 390.

force by enforcing extraterritorial self-defense through the "Unable or Unwilling standard". According to this standard, states have the right to respond to attacks generated by NSAs from the territory of another state without their consent, when NSA use the host state's sovereignty as a shield to protect themselves[442] , or if the host state is unwilling or unable to deal with the threat possessed by the NSA. The standard was led by a former British official Daniel Bethlehem who in 2012 published a set of sixteen principles as a legal foundation of the justification to use force against NSAs in nonconsenting territorial states, what is commonly known as "Bethlehem Principles"[443]. The roots of the standard can be traced back to Emer de Vattel under the law of neutrality that obliges neutral states to ban belligerent forces from operating within their territory, as later codified in the 1907 Hague Convention.[444]

In the aftermath of the terrorist attacks of 11 September 2001, the use of force in self-defense has been continuously applied to new circumstances involving non-state actors, particularly international terrorist groups. But an increasing number of states are supporting a broader interpretation of the right to use force in self-defense to intervene against non-state actors whenever and wherever they operate.[445] An approach that contradicts with the narrow requirement of "substantial involvement" stressed by the ICJ in the Nicaragua case when defining aggression in Article 3(g) that noted the attribution along with situations involving a state's substantial involvement in the non-state attack. The substantial involvement requirement was recognized by the UNSCRs 1368 and 1373 that recognized the inherent right to self-defense against international terrorism committed by violent NSAs and called on all states to adjust their national laws so that they can ratify all of the existing international conventions of terrorism[446]. That had direct impact on justifying the operations in Afghanistan, by stressing that these operations did not invoke the unwilling or unable standard, instead, it

[442] Trinkunas H. and Clunan A., Alternative Governance in Latin America, Routledge Handbook of Latin American Security, vol. 99, p. 103.
[443] Martin C., Challenging and Refining the "Unwilling or Unable" Doctrine, Vanderbilt Journal of Transnational Law, 2019, p. 7.
[444] Ibid., p. 16.
[445] J Wright QC MP , The Modern Law of Self-Defense, Transcript of speech given at the International Institute for Strategic Studies, London, EJIL: Talk, Blog, 11 January 2017. Speech of the UK Attorney-General that noted : "… A number of States have confirmed their views that self-defense is available as a legal basis where the state from whose territory they actual or imminent armed attack emanates is unable or unwilling to prevent the attack or is not in effective control of the relevant part of its territory."
[446] UN Security Council resolution (Res) 1368 of September 12, 2001 UN Doc S/RES/1368 and UNSC Res 1373 of September 28 2001, UN Doc S/RES/1373.

was based on the fact that the Taliban regime has supported the Al-Qaeda[447]. The standard was also invoked through the drone strikes conducted by the US that targeted Osama Bin Laden in Pakistan in May 2011 without the consent of Pakistan that in return flagged this violation of Pakistan's sovereignty. However, the US has justified the operation based on the Unwilling or Unable standard and considered it to be a lawful use of force since Pakistan was not willing or unable to deal with the threats and influence of Al-Qaeda. Similarly, the operations against ISIS in Syria were considered by the US, Canada, Turkey, and Australia as legitimate since the Syrian government is unwilling or unable to prevent the use of its territory for such attacks.[448] Consent has never been requested by territorial states to justify these operations, rather the issue of invitation or consent was not mentioned in the legal justifications provided by the intervening states. For example, the US State Department indicated that the US-led coalition was not looking for the approval of the Syrian regime, and ruled out any cooperation with Syrian government forces.[449]

Although ISIS has exercised to a certain extent a substantial degree of territorial control over parts of Syria and Iraq, the intervention by the Western States, in Syria particularly, is relevant to the unable or unwilling standard. On the other hand, Germany and Belgium indicated that the threats were legally confronted since they were generated from a territory where the Syrian authorities did not exercise effective control and linked their self-defense arguments to UNSC resolution 2249 which indicated that "ISIS constitutes a global and unprecedented threat to international peace and security because of its control over significant parts and natural resources across Iraq and Syria calling upon states to take all necessary measures, in compliance with International law on the territory under the control of ISIS".[450] The US and a

[447] See the letters of the United States and the United Kingdom to the Security Council regarding their operations in Afghanistan, UNSCOR, 56th Year, UN Doc S/2001/946, and UNSCOR, 56th Year, UN Doc S/2001/947.

[448] See for example letters of the Intervening states in Syria: UN Doc. S/2014/695, 23 September 2014, letter from the Permanent Representative of the united States of America to the UN addressed to the Secretary-General. See also, UN Doc. S/2015/563 of 24th of July 2015, Letter from charge d'affaires a.i. of the Permanent Mission of Turkey to the UN addressed to the President of the Security Council. See more, Keskin F., Trujey trans-border operations in northern Iraq: Before and after the invasion of Iraq, Research Journal of International Studies, 8 November 2008

[449] See, "White House won't commit to asking Congress for Syrian Strike", The Hill, 25 August 2014. https://thehill.com/policy/defense/215905-white-house-wont-commit-to-asking-congress-for-syria-strike. See also,. Gearan A., "U.S. rules out coordinating with Assad on airstrikes against Islamists in Syria", Washington Post, 26 August 2014. Available at: https://www.washingtonpost.com/world/national-security/us-rules-out-coordinating-with-assad-on-airstrikes-against-islamists-in-syria/2014/08/26/cda02e0e-2d2e-11e4-9b98-848790384093_story.html

[450] Arrocha P., An Insider's View of the Life-Cycle of Self-Defense Reports by the U.N. Member States "Challenges posed to the International Order", www.JustSecurity.org , April 2, 2019.

coalition of several other states stated in the letter of September 2014 to the UN Security Council that: "states must be able to defend themselves under the inherent right to individual and collective self-defense when the government of the State where the threat is located is unwilling or unable to prevent the use of its territory for terrorist attacks"[451]. Furthermore, the U.S. Ambassador to the UN "Samantha Power" has announced openly that the airstrikes in Syria are based on the unwilling or unable test as a newly devised justification for militant self-defense and humanitarian action[452]. Therefore, several states have confirmed their view that self-defense is available as a legal basis where the state from whose territory the actual or imminent armed attack emanates is unable or unwilling to prevent the attack or is not ineffective control of the relevant part of its territory.

The previous examples and statements will be seen to evolve in the era of hybrid threats through NSAs, and even though there is no clear reference in Article 51 to the unable or unwilling standard, some states argue that these actions are legal under the interpretation of the article in concern. The standard cannot yet be understood as being part of customary international law, and aspects of it are inconsistent with long-established principles of jus ad Bellum. For example, according to Bethlehem " the primary objective of his effort was to move the policy away from the rhetoric of a global war on terrorism, with its lack of geographic and temporal and other limitations, hinged on status-based targeting and driven by operational decision-making, and back to a legal framework that turns on an appreciation of imminent threats, of sovereignty, of limitations rooted in necessity and proportionality"[453]. Therefore, if international law evolved to embrace the standard, the threshold for using force in self-defense would be lower at all circumstances that would destabilize the jus ad Bellum regime, but at the same time will limit the ability of NSAs to operate behind the shield of territorial sovereignty of other states in ungoverned spaces.

The majority of states have been quiet about the Unable and Unwilling standard, but some states have raised concerns about expanding their applicability in international relations without reaching a concrete result. For example, the Community of Latin American and Caribbean States (CELAC) expressed that any use of force that is not in compliance with the

[451] UNSCOR, 69th Year, UN Doc S/2014/695
[452] Deeks A., Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense, Virginia Journal for International Law, 2012, , p. 495.
[453] Bethlehem D., Principles of Self-Defense - A Brief Response, American Journal of International Law, 2013, at 580.

UN Charter is not only illegal, it is also unjustifiable and unacceptable. Further consideration should be given in an open and transparent debate on this issue.[454]

On the other hand, according to Ashley Deeks, who explored the theoretical and historical foundations for the standard, states that wish to apply the "Unwilling or Unable doctrine" to counter threats posed by non-state armed groups operating from the territory of another state, have to follow certain guidelines[455]:

- A state must seek permission from the territorial state to use force within its territory, and if such permission was granted then there is no need to apply the unable or unwilling doctrine. But if such permission was not granted then the targeted State must propose to undertake a joint military operation against the NSA[456]. For instance, the ICJ in 2005 had reviewed the presence of the Ugandan military forces in the Democratic Republic of Congo that a state could use force legally with consent.[457]
- Analyzing the nature of the NSA and whether the host state is willing and able to subdue the threat on its own. Such analysis covers mainly the capacity of NSA and the level of sophistication of the attacks, the capacity of the governments' forces, the geographical terrain of the territorial state as to whether the NSA can establish safe havens that are hard for the host state to contain.[458]
- Assessing the willingness of the host state to subdue the threat. This is very important to prove that the host state is aware of the threat and can take necessary measures to counter the threat before any actions are taken by the victim state without the consent of the territorial state.[459]
- Likewise, assessing the capability of the territorial state to counter the threat generated from its territory even if it has the will to counter such a threat[460]. Such a scenario can be easily identified in cases where the territorial state has lost its control over an area in its territory or what is also known as ungoverned spaces. Turkey for example has

[454] Measures to Eliminate International Terrorism, Statement by the Permanent Mission of the El Salvador to the United Nations on behalf of the Community of Latin American and Caribbean States (CELAC), New York, 3 October 2018.
[455] Deeks A., Ibid., p. 506.
[456] Ibid., p 519.
[457] ICJ Judgment, Armed Activities on Territory of Congo, 2005, at 168.
[458] Deeks A., Ibid. at 525-29, 541.
[459] Ibid., at 510-11.
[460] Ibid., at 529-29.

justified its intervention against the Kurdish rebels in Iraq "PKK" which was operating in a territory not ungoverned by Iraqi forces.[461]

- A territorial state must evaluate whether it can handle the situation independently or be assisted by the targeted state. The willingness of the territorial state will be identified if it is incapable of countering such a threat independently and refused the proposed assistance.[462] This also needs an evaluation from the targeted state proposing assistance and the territorial state's experience with previous assistance. So, while in the past the territorial state may have been supportive of the victim state, it may not necessarily be the same in the future, and vice versa.[463]

To illustrate, numerous studies contributed to analyzing the right to self-defense if the attack by NSA was imputed to a state. Though, according to David Kretzmer, it seems to be clear is that the mere fact that a group of NSAs operates out of the territory of a state does not imply that an armed attack by the group against another state may be imputed to the host state. While all states have the duty under international law to prevent their territory from being used by NSAs to violate or breach the rights of the third state, an obligation that finds its roots in the domain of human rights and environmental law, compromise taking all means reasonably available to the state to prevent unlawful activities conducted by such groups[464]. Still, violation of this duty does not of itself amount to an armed attack and therefore does not trigger the right of the victim state to use force against the host state in self-defense[465]. Although, the current practice supports the view that states that harbor irregular forces have duties towards the civilians in the victim states and that failure to fulfill these duties 'activate the injured state's right to self-defense, this also applies to weak states which are unable to fulfill their duty to prevent their territory being used as a base for activities against the injured state[466].

Additionally, the ICJ in the Nicaragua case considered that armed attack could extend to cover attacks by armed bands, groups, irregulars, or mercenaries if they have been sent by or

---

[461] Riamei L., The Kurdish Question: Identity, Representation and the Struggle for Self-Determination, 2015, p. 11.
[462] Qureshi W., International Law and The Application of the Unwilling or Unable Test in the Syrian Conflict, Drexel Law Review, 2018, vol. 11, p. 72.
[463] Ibid., p. 73.
[464] The Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Merits, 26 February 2007, ICJ Reports 43, at 221, para. 430; Corfu Channel (UK v. Albania) (Corfu Channel), Merits, 9 April 1949, ICJ Reports 4, at 22. See also Island of Palmas Arbitration (The Netherlands v. US), Decision of 4 April 1928, reprinted in UNRIAA, vol. 2, 829, at 839.
[465] Kretzmer, D., Ibid. p. 244,245.
[466] Reinold, Th., "State Weakness, Irregular Warfare, and the Right to Self-Defense Post- 9/11", American Journal of International Law, Vo. 105, No.2, 2011, p. 284.

on behalf of a state[467]. This has been confirmed by the ICJ in its Advisory opinion on the Legal Consequences of Construction of a Wall, by opining that Israel could not defend the legality of the separation barrier in West Bank based on its right to self-defense under Article 51 since it did not claim that the attacks which the barrier was designed to prevent were imputable to another state[468]. Moreover, although NSAs had a major role in the DRC v. Uganda case, yet the court held on the requirement of attribution implying to follow the state armed attack concept by stating that: "there is no satisfactory proof on the involvement in these attacks, direct or indirect, of the government of the DRC. The attacks did not emanate from armed bands or irregulars sent by the DRC or on behalf of the DRC, within the sense of Article 3(g) of GA resolution 3314 (XXIX). The court is of the view that on the evidence before it, even if this series of deplorable attacks could be regarded as cumulative, they remained non-attributable to the DRC.[469] Yet the court did not fully confirm the state-centric concept of an armed attack, as it added that: "There is no need to respond to the contentions of the parties as to whether and under what conditions contemporary international law provides for a right of self-defense against large-scale attacks by irregular forces[470]. Similarly, clarity as a requirement to legal rules does not meet the justifications provided by states promoting this standard, by which expanding the right to self-defense to include threatening deployments that do not have imminent attack without objective assessment in the law of self-defense will lead to remove the legal constraints on the inter-state violence and endanger the foundational legal principles of sovereignty and non-intervention.[471]

Hybrid adversaries tend to use proxy fighters to conduct attacks against other states to avoid direct attribution to the conflict, and the view that attacks by NSAs that are not attributable to a state cannot constitute an armed attack creates the loophole of hybrid campaigns and an evolving tension between the expansionist and the traditional approach of jus ad Bellum. However, the majority of scholars rejected such claim, by arguing that Article 51 does not refer to an armed attack by a state and that the UN Security Council justified that the use of force against the armed attack of 9/11, is an inherent right of individual and collective self-defense

[467] ICJ, Nicaragua v United States of America, Ibid. at 195.
[468] ICJ, Legal Consequences of the Construction of a Wall in the occupied Palestinian Territory 2004, Rep. 136 at para.139. See also, Scobbie, Words My Mother Never Taught Me- In Defense of the International Court, American Journal of International Law (AJIL), 2005, p.67
[469] ICJ, Armed Activities on the Territory of the Congo, ICJ Reports 2005, 168, para. 146.
[470] ICJ, Ibid., note 33, para. 147
[471] For more information about these arguments see, Von Bernstorff J., Drone Strikes, Terrorism and the Zombie: On the Construction of an Administrative Law of Transnational Executions, European Society of International Law (ESIL) Reflections, 2016, p.2-6.

under the UN Charter[472], and implicitly recognized the state's right of self-defense in response to the attacks by Al -Qaeda, although self-defense as an exception to article 2/4 of the UN Charter can be justified by UN Security Council under Chapter VII of the Charter. However, these resolutions cannot but are read as affirmations of the view that large-scale attacks by NSAs can qualify as armed attacks within the meaning of Article 51.[473]

Furthermore, with the technological developments of weapons and the use of cyberspace to conduct attacks, in addition to the role of unconventional insurgent groups such as ISIS or the Ukrainian separatists, where they possess strong capabilities that regular armed groups without qualifying them as full-fledged armies with weapons traditionally associated with nation-states, the pre-emptive use of force are being justified by states as a defensive measure against non-state armed groups, similarly to threats from terrorist attacks.[474] The High-Level Panel of Experts, that was appointed to examine UN reform, stated that: "A threatened State, according to long-established international law, can take military action as long as the threatened attack is imminent, no other means would deflect it and the action is proportionate".[475] So, State practice (though not universally accepted) acknowledged that the use of force as pre-emptive self-defense may be allowed to counter an imminent attack.

To conclude, the use of force in self-defense against NSA, within the territory of a non-consenting host state, thus prima facie constitute an internationally unlawful violation of the host state's territorial sovereignty, even if the injured state has the right to self defense. The unable or unwilling standard as a rule rather than ad hoc decision by states requires to be embraced by consistent and widespread practice accompanied by opinio Juris as a matter of promulgation[476]. The shift in norms is not as fluid and rapid as the evolution of contemporary

---

[472] UN Security Council Resolution 1368 (2001) adopted 12 September 2001 (preamble) and Resolution 1373 (2001)

[473] See, ICJ., Armed activities on the territory of the Congo (Democratic Republic of Congo v. Uganda), Rep. 168, 2005, Separate Opinion of Judge Simma, at 11.

[474] Arend A., 'International Law and the Preemptive Use of Military Force', The Washington Quarterly 2003, p. 89. See also, In the National Security Strategy of the United States 2002, available at: www.globalsecurity.org/military/library/policy/national/nss-020920.htm by which the US declared that if necessary it would act pre-emptively to forestall or prevent hostile acts by its adversaries, 'even if uncertainty remains as to the time and place of the enemy's attack'.

[475] A More Secure World: Our Shared Responsibility, Report of the High-level Panel on Threats, Challenges and Change, 2004, UN Doc A/59/565, at para. 188

[476] The ICJ explained opinion juris in the Nicaragua case as follows: "… for a new customary rule to be formed, not only must the acts concerned amount to a settled practice, but they must be accompanied by opinio juris sive neccessitatis. Either the States taking such action or other States in a position to react to it, must have behaved so that their conduct is evidence of a belief that the practice is rendered obligatory by the existence of a rule of law requiring it. The need for such belief, the subjective element, is implicit in the very notion of opinio juris."

conflicts and their means, and legal rules must reach the level of certainty, reasonability, and clarity to be promulgated. The unable or unwilling standard has not reached this level yet despite being promoted by relatively powerful western states. Taking for example cyber-attacks by non-state armed groups in the territory of a state unable to detect or intersect these activities, would threaten the host state's sovereignty from military intervention even if it is willing to take sufficient measures against these groups, but unable because of the nature of these attacks that are hard to be detected and requires developed interceptive systems most of the states are not equipped with. So, states find themselves obliged to consent to the intervention or it will be forced upon them. In this context hybrid warfare through NSAs and cyber operations of transnational effect are shifting the applicable law on the use of force to be stretched by ad hoc decisions by states to deter such operations, creating a pattern that could evolve to customary rule.

2.3.2. Self-Defense against Proxy Armed Groups

According to Andrew Mumford, a proxy war is an indirect engagement in a conflict by third parties wishing to influence its strategic outcome.[477] The indirectness of such activities is in many instances linked overtly to another state or alliance that supports proxy armed groups directly or indirectly by which the problem of attribution will not be an obstacle. For example, the international coalition in Libya provided support to the rebel forces by weapons and training that acted as a surrogate for ground forces against the Gaddafi forces, while the alliance participated in the conflict through the airstrikes. At the same time, the use of proxy forces can provide the government with "plausible deniability", by which it refers to covert activities against another state in a way that the adversary state can disclaim responsibility with a measure of credibility. While any involvement that widens, prolongs, or increases a war's destructiveness is impermissible regardless of the just cause[478], however, in contemporary conflicts and unrest, armed attacks emanate from NSAs, and acting as proxies are a legal dilemma in many instances. The confusion such groups create is whether they are affiliated with another state, therefore acting as a proxy that could involve directly the state these groups

[477] Mumford A., Proxy Warfare, Policy Press, Cambridge 2013, p. 11.
[478] Pfaff A., Strategic Insights: Proxy War Norms, Strategic Studies Institute, The United States Army War College Press, December 2017, p. 3.

fighting on behalf, or be dealt with the case as an internal conflict or disturbance that is covered by different legal regimes.

The legal classification of such proxy operations concerning the legal rules that apply to them varies and intersects in jus ad Bellum and jus in Bello creating legal certainty for military leaders. For instance, a conflict between state and NSA under IHL is classified as NIAC even if another state was involved to support the host state, nonetheless, if the non-state actor is fighting on behalf of another state, then the conflict is considered IAC since effectively one state is fighting against another.[479] Although the international practice has accepted that the right of self-defense extends to attacks originated by such groups, the ICJ has stated that this right should not be used if the attack originates from within, and not outside the target's territory, since it would bring into play the territorial integrity of another state.[480] This means that if a State recruit proxies, it will be more difficult for the targeted state to attribute violence to its adversary, especially since states engaging in military conflict through proxy actors actively evade attribution under law. The previous statement meets the efforts of hybrid adversaries to advance one's security objectives at the expense of a rival using means beyond those associated with routine statecraft and short of means associated with direct military conflict[481], by which the use of proxies and state-controlled forces to undertake kinetic action below the threshold of all-out war has been an important tool and more pervasive in current hybrid cyber warfare environment.[482] The coercive tools range from:

- Disinformation and online troll farms by which the cyber domain is of crucial importance as it facilitates the acquisition of information via espionage campaigns, disruption of critical infrastructure, or the dissemination of disinformation specifically in election processes by which to day there are no commonly accepted or codified norms on the non-interference in other states' election process[483]. This has led in

[479] Somer J., Acts of Non-state Groups and the Law governing Armed Conflict, American Society of International Law Insights, 2006, Vol. 10, no. 21.
[480] ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion. 43 ILM (2004), 1009, para 139.
[481] Dalton M. and Shah H., Partners, Not Proxies, CSIS Briefs, May 2020, p.1. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20528_Dalton_NotProxies_Brief_v7.pdf
[482] Ibid, p. 3
[483] Mattessich W., Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting no Physical Damage, Colombia Journal of Transnational Law 54, 2016, no. 3.

numerous instances to clear violation of the spirit of the norm of non-intervention as a core principle of the UN Charter.[484]

- Terrorist financing and paramilitary provocations in an arena between routine statecraft and open warfare, what is the so-called grey zone. There are many cases in which states and NSAs can bear responsibility for the contribution to harmful activities that violate the international legal norms, that is mainly provided by the legal framework structured through the International Law Commission Articles on the Responsibility of States for Internationally Wrongful Acts (2001) (hereinafter the ILC Articles) that highlights the state culpability for the actions of their dependent proxy actors[485].

In the rise of the Ukrainian conflict, a heavily masked armed group with unidentified insignia, attacked and took over the parliament in Simferopol - the Crimean Peninsula in 2014. This armed group was named "Little green men" due to its members' green uniforms and veiled identity. Although the group raised the flag of the Russian federation over the parliament, Russia denied any relation to the group and considered them local self-defense groups.[486] Little green men are non-state armed groups that can conduct covert operations and impose power. The group's hybrid features expanded its success and ability to challenge the victim state from different legal perspectives:

- The ambiguity of group: The ability to mask its real identity and infiltrate in local community denying any relation with external State (Russia in this case). Considering the elements of armed attack from a ratione personae standpoint, such group obstructs Ukrainian response, as the ratione personae element considers that acts committed by state actors or groups sent by or on behalf of a State constitute an armed attack if these attacks can be attributed to that state. Similarly, the ICJ advisory opinion recognizes the existence of an inherent right of self-defense in the case of an armed attack by one State against another State.[487]

---

[484] Russia's interference campaigns in the 2016 US presidential elections by hacking the Democratic National Committee (DNC) and lacking sensitive documents. See "US Officially Accuses Russia of Hacking DNC and Interfering with Election," The Guardian, October 8, 2016. Another example is how pro-Russian groups released hacked emails and delayed by that the presidential elections' results in Ukraine 2014. See "Ukraine Election Narrowly Avoided 'wanton Destruction' from Hackers," Christian Science Monitor, June 17, 2014.

[485] Torossian B., Fagliano L., and Gorder T., Hybrid Conflict "Neither war, nor Peace", Strategic Monitor 2019, https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/hybrid-conflict/

[486] Online Article "Putin says those aren't Russian forces in Crimea" March 4, 2014. https://www.npr.org/sections/thetwo-way/2014/03/04/285653335/putin-says-those-arent-russian-forces-in-crimea?t=1590235318330&t=1609180949360

[487] ICJ Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Ibid. para 139.

- External power deniability: Russia has denied any official relationship with the group and any involvement in the conflict in Ukraine. Russia has successfully used international law on attribution to avoid any direct responsibility for the little green men activities. The effective and overall tests that are required by international law for the activity of NSAs to be attributed to a state are inadequate in many instances when it comes to hybrid operations.[488]
- Admittance after control: Russia has admitted that the Little Green Men were Russian "Spetsnaz"[489], but that was after one year of actual operations and the annexation of Crimea. Russia justified the involvement of these groups claiming that they were exercising self-defense in the protection of Russian nationals and Russian-speaking minorities in Ukraine.[490] The three-phased success of the Little Green men operation has delayed the determination of the identity, origin, and attribution needed to execute a self-defense response. This highlights the main strategy of a hybrid aggressor in using non-state armed groups to conduct operations under the threshold of armed attack of well-defined attribution.

So, states contemplating a relationship with NSAs involved for instance in cyber operations against another state can weaken the international legal architecture for assessing responsibility and imposing accountability statutes concerning such harmful operations. States are held accountable for the wrongful actions of the proxies they control, as Article 8 of ILC Articles states: "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is acting on the instructions of, or under the direction or control of, that state in carrying out the conduct."[491] Proxy hybrid NSAs that can disguise their real identity and use cyberspace, new technologies, and covert financing systems are highly challenging to any targeted state and the international law rules in concern. The legal dilemma is that either state has to consider such operations as traditional armed attacks and

[488] Explained in depth in section 4.2 of this chapter.
[489] Spetsnaz are special operations unit of the Russian military that includes the Russian Navy, Airborne troops, and FSB (Formerly the KGB).
[490] Russia has used the same justification during its intervention in Georgia following the conflict in south Ossetia. The UN rejected the justification based on the unnecessary and disproportionate use of force, but not the argument itself. The fact that many states do rely on such justification as a mean of self-defense. See Gray C., The Protection of Nationals abroad: Russia's Use of Force in Georgia, Constantinides and Zaikos eds., The Diversity of International law 2009, p. 133.
[491] Though these articles were not considered as binding treaty, yet they constitute part of wider binding framework of customary international law given that the ICJ has referred to them in its jurisdiction and states have widely accepted the norms they represent. See Responsibility of States for Internationally Wrongful Acts, International law Commission (ILC), 2001, Article 8.

respond to them under the law of armed conflict, or equate them to criminal activities and deal with them under domestic criminal laws. And currently, the prevailing view of states is the latter by which there is uncertainty over whether cyber-attack can qualify as an armed attack and due to the uncertainty of attribution of such attacks to a foreign power before responding with force[492].

According to the Tallinn Manual, a state bears international legal responsibility for a cyber operation attributable to it and which constitutes a breach of an international obligation[493]. The latter is a reflection of the ILC Articles of 2001 by which any cyber-attack carried out by a State's intelligence agencies or private contractors could qualify the use of force if the attack is attributable to the state. However, The Tallinn Manual expanded the rules of attribution adopted by the ILC Articles by considering that the right to self-defense could be exercised on the territory of another State in case the latter is unable or unwilling to take effective measures to repress cyber-attacks originating from its territory by on-state actors, while article 10 of the ILC articles stated that conduct of an insurrectional movement can be considered as an act of the State only if the movement becomes the new Government of the State, or if it succeeds in establishing a new state in part of a pre-existing state[494]. This can be seen in line with the opinion of the ICJ that justifies self-defense on the territory of another state only when the group's activities can be attributed to a State under the laws of attribution such as sending groups by or on behalf of a state which carries out acts of armed force against another state of such gravity that amount to an armed attack. Therefore, the Manual has widened the spectrum to the use of force against states that could have a dramatic impact on future conflicts to deter the ambiguity of cyber-attacks. Despite the disparity between existing international legal norms and the hybridity forms of conflicts, these norms that include state responsibility, non-intervention, and non-discrimination rules can be applied to hybrid campaigns if adapted, interpreted, and applied to cases that involve proxy or cyber operations despite the confusion that these operations impose at the state level and its international legal means.

2.3.3. The Ambiguity between Use of force in Self-Defense and Potential Armed Reprisal crafted by Hybrid Warfare

[492] Carr J., Inside Cyber Warfare, Responding to International Cyber Attacks as Acts of War, 2nd Edition, O'Reilly Media, December 2011.
[493] Tallinn Manual, Ibid., rule 6 p.29.
[494] Boulos S., The Tallinn Manual and Jus ad Bellum: Some Critical Notes, ResearchGate Publications, May 2017, p.8.

Initially, according to the 1934 resolution of the Institut de Droit International: "Reprisals are measures of coercion, derogating from the ordinary rules of international law, decided and taken by a state, in response to wrongful acts committed against it, by another state and intended to impose on it by pressure exerted through injury, the return to legality"[495]. Numerous scholars had commented on the legal basis of the institution of armed reprisals.[496] According to Yoram Dinstein, armed reprisals are forcible measures short of war taken by one state against another state, in which will be considered unlawful if not to rectify an initial wrongful act[497]. Reprisals, also known as proportionate countermeasures, provide another way for states to address illegal uses of force against them as an exemption that allow victim states to take normally unlawful actions against other states when they are violating their international obligations to the victim state.

In contemporary conflicts, armed reprisal is no longer acceptable, however HW could trigger a loophole that is vital when analyzing the threat hybrid adversaries can create in peacetime. The general prohibition in the use of force in the UN Charter prohibits any threat or use of force unless authorized by the Security Council under Article 42 and self-defense under Article 51, then the questions whether such prohibition covers armed reprisals or not were answered by the Resolution 2625 of the General Assembly that stated the following: "states have to refrain from acts of reprisal involving the use of force". Yet in the pre-charter era, reprisals were accepted as a lawful response to the use of force against a state to achieve redress by compensation and/ or to prevent or deter repetition of the unlawful act in the future. In the well-known Naulilaa Arbitration between Portugal and Germany in the aftermath of an attack by Germany on Portuguese territory in Africa[498], the arbitrators held that there must be three

[495] Institut de Droit International, Session of Paris 1934, Régime de Répresaillies en Temps de Paix, Article 1.

[496] Roberto Barsotti considered that: "the features which distinguish the customary right of reprisal are anything but clear and unambiguous", he stated that: "at the time when resort to war was unconditionally permitted, the need to define and distinguish between the single measures short of war was not felt, since their lawfulness was never in doubt. Thus, when the necessity to make this distinction arose (in consequence of the prohibition of war and even of the threat of use of force), it became apparent that there was some uncertainty as to the essential characteristic of the reprisal." See, Roberto Barsotti, 'Armed Reprisals' in Antonio Cassese edn., The Current Legal Regulation of the Use of Force, Martinus Nijhoff, Leiden 1986. Similarly Antonio Cassese has commented that: " The requirement whereby armed reprisals are lawful only to the extent that they constitute a reaction to a wrong committed by another State presupposes the emergence of a rule prohibiting forcible intervention, that is, any interference in another State by the threat or use of force…So long as such intervention was admitted, armed reprisals hardly made up a separate category, for it did not matter very much whether forcible measures short of war were to be labelled 'intervention' or 'reprisal'." Cassese A., International Law, 2nd edn., Oxford university Press 2005, p. 299

[497] Dinstein Y, War, Aggression and Self-Defense, Cambridge University Press 2005, 4th ed. p. 16

[498] Germany and Portugal had set up a Special Arbitral Tribunal after an incident in 1914 in which the Governor of German South-West Africa ordered reprisal attacks on Portuguese forts and posts after two German officers and an official were killed by Portuguese soldiers. The Tribunal found the killings were due to a misunderstanding,

requirements for a reprisal to be lawful: " A prior act contrary to international law; An unsatisfied demand for reparation to the alleged wrongdoer, The proportionality of the reprisal"[499]. The tribunal noted that: "Reprisals are illegal if they are not preceded by a request to remedy the alleged wrong. There is no justification for using force except in cases of necessity. Reprisals that are altogether out of proportion with the act that prompted them are excessive and therefore illegal. This is so even if it is not admitted that international law requires that reprisals should be approximate of the same degree as the injury to which they are meant to answer" [500]. Generally, reprisal involving the use of force is prohibited by the Charter, and that has been reflected by several scholars of international law. Reprisals are only applicable to coercive measures not involving the use of armed force, known today as counter-measures[501]. For instance, J Brierly noted that: "it is beyond argument that armed reprisals would be a flagrant violation of International Law" [502], while Brownlie considered that the unambiguous prohibition of forcible reprisals was finally accomplished by UN Charter[503]. Also, Cassese stated that: "armed reprisals are considered indisputably contrary to Article 2(4) of the UN Charter".[504]

The illegality of armed reprisal finds its roots in international law documents[505], and it is only admissible if it does not involve the use of armed force[506], by which reprisals carried by economic, financial, or other peaceful means are not considered a violation of the UN Charter. The International Law Commission (ILC) during the preparation of the Articles on State Responsibility, has addressed armed reprisals and dismissed any attempts to legalize such actions by stating the following: "The contrary trend, aimed at justifying the noted practice of circumventing the prohibition by qualifying resort to armed reprisals as self-defense, does not

---

which did not qualify as a 'violation of a rule of international law by the State against which the reprisals are directed'. See, Portugal v. Germany (The Naulilaa Case), Special Arbitral Tribunal, 31 July 1928 (1927-28) Annual Digest of Public International Law Cases, p. 527

[499] Zollman,J. Naulila 1914, World War I in Angola and International Law: A Study in Post-Colonial Border Regimes and Interstate Arbitration, 2016.

[500] The Naulilaa Case, Ibid. p. 527.

[501] O'Connell M.E., The Popular but Unlawful Armed Reprisal, Ibid. p. 339.

[502] Brierly J., the Law of Nations, Clarendon Press 1963, p. 415

[503] Brownlie, Principles of Public International Law, Oxford University Press 2008, p. 466.

[504] Cassese A., Return to Westphalia? Considerations on the Gradual Erosion of the Charter System in Cassese, The Current Legal Regulation of the Use of Force, p. 514.

[505] The International Court of Justice (ICJ) has occasionally commented on the legality of armed reprisals. In the *Nuclear Weapons* advisory opinion, the Court observed that:
Certain States asserted that the use of nuclear weapons in the conduct of reprisals would be lawful. The Court does not have to examine, in this context, the question of armed reprisals in time of peace, which are considered to be unlawful. See ICJ Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, General List No 95, para 46.

[506] Simma Br., the Charter of the United Nations: A Commentary, Oxford University Press 2012, 3rd Ed., Vol, I, p. 794.

find any plausible legal justification and is considered unacceptable by the Commission. Indeed, armed reprisals do not present those requirements of immediacy and necessity which would only justify a plea of self-defense"[507].

Similarly, the Security Council Resolution 270 condemned Israel's attack on villages in Lebanon as a violation of the Charter and previous resolutions by declaring that: "such actions of military reprisal and other grave violations of the cease-fire cannot be tolerated and that the Security Council would have to consider further and more effective steps as envisaged in the Charter to ensure against the repetition of such acts"[508]. For the interest of this chapter, analyzing the close relation and distinction between armed reprisal and use of force as self-defense is relevant for hybrid adversaries that tend to craft to create an ambiguity in the response to an armed attack due to the lack of the main factors such as an armed attack, necessity, and attribution. As the state might find itself under an attack of low intensity and drag itself to use force against another state with no clear evidence that such attack has crossed the threshold or whether the attacks were launched by a state or non-state armed group of transnational power. Although states might justify such actions as self-defense, however, it might fit more like an armed reprisal which is a violation of international law. For example, the USA launched a series of airstrikes against Libyan military sites aftermath of the terrorist bombing in Berlin, where two American service members were killed. And while the US justified this operation as self-defense under article 51 of the Charter[509], the case simply did not fit the requirements of self-defense, and counter-attacks lacked shreds of evidence of the necessity for military actions, therefore was condemned by the UN General Assembly[510]. Therefore, under contemporary international law, armed reprisals are no longer considered lawful, yet reprisals shall be understood as countermeasure that are proportionate , with limited aim and scope.

The ambiguity of actors and the transnational element of hybrid adversaries in contemporary conflicts is a challenge to states' response and ability to justify legally its actions, especially if for example cyber-attacks launched from the territory of a state by a non-state armed group based on the territory of another state (other than the state from which the cyber-attacks were

[507] ILC, Summary Record of the 242th Meeting of 21s July 1995, Yearbook of the International Law Commission, 1995, Vol. I, p. 297
[508] Security Council Resolution 270 of 26 August !969, para. 4
[509] Lobel J., The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan, Yale Journal of International Law 1999, vol. 24, p. 537, 548-49
[510] UN General Assembly Resolution 41/38 of November 20, 1986, para 2.

launched) that is unable or unwilling to stop their threat. This example highlights the challenging elements of HW when it comes to fluidity, fusion, and technological means to a single battlefield as it might lead to wrongful acts for it is wrong and immoral to transform the sense of injustice into vengeance[511]. According to Aurel Sari, the fact that legal thresholds are vulnerable to exploitation, underlines one of the enduring dilemmas of international affairs, especially that adversaries that are prepared and can combine subversive activities with the use of force falling below the level of intensity of an armed attack will advance strategic interest without provoking a forcible response from the targeted state. Therefore, the legal basis for responding to hybrid attacks must be clear, as one of the defining characteristics of hybrid attacks is the exploitation of legal gray areas. Response from the respective of international law to the use of force can be through the UN Charter, mainly Article 51 and the UN Security Council Chapter VII action[512], by which international law does not stand still and will be subject to further efforts to increase its resilience to exploitation and subversion[513].

On the other hand, international law provides several measures to counter hybrid aggression without requiring the use of force such as sanctions, financial protection, capacity building, cyber-defense, so there is ample legal basis for creative horizontal escalation to counter HW[514]. For example, if the state either instructs NSA to launch physically destructive or lethal operations against another state or exercises overall control over an organized armed group, it will find itself in conflict with the targeted state. Therefore, states contemplating a relationship with NSAs involved in hybrid campaigns against another state must tread very lightly because it weakens the international legal architecture for assessing responsibility and imposing accountability for harmful or physical operations. So, it is necessary to examine state practice when interpreting legal norms that lack absolute clarity, and by employing proxies, states effectively help hold the legal door open for other states to do likewise. For the same reasons, states must clearly articulate their position on the matter whenever it can be established that a state has resorted to a proxy to conduct harmful cyber operations. Silence will typically be interpreted as acquiescence, although that is technically a questionable conclusion as a matter of law. Only by objecting to such use based on a strict application of the law of state responsibility's rules on attribution can states hold the line against actions that weaken the

[511] O'Connell M.E., The Popular but Unlawful Armed Reprisal, Ibid. p. 349.
[512] A Multinational Capability Development Campaign Project, (MCDC Project), Countering Hybrid Warfare, MCDC February 2019, Info-box 5.2, p. 57
[513] Sari, A., Hybrid-Warfare, Law and the Fulda Gap, Ibid. (Complex Battle spaces.)
[514] MCDC Project, Ibid. p. 57

extant norms. This also concerns cyber operations that are below the threshold of use of force or that do not constitute physical damage by directly causing any death or injury or even destruction to infrastructure. In this matter, even though the San Francisco Conference rejected the Brazilian proposal that prohibition on the use of force does not extend to cover economic and political pressure, but that does not mean that all cyber operations do not fall under the use of armed force.

According to the ICJ in the Nicaragua case, even minor acts of interstate force fall under the general prohibition of art 2(4) of the UN Charter regardless if they qualify as acts of aggression or armed attacks entitling the targeted state to resort to self-defense and an exception to article 2(4)[515]. This relocates cyber-attacks in a gray area to UN charter, and neither opinio Juris nor State practice has provided clear criteria regarding the threshold at which such acts not causing death and injury must be regarded as prohibited under Article 2(4) UN Charter. Accordingly, it is agreed that cyber-attacks that cause injury or death of persons, even damage or destruction of property violates article 2(4) which is the prohibition to use force in international relations[516]. However, certain operations which do not have destructive or injurious consequences would still qualify as a use of force, according to the group of experts in the Tallinn Manual[517]. For instance, while the Tallinn Manual's experts agreed that the 2010 Stuxnet operations were of sufficient scale and effects to qualify as use of force, only some of the experts regarded Stuxnet as grave enough to qualify as an armed attack[518]. Yet, this right is protected by the principle of sovereignty and non-intervention in international law. Rule 1 of the Tallinn Manual stated that sovereignty empowers a state to exercise control over cyberinfrastructure and activities within its territory and protecting the cyberinfrastructure as well at its territory from any attacks[519]. But the problem was that this principle covers the territory, not the object targeted. Therefore, if the computer of a state is targeted on the territory of another state, then the sovereignty of the state where the computer is located will be breached[520]. On the other hand, the principle of non-intervention can be violated with any cyber support to groups in other states or by supplying malware to them, such acts would qualify as intervention by the state sponsor. This can be seen by the statement of the ICJ in the Nicaragua

[515] International law Commission, Report of the International Law Commission on the work of its Thirty-second session, 5 May–25 July 1980, Official Records of the General Assembly, Thirty-fifth session, Supplement No. 10, UN document A/35/10, 1980, p. 44
[516] Tallinn Manual, para. 8 of commentary to Rule 11.
[517] Ibid., para. 10 of commentary to Rule 11.
[518] Tallinn Manual, Ibid. n.3, p. 58.
[519] Micheal Schmitt & Liis Vihul, Ibid, p.60.
[520] Ibid

case[521]. In all cases, such attacks must be attributable to a state to be considered as a breach resulting in a state responsibility. In the same manner, hybrid actors that blend their non-state character with the cyber operations at the armed attack level of gravity that are not conducted or hardly attributed to any state is an unsettling challenge. There is little prospect for the establishment of a treaty regime to deal with the use of proxy cyber actors. States that turn to them will be hesitant to embrace such a regime and in the absence of their consent treaties do not bind them. The reality is that states can only shape the understanding of the current law through their practice.

To sum up, an armed attack once occurred allows the victim state to use force in self-defense, as understood in the Jus ad Bellum rules. It is though hard to distinguish between the use of force and armed attack which creates a gap between article 2(4) and Article 51 of the UN Charter, especially that all armed attacks are the use of force, but not all uses of force amount to an armed attack. A confusion that is considered a fertile environment for hybrid aggressors. Moreover, while the Jus ad Bellum is mainly concerned with what is required to justify going to war in the first place, the Jus in Bello focuses upon what may be done within war and against whom. The distinction between the two is very important for drawing a line between spheres of moral or/and the legal responsibility and the actual conduct of the war, also in understanding the challenge HW imposes to the related but discrete criteria of both. Therefore, the legal concepts of armed conflict and armed attacks are of particular interest to clarify the nature of hybrid war, and whether the aggression meets the threshold requirement of an armed attack as a manifest violation of the UN Charter in the use of armed force by a state against another state sovereignty, territorial integrity or political independence, by which the vagueness inherent in the concept of war is an essential feature of the nature of hybrid warfare. The unclarity and confusion that hybrid operations entail, can have an ontological nature by which it is arbitrary to the victim state to decide whether to consider the situation as an act of aggression or not and to draw the line between war and peace politically.

To conclude, as already established, HW's main legal implications are based on the fusion of multiple means and tools to a single setting that may erode the effectiveness of armed attack notion as these operations maintain a certain level that does not reach the armed attack threshold but bring same effects as a large-scale armed attack. Nevertheless, if analyzed and

[521] ICJ, Military and Paramilitary Activities in and against Nicaragua, (Nicaragua v. United States of America), 27 June 1986, p.14, para 242.

addressed separately, the armed attack threshold will be incompetent to encompass them. The reason why many scholars promote the accumulation of events theory is to consider that even low-intensity operations if accumulated together can reach the threshold of an armed attack. In the end, even if HW is not as novel as some argue, however, the contemporary threats are rather different than those we experienced in the 20th century, raising questions about the suitability of certain normative frameworks that are supposed to govern it.

2.4. Exceptions Outside of the UN Charter System: Humanitarian Intervention and Responsibility to Protect Doctrine (R2P)

As explained previously, under the UN Charter states are prohibited to use force except when exercising their inherent right to self-defense or where the SC authorizes a state or group of states to respond to a threat to international peace and security. However, it was highlighted that the norms concerning the use of force tend to expand such as to justify military actions that include pre-emptive strikes or response to terrorist attacks or against states that allegedly harbor terrorists. Similarly, the SC has authorized actions that even expanded further in response to matters that were before seen as purely domestic. These actions by the SC are what are so-called "humanitarian interventions" were mostly authorized under Chapter VII of the Charter, by which it should not be confused with new justifications for the use of force without such authorization. The humanitarian intervention does not necessitate a link between the victims and the intervening states which emphasizes the need for international approval and support.[522] Important to note, that the SC veto system can block such authorizations, as demonstrated by Russia's failure to approve the use of force against the Assad regime, which was an obstacle for the international community to intervene in humanitarian crisis when UN authorization is impossible. A clear separation must be taken into consideration between humanitarian intervention/ R2P and the protection of nationals abroad or diplomatic protection. The latter is applies to the protection of a state's nationals abroad from injury suffered as a result of a breach of international law, such as denial of justice, imprisonment without trial, discriminatory or arbitrary expropriation, nationalization or confiscation without compensation. Diplomatic protection must be exercised by lawful and peaceful measures, that

[522] Lillich R., Forcible Self-Help by States to Protect Human Rights, Iowa Law Review, 1967, Vol. 53, p. 332.

includes all the lawful procedures employed by a State to inform another State of its views and concerns, including protest, request for an inquiry or for negotiations aimed at the settlement of disputes. Other means cover dispute settlement such as negotiations, mediation, and conciliation to arbitral and judicial dispute settlement. The use of force, is not permissible method for the enforcement of the right of diplomatic protection.[523]

The international community has attempted to reshape the law on the use of force through Humanitarian intervention to prevent a humanitarian catastrophe, and is considered permissible under international law once it meets the legal requirements. The rule highlights that if a government fails to protect the rights of its people, the international community is entitled to intervene. However, there are debates around the permissibility of the use of force by states acting individually or collectively without the UNSC authorization to prevent or stop a humanitarian catastrophe. While the UN Charter does not include such a rule, however, some states now maintain its applicability. On the other hand, some state practice tend to justify their interventions by misusing the law under irrelevant justifications, similar to what we explained at the beginning of confusion between humanitarian intervention and protection of nationals abroad. Russian Federation, for instance, considered that it has intervened in Ukraine under international humanitarian law, to defend the rights of Russian-speakers living aboard[524], under what is so called the doctrine of protection of nationals, that is controversial doctrine to the use of force in international law. Such behavior is an example of the abuse of the law, as certain requirements must be met to conduct a limited rescue operation for nationals of a country that are under attack or territorial state where they reside is threatening to use lethal force against them, such as operations to save diplomatic staff or hijacking a civilian airplane and were conducted in critical situations (the 1980 Tehran hostage situation, the 1998 air strikes in Sudan and Afghanistan, the 1975 Mayaguez incident…etc.) therefore, such intervention does not even fit the protection of nationals abroad doctrine. While there is no credible evidence of deliberate attacks on persons of Russian ethnicity by Ukrainian government forces , justifying the use of force fails to meet the necessity of such behaviour and amounts to coercive intervention. Also for Russia to have the right to intervene under IHL, it must prove that there was an urgent humanitarian catastrophe it seeks to avert and why there is no alternative to its action, it should

[523] United Nations, Draft Articles on Diplomatic Protection with commentaries, 2006, available at: https://www.refworld.org/docid/525e7929d.html

[524] Buckley E. and Pascu I., "NATO's Article 5 and Russian Hybrid Warfare", Atlantic Council 17 March 2015, http://www.atlanticcouncil.org/blogs/natosource/nato-s-article-5-and-russian-hybrid-warfare

not act by stealth and revert the big lie, denying that its forces are engaged denying that its missile units shot down the Malaysian airliner MH17, and pretending to be the peacemaker[525]. Similar arguments fit Humanitarian intervention justification to attack Ukraine.

Humanitarian intervention originates from the State's right to self-defense that subsumes the defense of citizens of another state. If the population was targeted in extreme cases such as genocides conducted by the population's government or military forces, then it is assumed by some states that the right to Humanitarian Intervention applies. Humanitarian intervention can be narrowly understood as a reaction to an occurrence of the crime of genocide or crimes against humanity, as a widespread and systematic violations of fundamental human rights that can justify the use of armed force.[526] Handful of cases that relied on this doctrine had in common that the use of force was used in the context of large-scale and serious violations of core human rights (NATO intervention in Kosovo 1999, Vietnam in Cambodia 1978, and Tanzania in Uganda 1978), however not any of these interventions were seen as legitimate at the time they were conducted, nor they relied on humanitarian intervention justification. Although they were condemned but they served the purpose of halting a human catastrophe.[527] Legally speaking, a foreign state cannot invoke the collective right to self-defense in aid of the population under attack, as this will be a violation of Article 2(4) and the international law grants the right of individual and collective self-defense in the case of an armed attack on a warship, but not in the case of an armed attack by a government against its population.[528] Such a right is only granted by the Security Council within the collective response by the international community to aid the civilian population against its government in extreme cases. But following the recent developments, in particular the Syrian conflict, it was seen that this principle cannot merely rely on the UNSC authorization when one state can tie the hand of a collective aid. For instance, the International Commission on Intervention and State Sovereignty established by Canada stated the following: "It is a real question in these circumstances where lies the most harm: in the damage to international order if the UNSC is bypassed or in the damage to that order if human beings are slaughtered while the UNSC stands

[525] Buckley E. and Pascu I., Ibid.
[526] Cassese, Ex iniuria ius oritur: Are we moving towards international legitimation of forcible humanitarian countermeasures in the world community?, European Journal of International law, 1999.
[527] Gill T., Remarks on the Law Relating to the Use of Force in the Ukraine Conflict, Lieber Institute , March 9, 2022.
[528] Kress C., On the Principle of Non-Use of Force in Current International Law, Just Security, September 2019, https://www.justsecurity.org/66372/on-the-principle-of-non-use-of-force-in-current-international-law/

by"[529]. So, as stated the trigger event for humanitarian intervention is violation of core human rights amounting to genocide (that requires a "special intent or dolus specialis" to destroy a specific group in whole or in part on the basis of race, religion, nationality, or ethnicity), crimes against humanity, or serious large-scale violation of the LOAC that would amount to war crimes. Unilateral humanitarian intervention continues to be considered unlawful as there is no state practice or opinio Juris that would modify existing norms.

In other words, although humanitarian intervention became acceptable practice in particular circumstances, yet it is not an established exception and it does contradict the non-intervention principle and challenge the authority of the UNSC if established without its authorization. As in 1990, states were divided between those who were in favor of humanitarian intervention and those who viewed such a doctrine as an indefensible infringement upon national sovereignty. Nonetheless, humanitarian interventions must be employed after all other non-forcible actions fail (diplomatic means, sanctions, negotiations), according to article 33 of the UN Charter. And if the military force is deemed necessary, then it is only the SC that must authorize, otherwise, such actions will be abused. That will create the needed balance between state sovereignty and human rights protection by considering humanitarian intervention as a last resort, in accordance with the UN Charter.

After the end of the Cold war in 1990 and the outbreaks of intra-state conflicts, the first cases for applying the concept of humanitarian intervention were in Somalia and Kosovo where the two states were facing brutal NIACs in 1992. The changing nature of warfare and the recurrence of intra-state conflicts have deepened the challenges with regards to the protection of human rights and the principle of sovereignty, and have led to believe that it would be impossible to find consensus around any set of proposals for military intervention that acknowledged the validity of any intervention not authorized by the UNSC or the General Assembly.[530] Taking into account the recent military invasion of Ukraine by Russia, any justification based on humanitarian intervention falls short from the requirement indicated

[529] Report of the International Commission on Intervention and State Sovereignty, The Responsibility to Protect, ICISS, December 2011, p. 55.

[530] The International report on intervention and state sovereignty (ICISS), considered that: "But that may still leave circumstances when the Security Council fails to discharge what this Commission would regard as its responsibility to protect, in a conscience-shocking situation crying out for action. It is a real question in these circumstances where lies the most harm: in the damage to international order if the Security Council is bypassed or in the damage to that order if human beings are slaughtered while the Security Council stands by." See, the ICISS, The Responsibility to Protect, Ottawa International Development Research Centre, December 2001.

above. There has been no evidence that Ukraine has conducted a policy of genocide against the Russian speaking population in Ukraine. Moreover, the scale of the invasion employed by Russia in the territory of Ukraine is in no way proportionate to the actions taken by Ukraine to restore control over the self-declared territory in Donbass region. The votes of the 11th Emergency special session of the UN General Assembly on 2nd of March 2022, reaffirm that Russia has blatantly violated the UN Charter on the prohibition of the use of force, and dismissed indirectly any abuse of law by justifications that do not meet any legal requirements to justify the use of force in international relations.

2.4.1. From "Right to Intervene" to "Responsibility to Protect (R2P)"

Following the recurrent failure of the international community to protect populations in conflicts from the atrocity of conflicts, and the refusal of interventions unauthorized by the SC (Kosovo case), an evolution on the legality to use force in international relations has been highlighted by a more advanced version of what is known by the "Responsibility to Protect (R2P)", a doctrine that was developed by an International Commission on Intervention and State Sovereignty (ICISS)[531]. The doctrine highlighted that: A state is primarily responsible for the protection of its citizens or if it is not able or unwilling to do so, this is the responsibility of the international community through the Security Council for it to fall under lawful use of force. The report of the ICISS that was published in December 2001 and endorsed by the UN High-Level Panel on Threats, Challenges, and Change in 2004[532] and 2005[533], has proposed a shift from the "right to intervene" to "responsibility to protect". The World Summit Outcome Document in 2005 has also committed to the principle of the R2P doctrine.[534] The document stated that states are under a responsibility to protect their population from genocide, war crimes, ethnic cleansing, and crimes against humanity, also declared their preparedness to take timely and decisive action, under the UN Charter and in cooperation with relevant regional organizations, when national authorities manifestly fail to protect their populations. A shift that is seen to be based on justification of regional organizations or coalitions using force to prevent mass atrocity crimes and intervene in humanitarian crisis when the SC is unable to act in a

[531] Ibid.
[532] Report of the Secretary-General's High-Level Panel on Threats, Challenges and Change on A More Secure World: Our Shared Responsibility, 2004, (A/59/565).
[533] Report of the Secretary-General on In Larger Freedom: Towards Development, Security, and Human Rights for All (A/59/2005)
[534] World Summit Outcome Document 2005, Resolution adopted by the General Assembly on 16 September 2005, https://undocs.org/A/RES/60/1 , para. 138-140.

timely and appropriate manner. The R2P doctrine sets certain criteria that need to be met. The criteria include the following: "A prima facie case must be established that atrocity crimes are occurring or are about to occur. Peaceful options must have been exhausted. The Security Council is unable to act in a timely and appropriate manner. Any military force used must be limited to low-intensity options designed to protect civilians and must be carried out in such a way as to limit collateral damage. The use of low-intensity military force must be authorized by a legitimate authority, which could include UN General Assembly, regional organizations, or international Coalitions. The intervention must come at the request of credible opposition groups that represent victims of atrocity crimes and shall be done collectively by members of the international community, and the use of force should be followed up with or integrated into a larger strategy and policy for addressing the humanitarian crisis."[535]

Accordingly, R2P offered a wider opportunity for the use of military force than the one offered by Humanitarian intervention that is based on the SC authorization. That would allow the interventions outside of the Charter system to protect the population when the SC has failed to or unable to do so. It is important to highlight that R2P provides exclusively measures for military intervention in case of an intra-state conflict that is within sovereign jurisdiction. According to R2P, states must act to prevent mass atrocity crimes and protect all populations from risks related to their occurrence. When states lack the capacity to take such measures, the international community has a responsibility to aid by taking the necessary measures. For example, the ICISS report and the UN Secretary-General Kofi Annan, in his report "In Larger Freedom 2005", proposed five "precautionary principles" or "criteria of legitimacy" to help guide possible military action under the UN Charter:[536]

1- "Seriousness of harm. The threat of atrocities must be clear and extreme enough to justify military force;
2- Proper purpose. The central purpose of the intervention must be to prevent or halt suffering;
3- Last resort. Military force must be the last resort with every reasonable non-military option having been explored;
4- Proportional means. The scale and duration of military action must be commensurate with the ends sought;
5- Balance of consequences. Is there a reasonable chance of success in averting the threat of atrocities without worsening the situation?"

[535] Williams P. and Pearlman S., Use of Force in Humanitarian Crises: Addressing the Limitations of UN Security Council Authorization, American University Washington College of Law, 2019, p. 216-217.
[536] The responsibility to Protect: A background briefing, 14 January 2021. Available at: https://www.globalr2p.org/publications/the-responsibility-to-protect-a-background-briefing/

R2P is not yet a rule of customary international law, but has its basis upon existing legal foundations, including the Genocide convention, and therefore can be described as an international norm. Once such a norm gain widespread usage, and not only formal acceptance as adopted in 2005 World Summit, it can become part of customary international law. R2P has been invoked in multiple UNSC resolutions, in situations such as Central African Republic, Mali, DRC, Somalia, threats to international peace and security caused by terrorist acts. The doctrine was considered following the mass atrocities in Libya, the resolution 1973 of 2011 authorized member states to use all necessary means to protect civilians and civilian-populated areas from the Qaddafi governmental forces that were advancing and threatened large numbers of civilians. On the other hand, the R2P failed in the Syrian crisis due to the Russian involvement in the conflict. Russia and China have jointly vetoed at least eight drafts of UNSC resolutions with R2P language over Syria[537] which combined with the mixed nature of the conflict, has led to a dead-end to the R2P doctrine to be enforced.

To conclude, despite the development in the justifications to use force in international relations as an exception to the exceptions in the UN Charter, the shortcomings in the humanitarian intervention are mostly regulated now and applied under R2P that plays an important role in keeping the balance between the principle of sovereignty and human rights. They also have expanded the opportunity of intervening to stop atrocities in intra-state conflicts that are increasing through HW means and the role of NSAs. States tend to deal with such situations based on their interest by either considering it a NIAC with more rights to use armed force under IHL. Nonetheless, R2P has faced the same problems as humanitarian intervention particularly due to the lack of resources and political will, such as in the case of Syria. In addition, though the doctrine has certain criteria that must be met, it still would allow some states to engage in lawfare by exploiting the legal conventions for strategic interests. For example, Russia has used the R2P language to justify unilateral incursions into Georgia and Ukraine, while having little to do with protecting vulnerable populations. Therefore, conceptual development for the concept is needed, as new atrocities and threats are arising, a broad international consensus about how to respond in the context of R2P is vital. Though this is not covered in the scope of our thesis, nonetheless the R2P doctrine in the contemporary hybrid nature of conflicts must be carefully implemented and assessed to avoid an over-extended

[537] Babbitt E., Responsibility to Protect: Time to Reassess, Journal of Human Rights Practice, 2017, Vol. 9, pp. 431, 433.

interpretation. Yet, R2P brings up a big hope for a world free from genocide, war crimes, ethnic cleansing, and crimes against humanity.

3. Legal Basis of the Attribution of International Responsibility to a State

Under International law, to establish the responsibility of states for internationally wrongful acts, two elements are identified. The first is chargeability (attribution) of the internationally wrongful act to the State (subjective element), and the second is that the conduct must constitute a breach of an international legal obligation in force for that State at that time (objective element). Along with the existence of a breach of a legal obligation, attribution, therefore, is one of the constitutive elements of an internationally wrongful act of a State. Attribution denotes the operation of attaching a given action or omission to a State under International law. In attributing wrongful acts to the state, it shall be taken into account the identification of the connection between the persons engaged in the conduct and the State. The latter was confirmed by the Iran-US claim tribunal that stated: "to attribute an act to the State, it is necessary to identify with reasonable certainty the actors and their association with the state."[538]

Furthermore, state responsibility covers the legal consequences of a state's violation of international law, a major body of customary international law, by which states are responsible for their internationally wrongful acts to other states they have caused harm. However, for this chapter, discussions will focus on attribution and not the entire characterization of conduct as internationally wrongful. Particularly, as HW's main challenge is lack of attribution through NSAs and cyber means.

The responsibility of a State is engaged if the actions of its agents or groups attributed to it, constitute internationally wrongful acts in violation of its international obligations. In this regard, the rules of attribution under international law are reflected in the International Law Commission's Articles on State Responsibility (ILC Articles) which have been recognized as reflecting customary international law, and it has led to the systematization of a widely accepted set of secondary attribution rules. The rules of attribution under the ILC Articles

[538] Kenneth Yeager v. The Islamic Republic of Iran, Iran-U.S. C.T.R. of 1987, vol. 17, p. 92, at pp. 101-102.

respond to normative criteria and not merely to a factual relation, and it is for the international law to determine whether or not conduct can be attributed to a State.

The attribution concept is more complex when the conduct of private persons cannot be legally linked to a state, which protects a state from being held international legal responsibility unless certain conditions are met. Taking into consideration that responsibility will be attributed if the state either acknowledges and adopts the conduct of the non-state actor as it is own, or it directs or controls the non-state actor. The rules that are specified in the Draft Articles on Responsibility of States for Internationally Wrongful Acts (hereinafter DARSIWA) are cumulative but are also limitative. So, in the absence of a specific undertaking, a state is not responsible for the conduct of persons or entities in circumstances not covered by these conditions[539]. These conditions or rules in the DARSIWA consist of the following:

- Actions of persons directed or controlled by the state, if such actions are under the instructions of, the direction or control of that state in carrying out the conduct[540].
- The person is empowered to exercise elements of governmental authority[541]. Such condition applies too in case of actual absence of government and in circumstances such as to call for the exercise of those elements of authority[542]
- The conduct of persons is acknowledged and adopted by a state as its own, which is not so common in actions that violate international law[543].
- Actions conducted by an insurrectional, movement, or others, which succeed in establishing their state, when such actions are attributed to their newly established state[544].
- The person acts as an organ of a state and in the capacity of this organ. The state organ is intended in the most general sense and no distinction is made for this purpose. Thus, in the Salvador Commercial Company case, the court stated that: "A State is responsible for the acts of its rulers, whether they belong to the legislative, executive, or judicial department of the Government, so far as the acts are done in their official capacity."[545]

[539] DARSIWA, Ibid. Ch. II, Commentary para. 9.
[540] DARSIWA, Ibid. Art. 8.
[541] Ibid. Art.8
[542] Ibid. Art.9
[543] Ibid. Art.11
[544] Ibid. Art.10
[545] Salvador Commercial Company, UNRIAA, vol. XV, no. 66, 1902, p. 477. See also the ICJ, In Difference Relating to Immunity from Legal Process of a Special Rapporteur of the Commission on Human Rights, it stated: "According to a well-established rule of international law, the conduct of any organ of a State must be regarded as an act of that State. This rule … is of a customary character", p. 87, para. 62.

Similarly, In the Tellini case in 1924, the special committee of jurists stated that: "a State may be held responsible for the criminal acts of NSAs when it neglects to take all reasonable measures for the prevention of the crime and pursuit, arrest and bringing to justice of the criminal."[546] In this matter, it requires acts that breach an international obligation and definite attribution of such acts to the accountable state[547]. International law requires states to immediately cease the offending conduct, comply with required duty and make full reparation[548]. Yet, in a cyber context, the ability to attribute the attacks to perpetrators due to the anonymity through NSAs is more complex particularly due to the high threshold for establishing states' "strict" or "effective" control over proxy actors.

To sum up, the ILC articles provide a legal framework for understanding state responsibility for the actions of their dependent proxy actors. While such proxy actors might lack the international legal personality necessary for accountability, nonetheless the ILC articles though not legally binding, stem from the customary international law. Therefore, it represents a wider norm of state accountability for the wrongful actions of the proxies they control. It is understood that with regards to the conduct of organs to the State, it includes any organ irrespective of whether they exercise legislative, executive, or judicial, by which it includes any entity which has that status per the internal law of the State. According to Crawford, the term "includes" means that it cannot be limited to those who have the condition under internal law. That will not give the chance to states to avoid attribution of organs based on the fact that they lack such status under internal law.[549] On the other hand, the principle of responsibility of the state for wrongful acts includes persons or entities that act on behalf of the state or non-state body.

3.1. Attribution and Hybrid Warfare

Contemporary conflicts, in particular hybrid ones, are controversial and challenging to modern international law. This has been seen through the indeterminacy of state practice and opinio

[546] Tellini case 4, League of Nations O.J. 524, 1924
[547] Responsibility of States for Internationally Wrongful Acts, United Nations, Article 2.
[548] Ibid., para. 1 of chapeau to Chapter II
[549] Crawford J., The International Law Commission's Articles on State Responsibility: Introduction, text and commentaries, Cambridge University Press, 2002, p. 89.

Juris in response to modern technologies such as proxy wars, cyber-attacks, and unmanned aerial vehicles (Military drones as an example) that created a legal gray zone or legal indeterminacy. However, as explained before, a state being targeted by a NSA from the territory of another state does not give the right to state to violate the sovereignty of another state if such attack was not attributed to the state from which NSA is operating from, thereby not holding responsibility. So, for a state to be held responsible for activities by NSAs, several rules and conditions are articulated by the ILC in its Articles on State Responsibility for Internationally Wrongful Acts, and by the ICJ in the Nicaragua and Genocide cases[550].

Commonly, a state conducts an internationally wrongful act when actions or omissions are attributable to the state under international law and constitutes a breach of an international obligation[551]. Also, attribution of conduct to the state as a subject of international law is based on criteria determined by the former and not on the mere recognition of a link of actual causality[552]. Moreover, ILC articles are secondary rules that apply in case of any breach of an international obligation by a state, without ruling on the characteristics or substance of the primary obligation which is violated[553]. However, under international law, the performance and activities of public institutions (e.g. police) are attributed to the state, even if they are considered as autonomous and independent of the executive government under the state's national law.[554] Moreover, a state to which the cyber operation of NSA is attributable is legally required to do all possible means to cease these operations[555], otherwise various actions set forth for countermeasures in the law of state responsibility can be applied[556].

To constitute a violation of a rule of public international law which could constitute an internationally wrongful act, the attack must be attributed to a state or a group of identifiable individuals operating on behalf or under the direction of a state, and that will require a fairly high degree of certainty. In cyberspace, for instance, such groups of individuals are known as

[550] Milanovic, M., Self-Defense and Non-State Actors: Indeterminacy and the Jus ad Bellum, Blog of the European Journal of International Law, February 2010.
[551] International Law Commission (ILC), Draft Articles on Responsibility of States for Internationally Wrongful Acts, (hereinafter DARSIWA), November 2001, Supplement No. 10 (A/56/10), Art. 2.
[552] Ibid. Ch. II, Commentary para.4.
[553] Alvarez Ortega E., The Attribution of International Responsibility to a State for conduct of Private Individuals within the Territory of Another State, INDRET Barcelona 2015, p.3.
[554] DARSIWA, Ibid. Ch. II, Commentary para. 6
[555] Micheal Schmitt & Liis Vihul, Proxy wars in Cyberspace: The Evolving International Law of Attribution, Fletcher Security Review | Vol I, Issue II Spring 2014, p. 58.
[556] Responsibility of States for Internationally Wrongful Acts, Ibid, article 49-54

patriotic hacktivists that use cyberspace legally or illegally to express ideology or political agenda[557]. One of these examples is the "Anonymous Group" which consists of a mixed group of people ranging from script kiddies to professional black hats connected through a variety of non-mainstream social networking services such as "4chan" and "711chan" forums, that involves a type of war on the Scientology, various support actions during the Arab Spring and attacks on companies such as Louis Vuitton, Sony, Mastercard, and U.S. Government websites[558]. However, more sophisticated groups are cyber militias that are able and willing to use cyberspace for political objectives by utilizing communication channels covertly by hiding their true identities. Such militias could consist of mercenaries that take part in military actions in cyberspace and are loosely connected in real life, keeping their identity and link very vague.[559]

Correspondingly, states benefit from employing NSAs in cyberspace operations for the following reasons:

- The attacker gains the initiative and element of surprise by benefiting from plausible deniability;
- The attacker can choose a target and attack vector with low cost, even by using one computer to launch the attack, while the defender has to efficiently shield all its cyber-resources;
- The attacker can determine the scale and duration of an attack;
- Exploit legal uncertainties by which even if the attacker was identified by the defender the lack of applicable international laws covering cyber-operations creates legal ambiguity;
- Attackers can recruit proxies such as hacktivists, criminal groups, or even cyber militias making the counterstrike negligible.

The indirect approach of warfare is more efficient than direct ones, by which hybrid warfare relies on covert and indirect means through the use of asymmetrical warfare or cyber means. A similar line of argument could apply to attribution, as one of the core elements of HW strategy is using all available methods and means to evade the establishment of a link of

---

[557] Handbook on Maritime Hybrid Threats – 10 Scenarios and Legal Scans, Hybrid CoE, p. 19, https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Handbook-on-maritime-threats_RGB.pdf

[558] Bernstein M.S., Monroy-Hernandex, Harry D., Ande P., Panovich K. and Vargas G., An Analysis of Anonymity and Ephemerality in a Large Online Community, Fifth AAAI Conference on Weblogs and Social Media, July 2011.

[559] Ottis R., Proactive Defense Tactics On-Line Cyber Militia, in the proceedings of the 9th European Conference on Information Warfare and Security (ECIW 2010) Thessaloniki - Greece, July 2010.

attribution for hostile acts and to prevent the applicability of existing legal regimes. Although, the ICJ has resisted the notion of recognizing the possibility of self-defense against NSAs and lowering the threshold of attribution for jus ad Bellum, yet the role of attribution certainly continues to play a central role for state responsibility with regards to the challenging features of HW explained before. Such means find their refuge in relying on proxy military forces or non-state armed groups (unmarked or marked), cyber-attacks, and the instrumentalization of laws. Attribution functions to create a linkage between human conduct and a state, and while Article 51 is silent on any attribution rules, the ILC Articles on State Responsibility, which codifies customary law is fundamental for identifying and analyzing this bond.

The difficulty of attribution is the main challenge for nations in reducing the overall insecurity coming from the above features, which leads to legal difficulties when it comes to the response by the targeted state to such acts and tools structured to protect the anonymity of perpetrating state or non-state actor. Similarly, is the misattribution or what is so-called "False Flag", that can be used as propaganda or deceptive tactic. According to Article 2(4) of the UN Charter, only states are involved in using or threatening to use force, therefore such use of force must be attributed to a state legally. In international law, acts will be attributed to a state if they are performed by persons or entities acting on behalf of a state or under its command, while others who are not acting, in the same manner, cannot be regarded as state agents, yet can be described as NSAs. Therefore, in theory, any counterattack against a non-state actor acting from the territory of another state, in the absence of the targeted state's consent and its responsibility to such act, violates the prohibition on the use of force by disrupting the territorial sovereignty, integrity and its right to non-interference.

International law dictates that a state may not allow knowingly its territory to be used for acts contrary to the rights of other states and this applies to cyberinfrastructure too[560]. According to the individual attribution to a state, it must be determined based on the international law of state responsibility which is regulated by the Draft Articles on Responsibility of States for Internationally Wrongful Acts 2001 (hereinafter "DARSIWA")[561]. In this matter, some state agents carrying such attacks can be either government agents "de jure", which un-controversially constitutes attribution to a state, or private contractors "de facto agent"[562]. So, the responsibility of a state is thus limited to acts of its organs and agents exercising public

[560] Tallinn Manual, Ibid, Rule 5 and its commentary.
[561] UN General Assembly resolution A/RES/56/83 of 12 December 2001 and its annex
[562] Nils Melzer, Ibid. p. 10.

authority[563]. Nothing in Article 2(4) prohibits directly the NSAs and use of cyber operations which may be relevant according to IHL and International Criminal law, but the support and sponsoring of state to such groups can amount indirectly as a use of force violating by that Article 2(4) and the principle of non-intervention. This was noticed by ICJ in the *Nicaragua Case*, by which it ultimately concluded that the relation between the United States and the Contra rebels did not qualify as a de facto agency but that the United States' conduct under review constituted "indirect use of force"[564]. Therefore, the attribution of a non-state actor to a state will make it responsible internationally based on such assistance.

In this context, the attribution of NSAs to a state is only established when such actors are acting under the direction or control of a state[565]. This highlights the legal complexity of HW concerning attribution and state responsibility. For example, lawfare might misuse the fact that applicable law prescribes a certain threshold for activation of the right to self-defense or countermeasures. Similarly, low-scale operations fall below the threshold and thus in a bad faith deprive the adversary of their rights to respond lawfully[566]. HW seeks to exploit such legal threshold of an armed attack, that is not novel as agreed before, but its challenging elements considered in this research, thrive on these thresholds, due to technical, legal, and strategic reasons that will be subject to great uncertainty, debate, opacity, and lack of verifiability.[567] For example, attacks on Estonia, in which the information about the source of the attack on the Estonian computer system took months to assemble, and an ultimate responsibility on the state or actor behind these attacks through directing or encouraging remains disputable. This haziness surrounding cyber-attacks and NSAs with regards to the difficulty in reaching an agreement on legal judgment, brand them as an appealing weapon to some states.

Nevertheless, attribution of a cyber-attack to a state is a key element in building a functional legal regime to mitigate such attacks. The key problem is that states do not operate through formal state bodies in cases of cyber-attacks, but rather they use NSAs that are less visible, more remote, and offer plausible deniability. This creates both a factual and legal attribution

[563] Lanovoy V., Ibid. p.573.
[564] International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), 1986, p 115, 205, 247
[565] Articles on State Responsibility, Ibid, paras. 2-3 of Chapeau to Chapter II.
[566] Sari A., Legal Aspects of Hybrid Warfare, Lawfare Blog, October 2015, available online https://www.lawfareblog.com/legal-aspects-hybrid-warfare
[567] Waxman M., Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), The Yale Journal of International Law, 2011, Vol. 36, p. 443

challenge to this type of attack[568]. According to the API, attacks mean acts of violence against the adversary whether defensive or offensive[569]. Therefore, acts of violence do not necessarily require the use of kinetic violence but include cyber operations as well. The Tallinn Manual affirmed that cyber operations may constitute unlawful uses of force if they are attributed to the armed forces of a state or if their effects mimic those of traditional military operations[570]. Yet, a state is allowed to use force in self-defense only in response to an armed attack (most grave use of force), but it is unlikely that acts of cyber espionage focused primarily on gathering intelligence or data could be ever characterized as an armed attack under this definition[571].

Although the conditions above highlight the activities of persons or secessionist entities that identify the attribution criteria, yet they did not explain the threshold of such relationships and what could be considered as such. However, the opinio Juris has developed several types of attribution tests based on the conditions drafted by the DARSIWA. The first two standards introduced by the ICJ in the Nicaragua case are "Strict control and Effective Control" which was found to be extremely difficult to establish an effective control by the outside power over individual operations or activities of the secessionist entity. While the ICTY has introduced a lower degree control test, the "Overall Control test" in the Tadić case that depended on whether the acts of the armed forces of the Bosnian Serb secessionist entity within the territory of Bosnia and Herzegovina could be attributed to an outside power. However, it is important to examine whether any of the following tests can assess the HW concept while dealing with attribution.

3.2. Effective and Overall Control Tests

3.2.1. Effective Control Test

The ICJ in the Nicaragua case considered that control results from dependence that creates the potential for control.[572] The following test was produced in the Nicaragua case that dealt with

[568] Finlay L., Why International Law is failing to keep pace with technology in preventing cyber-attacks, available online:
https://www.murdoch.edu.au/news/articles/why-international-law-is-failing-to-keep-pace-with-technology-in-preventing-cyber-attacks
[569] ICRC, Protocol I, 8 June 1977, Article 49.
[570] Tallinn Manual on the International Law Applicable to Cyber Warfare, Ch. 1, Michael Schmitt ed. 2013.
[571] Finlay L., Ibid.
[572] ICJ., Nicaragua v. United States, Ibid., para. 277.

the question of whether violations of IHL committed by private individuals "the contras" during the Nicaraguan civil war could be attributed to the United States and later the test was elaborated in the Genocide case. Firstly, the effective control was applied by the Nicaragua case court (hereinafter "the court") in cases where there is evidence of partial dependency on outside power, by which the court stated that "for a conduct to give rise to the legal responsibility of the United States, it would in principle have to be proved that that State had effective control of the military or paramilitary operations in the course of which the alleged violations were committed."[573]. The court considered that it applies on situations when the persons are being directed or controlled by a third state as codified under Article 8 of DARSIWA[574], inter alia, from the provision of financial assistance, logistic and military support, the supply of intelligence, and the selection and payment of the leadership of such groups or entities[575]. Partial dependence does not allow the court to consider the entity or NSAs as a de facto organ of the outside power, but rather the responsibility of conduct will be established on a case-by-case basis[576]. For example, the court on the question of whether the conduct of the contras was attributable to the US to hold the latter generally responsible for breaches of IHL committed by the contras, considered that: "The U.S was responsible for the planning, direction and support are given to Nicaraguan operatives, but it rejected the broader claim of Nicaragua that all actions of the contras were attributable to the U.S. because of its control over them"[577]. The court famously affirmed that mere financial and material support for guerrilla activities do not constitute a basis for the attribution, but the existence of direct control in form of exact orders or detailed guidance issued by the state, must be proved to enable the attribution[578]. In other words, the court emphasized the high evidentiary threshold of the effective control test by which it is not required that the persons who have conducted an act as a violation of international law be in a completely dependent relationship on the respondent state. It will be enough to prove that they acted under the instructions or effective

[573] Ibid. para. 115
[574] DARSIWA, Ibid. Art. 8 that states the following: "The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct"
[575] ICJ. Nicaragua v. United States, Ibid., para. 112; Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (hereinafter 'Bosnian Genocide'), Judgment of 26 Feb 2007, ICJ Rep 2007, para. 241, p. 388-394
[576] Talmon S., The Various Control Tests in the Law of State Responsibility and the Responsibility of Outside Powers for Acts of Secessionist, Legal Research Paper Series no. 16, University of Oxford 2009, p. 8.
[577] ICJ., Nicaragua v. United States, Ibid., para. 86.
[578] Cassese A., The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide. The European Journal of International Law. Vol. 18, no. 4, 2007, p. 653.

control of the state, and that the type of control has been exercised, or that the state's instructions were given, in respect of each operation in which the alleged violations occurred.

In the cyber context, the legal problem of attribution under effective control is that states will mask their involvement in cyber-attacks given the high threshold set under such criteria. Therefore, simply providing financial aid or equipment to support a cyber-attack, or even providing a haven base for individual hackers, would not be enough to meet the effective control test. But rather, the only instance in which states sponsors of cyber-attacks would apply is if their effective control by the state is beyond any doubt, given that it is highly unlikely that states under the required threshold of the ICJ will be held any legal responsibility. This makes the effective control requirements under unreachable evidentiary thresholds that impose on the victim an unrealistic obligation to provide evidence of specific instructions or directions of the de facto intervening state relating to the armed attack or conflict[579]. The reason why in 9/11 attacks on the US have undermined the position of strict approach and promoted lower threshold of more liberal nature or what will be explained later as "overall control". According to Antonio Cassese "Overall control once applied, it will be less difficult to prove that certain terrorist units or groups' actions that were coordinated or planned by a specific state or entity, are attributed to the state in question."[580] Cassese emphasized that this would make it possible to attribute to some specific states of the Middle East responsibility for the gross violations of human rights perpetrated by terrorist groups on which they have exercised a strong influence, not only because these states provided support, financing, training, and weapons, but also helped coordinate and plan the groups' activities.

Furthermore, states face a challenge in justifying their military response to cyber-attacks when the process of attribution requires time, and that is based on a dominating assumption that attribution is one of the most intractable problems in cyber security. In the era of HW, the fusion of NSAs and cyber operations that were to precede the use of conventional tactics within a hybrid strategy, states will be constrained, divided and unable to act decisively as a result of an adversary engineering uncertainty through plausible deniability[581]. It is a critique that was also raised by the Appeals of Chamber in the ICTY arguing that the notion of an effective

[579] Vark R., State Responsibility for Private Armed Groups in the Context of Terrorism, Juridica International, XI, 2006, April 23, 2020., pp. 184-193.
[580] Cassese A., The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, The European Journal of International Law, Vol. 18, 2007, p. 666.
[581] Fitton O., Cyber Operations and Gray Zones: Challenges for NATO, Connections Vol. 15, no. 2, Spring 2016, p. 111.

control test was contrary to the logic of the law of state responsibility[582]. The rationale behind such rule is preventing states from masking operations that raise international responsibility through private individuals, or denying the role of individuals that participate in governmental authority, and considering them as nonstate agents under national legislation, in order not to involve state responsibility.

It is also argued that control must not be confused with support, the state must be able to control the beginning of the operation, the way it is carried out, and the end of it. Such condition is highly challenged by NSAs and their ability to use force transnationally in a more sophisticated and developed manner. ISIS, for example, shows the difficulty of applying the classical framework of attribution, it is very challenging first to prove any effective control in the era of modern technologies and communication, also online financial transactions and logistics. On the other hand, some NSAs have established quasi de facto public authorities in portions of sovereign states, such as the DNR and LNR in Ukraine, Hezbollah in South Lebanon, and Kurdish rebels in Syria and Iraq creating a black hole in terms of human rights infringements, the amnesty for the separatists and their attribution status.

For example, in July 2014, the Malaysia Airlines Boeing 777 "flight MH17" was shot down by an anti-craft missile "Buk Telar" type that was allegedly launched from the Donbas region of eastern Ukraine, and claimed 298 deaths. The part of Donbas from where the missile was launched is controlled by the pro-Russian separatist government of Lugansk-Ukraine, and that has raised legal doubts about the possibility of classifying it as a war crime or crime of terror and if so, who will be held responsible. Following this incident, the Dutch-led joint investigation team (JIT) which includes officials from the Netherlands, Australia, Belgium, Malaysia, and Ukraine has named three suspects including Igor Girkin (AKA Strelkov) who is a former colonel in Russia's FSB intelligence that was appointed the minister of defense in the rebel-held eastern Ukrainian city of Donetsk and believed to be the highest military officer in the area[583].

The Netherlands has also lodged the inter-state application, set out under Article 33 of the European Convention on Human Rights, against Russia on July 10, 2020.[584] According to the Netherlands, the plane was shot down by an air missile system that belonged to and was

[582] Prosecutor v Dusco Tadić (sentencing Judgment), IT-94-1-Tbis-R117, International Criminal Tribunal for the former Yugoslavia (ICTY), 11 November 1999, pp. 108-9.
[583] MH17: Four charged with shooting down plane over Ukraine, BBC News 19 June 2019, https://www.bbc.com/news/world-europe-48691488
[584] ECHR, New Inter-State application brought by the Netherlands against Russia concerning downing of Malaysia Airlines flight MH17, registered under no. 28525/20, July 2020.

provided by Russian Federation. In that sense, the attribution issue is raised under Article 1 of the ECHR that states the following: "State parties must secure to everyone within their jurisdiction the rights protected by the convention." Although that does not preclude the direct involvement of the Russian Federation, the link between the separatists and Russia that responded by denying any of its anti-aircraft missile systems had ever crossed the Ukrainian border, was established. Considering that the incident occurred over the Ukrainian territory, yet no international responsibility will be held by the de jure host (Ukraine) as the area where the plane was shot down was de facto controlled by the pro-Russian rebels[585]. Given this, international law must accommodate these different actors, analyze the nature of the affiliation between an actor and a state and their varying use of force ensuring that international state responsibility as a secondary rule of law remains an available option alongside criminalization in a domestic context.

The ICJ has also introduced the "Strict Control" with mainly three requirements that deal mainly with secessionist entities[586]. According to the "strict control," these three requirements must be fulfilled for the entity to be equated with the de facto organ. These requirements include that secessionist entity must be in total or complete dependency on outside power, with no real autonomy, leaving no doubts to attribution. Also, the dependency must extend to all fields of activity of the secessionist entity, by which the entity cannot conduct any activity without the assistance of the outside power state. And lastly, the outside power must have made use of the potential control, by which have exercised a particularly high degree of control. Therefore, it is beyond any doubt that such a high degree of control is not highly ineffectual to contemporary conflicts that rely heavily on covert and fusion of low-intensity activities. But again, such criteria is highly controversial and inadequate to conflicts and threats that stem from hybrid activities in a way distancing from reality, the reason why the ICTY in the Tadic case introduced a more lenient approach known as Overall test.

[585] Lachowski T., Ibid.
[586] ICJ, commentary on the Nicaragua v. United States, paras 109-110; see also Bosnian Genocide case, paras 392, 393.

3.2.2. Overall Control Test

On the other hand, the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the Tadic case has looked into the criminal responsibility of Duško Tadić[587] for crimes committed by the Bosnian- Serb army (VRS) of "Republika Srpska" (unrecognized Bosnian breakaway region) in Bosnia-Herzegovina to classify the armed conflict, to determine the applicable law and dealing with state responsibility as a preliminary question by setting the difference between IAC and NIAC. The court found that "the relationship of de facto organs or agents to the foreign power includes those circumstances in which the foreign power occupies or operates in certain territory solely through the acts of local de facto organs or agents" [588]. It concluded that the Bosnian Serb armed forces could be attributed to the Federal Republic of Yugoslavia, on the basis that these forces, as a whole, were under the "overall control" of that state[589]. Nevertheless, the statement has identified the ability to have an occupation by proxy and that a group can be attributed to a state if they are acting as de facto organs regardless of a difference in nationality[590]. And when deciding on the level of control necessary for attributing armed group conduct to the state, the ICTY established that: " It must be proved that the State wields overall control over the group, not only by equipping and financing the group but also by coordinating or helping in the general planning of its military activity." [591] That is highly relevant to hybrid campaigns, as this rule aims to prevent states from escaping international responsibility by having private individuals carry out operations that if carried out by state officials, would have triggered state responsibility. In other words, States are not allowed to act de facto through individuals or groups and disassociate themselves from such conduct when these individuals breach international law.

The overall control standard goes beyond the mere financing of armed groups, it also involves a state in its participation in planning and supervision of military operation According to these criteria, it has to be proved beyond a reasonable doubt that the state has recognized those acting

[587] A Bosnian Serb politician, former Social Democratic Party (SDS) leader in Kozarac and former member of the paramilitary forces supporting the attack on the district of Prijedor. Duško Tadić was convicted of crimes against humanity, grave violations of the Geneva Conventions and war crimes.
[588] ICTY, Prosecutor v. Tadic, case no. IT-94-1-T, Trial judgment, para. 584
[589] Prosecutor v. Tadic, n. 19, paras 120, 131, 144; see also Prosecutor v. Rajic, Case No IT-95-12-R61, of 13 Sep. 1996, paras. 22-32. Where the ICTY Trial Chamber disregarded the tests enunciated by the ICJ in the Nicaragua case and found that the conflict in Bosnia and Herzegovina was of an international character on the basis that the Bosnian Croats were agents of Croatia as the latter exercised a high degree of control over both the military and political institutions of the Bosnian Croats, see Prosecutor v. Rajic , Ibid. para 26.
[590] ICTY, Prosecutor v. Tadic, Ibid. para 584.
[591] Ibid. para 131.

persons; integrated them into its hierarchical operational structures in the relationship of dependency; entrusted them with certain functions; and can exercise general control over those persons, providing them guidance and/or support. [592].

The overall control test has lowered the threshold of control necessary for attributing responsibility to the state than the one set by a strict control test that required a link to the state organ. The former required a more general and less-intrusive level of direction and planning, conducted at the strategic and operational level of military operations. This means that the conduct of armed groups or their members may be regarded as the conduct of de facto State organs, despite whether the state in question has issued any specific instruction regarding the execution of each of those acts[593]. The Appeals Chamber of the ICTY in the Tadic case distinguished the level of state control required when dealing with an individual or non-organized group compared to an "organized and hierarchically structured group" by proposing distinct tests for state responsibility. The ICTY in the Tadic case considered that if a private individual or group that is not militarily organized acted as a de facto state organ, it will be necessary to ascertain whether instructions of the commissioned act were issued by the state. Control by a State over subordinate armed forces or militias, or paramilitary units may be of an overall character and must comprise more than the mere provision of financial assistance or military equipment or training. [594]

Nonetheless, the overall test has raised questions and critiques by the ICJ that considered it unsuitable for application in a state responsibility context on the basis that the responsibility so produced was overly broad and stretches the connection which must exist between the conduct of a State's organs and its international responsibility, the court squarely rejected the ICTY's analysis of the Overall standard.[595] The ICJ in the Nicaragua case intimated the requirement of clear evidence in the case of attribution of a non-state group's act to a state[596]. For example, the ICJ recognized this basis in the Tehran Hostages case, by which the court found that Iran bore [the seizure] by *Ayatollah Khomeini* and other organs of the Iranian State, the decision to perpetuate them and translated the continuing occupation of the Embassy and detention of the

[592] ILM, Vol. 38, No.6, November 1999, International Tribunal for former Yugoslavia, Prosecutor v. Duscko Tadic case, p. 1546, para. 145.
[593] ICTY, Prosecutor v. Tadic, Appeal Judgment Ibid. paras 130-45.
[594] Ibid. para. 137.
[595] Bosnian Genocide case, Ibid. para. 403- 406.
[596] ICJ, Nicaragua case, Ibid., para. 109.

hostages as acts of that State."[597]. As such clarity is not equated and absolute certainty or elimination of all possible alternatives is not required. Therefore, this can be seen as the divergence between the ICJ and ICTY legal rules due to the possible lack of coordination and practical development of regimes in international law, as the functional necessity of the cases before the competent court weakens any coordinated development of the international law regimes. Though the Nicaragua and Tadic cases are relatively different, still they reflect modern conflicts, particularly in analyzing their adequacy to HW means. Yet, the divergence between the two tests created a legal gap that allows a hybrid adversary to manipulate.

To illustrate, in the cyber context attribution is the ability to identify who attacked a computer network and from what location. While the process of attributing a cyber-attack is arguably the most difficult, the ability to find a link between the hacker and the State or organization that hires the hacker is even harder. In the same context, countermeasures often represent an effective means of self-help by allowing the injured state to take urgent action that would otherwise be unavailable to it, such as "hacking back", to compel the responsible state to cease its internationally wrongful cyber operations. States cannot respond to a cross-border cyber-attack with force without establishing state responsibility for the attack and once such attacks are imputed to a state that in return refuses to comply with the rules of international law, self-defense will be a legitimate response by the victim state.[598] Concerning proxies, if the NSA's cyber operations are attributed to a sponsoring state as a matter of law, it is lawful to take countermeasures upon the other state to compel it to use its influence and put an end to the non-state actor's operations.

Moreover, it is easy for malicious actors to identify and exploit the gaps in legal responses and remedies due to the technological limitations that surround cyberspace regarding the attack detection, attack classification, and tracing the attack which makes it more complicated for a victim state to detect and come up with the proper response.

Detection of an attack

The nature of cyber-attacks is that they are not easily detected even with the most developed programs. Therefore, attacks are being detected after they reach the target of the operations, and that will require time for the victim state to detect and will decrease the efficiency of the

[597] United States Diplomatic and Consular Staff in Tehran (US v. Iran), 1980 I.C.J. 3, para. 74 (May 24).
[598] Carr J., Inside Cyber Warfare, Ch. IV, Ibid.

use of active defense. Hence, it can enhance the active defenses for future attacks if such operation was seen as a series of ongoing attack. It is very hard to hide thousands of tanks, but very easy to hide cyber development activities.

Classification of an attack

The classification in this section mainly relates to the effect of an attack, whether it is passive or ongoing. If such an attack has caused severe, immediate invasive, direct, and measurable damage, then it can be classified as an armed attack. However, many attacks can potentially lead to future damages, that would deter the victim state to classify the attack and meet the requirement of the immediacy of future harm. States might find themselves directing their system administrators to respond to such attacks by force as self-defense only as an act of last resort, to avoid any unnecessary escalation.[599] The challenge here is more sophisticated and covert when conducted by NSAs groups that can have access to cyber weapons since they are cheap and can easily be created by highly skilled hackers.[600]

Tracing an attack

Cyber-attacks are generated to be covert operations that disguise the identity of attackers, and most attacks are hardly traceable, or they might be traced back to a state or system that is not the actual one. This confusion of whether the state where the attack originated is responsible or just a matter of misattribution is the core goal of such attacks. For example, the technique "Spoofing" is one of the most common techniques that is used to conceal the origins of the cyber-attacks, by allowing the perpetrator to make it appear that the cyber operation is from a source unrelated to the true origin of the cyber operation. And if the suspected state refused to comply with international law to prevent cyber-attacks or take any steps to deter such operations (enacting and enforcing stringent criminal laws, cooperation in the international field) the state will be responsible, especially in the era of digital transformation. For instance, the attack against Estonia in 2007, a state that depends on modern technology in every domain (banks, access to information), was launched by hacktivist group "the Nashi Hackers", although Russia was the main suspect nothing could be traced to it due to the nature and characteristics of this attack that is botnet creating thousands of zombie computers and servers connected all at once to Estonian websites and led to complete shut down for weeks. Russia

[599] Carr J., Inside Cyber Warfare, Ch. IV, Ibid
[600] Greco G., Ibid., p. 41.

said that the hacked servers and computers are located in more than 100 countries some even in the US, which makes cyber-attacks unpredictable and invisible. It is not easy to trace an IP address to an end-user, as these addresses are often associated with hundreds if not thousands of end-users. For example, DDOS attacks are mainly botnets not geographically limited, the malware that creates them moves freely across national borders. The internet traffic has been specifically designed to travel on the fastest possible route, they connect infected devices under the control of the botmaster (a person who operates the command and control of botnets) to carry out the attacks.[601]

It is concluded that in the presence of two conflicting standards of control generated from different legal regimes, it appeared that there is no unified regulatory mechanism that applies to current threats, particularly when international actors disregard certain rules for their interest. The strict ICJ requirement of "effective control" in the Nicaragua case can allow states to employ NSA in the gray zone where these strict conditions and proof cannot be met. While the ICTY's "overall control", according to the ICJ in Genocide case 2007, may be more suitable for the classification of armed conflict, it does not persuade for the purpose of state responsibility. Therefore, the complexity of the two different quality tests is challenging in hybrid warfare scenario, as a state can instigate an IAC by having "overall control" of acts of NSAs, but at the same time avoid state responsibility for the acts of those NSAs as the "effective control" test is not met. Also, the nature of cyber operations does not fit with the classical control tests introduced by the ICTY and ICJ. The uncertainty in the effective and overall control tests concerning current threats of cyber operations requires rapid steps by developing a clear policy and doctrine to bridge over any gap that HW successfully exploits through means of politicizing the law and legal arguments.

4. The Principle of State Sovereignty in the Era of Hybrid warfare

4.1. State Sovereignty under International law

State sovereignty is one of the most fundamental concepts of international law since the Treaty of Westphalia of 1648 and is universally accepted as customary international law. The principle is reflected in three distinct venues:

[601] Ibid.

- "the international independence of a state that guarantees the supremacy of the state's governmental institutions and gives the state the status of a legal person,
- the territorial authority that gives the state power to exercise authority over all persons and things within its territory,
- the personal authority to regulate its internal affairs without foreign dictation."[602]

The three core venues of sovereignty find their roots in different sources. According to Oppenheim, sovereignty is either external independence concerning the liberty of action outside its borders or internal independence concerning the liberty of action of a state inside its borders. As comprising the power of a state to exercise supreme authority over all persons and things within its territory, sovereignty involves territorial authority[603]. Additionally, Article 1 of the ILC Draft Declaration on the Rights and Duties of States provides that every State has the right to independence and hence to exercise freely, without dictation by any other state, all its legal powers, including the choice of its form of government[604]. Therefore, the sovereignty of states includes the political independence that allows the state to form freely its political, social, economic, and cultural system, and the right to exercise jurisdiction within the framework of International law that requires the respect of customary law related to non-interference and the protection of the individuals under IHL and Human rights law.[605] The right to non-interference that concerns the matters which are not regulated by international law and in which the state has maintained its discretionary power, qualify along with the principle of non-intervention as one of the fundamental rights of states in the international legal order.

Relatedly, states must not allow their territory to be used contrary to the rights of other States. Judge Alvarez in the Corfu Channel case stated that sovereignty encompasses a bundle of rights that a state possesses in its territory to the exclusion of all other states and also in its relations with other states[606]. For example, the views expressed by the court regarding the Albanian claims that the British vessels have violated its sovereignty, have highlighted that a State must

[602] Joyner Ch., and Lotrionte C., Information Warfare as International Coercion: Elements of a Legal Framework, European Journal of International Law ed. 12, 2001, p. 825,842.
[603] Oppenheim L., Oppenheim's International Law, 1996, Vol. 1, 9th edn, Jennings, R. Y. and Watts, A., London; New York, p. 382.
[604] Draft Declaration on the Rights and Duties of States with commentaries, text adopted by ILC in 1949
[605] The International Court of Justice in Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Merits, 27 June 1986, ICJ 14 ('the Nicaragua case'), which referred to 'matters in which each State is permitted, by the principle of State sovereignty, to decide freely. One of these is the choice of a political, economic, social and cultural system, and the formulation of foreign policy' (para 205). Although this was stated in the context of the non-intervention principle, it is still relevant to sovereignty as the non-intervention principle is itself a reflection of the principle of sovereignty.
[606] Corfu Channel Case, United Kingdom v. Albania, Separate Opinion, 9 April 1949, ICJ Rep. 43,

notify another state of the dangers posed by transit through the Corfu Channel and held Albania responsible for the damage and loss of life of the British vessels based on the right of the state in an innocent passage[607]. But, a contrasting conclusion was reached concerning the minesweeping that was conducted by the British vessels in the Albanian territory without Albania's consent. The court concluded that: "between independent States, respect for territorial sovereignty is an essential foundation of international relations. The Court recognizes that the Albanian Government's complete failure to carry out its duties after the explosions, and the dilatory nature of its diplomatic notes, are extenuating circumstances for the action of the United Kingdom Government. But to ensure respect for international law, of which it is the organ, the Court must declare that the action of the British Navy constituted a violation of Albanian sovereignty."[608] The latter has been reflected in the Friendly Relations Declaration that referred to the "Rights inherent in full sovereignty"[609].

Additionally, in 1973 the ICJ addressed the legality of French atmospheric nuclear testing in the South Pacific (Hereinafter the Nuclear Tests case) that involved the Australian request for a declaratory judgment that the French testing violates international law as well as a permanent order that prohibits France from carrying out further tests[610]. The case was dismissed on procedural grounds but it highlighted the position of the Australian government that the breach of sovereignty is a primary rule and stated that: "deposit of radio-active fall-out on the territory of Australia and its dispersion in Australia's airspace without Australia's consent violates Australian sovereignty over its territory."[611]

Territorial sovereignty can also be breached by activities that do not involve the use of force, under the principle of non-interference. For instance, in 2015 the ICJ in the "Costa Rica v.

[607] Corfu Channel Case, Ibid. at 63.
[608] Ibid. at 35
[609] Resolution 2625 (XXV) of 24 October 1970 containing the Declaration of Principles of International Law, Friendly Relations and Cooperation Among States in Accordance with The Charter of the UN, UN Doc. A/Res/2625.

[610] ICJ Judgment, Nuclear Tests, Australia v. France, Dec. 20, 1974, Rep. 235, 254. In its Memorial, Australia set forth its legal logic in making the claim: "The Government of Australia repeats that its case rests upon several bases: on the mere fact of trespass, on the harmful effects associated with trespass, and on the impairment of its independent right to determine what acts shall take place within its territory. In this connection, the Government of Australia wants to emphasize that the mere fact of trespass, the harmful effects which flow from such fall- out and the impairment of its independence, each clearly constitute a violation of the affected State's sovereignty over and in respect of its territory." See, Memorial of Australia, Nuclear Tests, ICJ. Pleadings, Nov. 23, 1974, at 454.

[611] Schmitt M. and Vihul l., Respect for Sovereignty in Cyberspace, Texas Law Review, Vol. 95, Issue 7, 2017, p. 1652.

Nicaragua" case[612] found that "Nicaragua has carried out various activities in the disputed territory since 2010, that included the excavation of three Caños (the Spanish designation adopted by both parties) and the establishment of a military presence in parts of that territory, to be a breach of Costa Rica's territorial sovereignty."[613] The judgment has set the rules firmly based on concepts of State responsibility, affirming that the obligation to respect territorial sovereignty is legally binding and that the court did not need to determine whether Nicaragua's conduct amounted to a breach of the prohibition on the threat or use of force under the UN Charter to consider that there was a violation of the sovereignty of Costa Rica, but such breach alone provides adequate satisfaction for the nonmaterial injury suffered on this account.

Any exercise of authority by a state in the territory of another state without its consent is considered a violation of state sovereignty, as well as violation to the non-interference principle into domestic affairs, this is reflected in the international jurisprudence. According to the Permanent Court of International Justice (hereinafter PCIJ) in the Lotus case, states under international law may not exercise their power in any form in the territory of another state.[614] The court in the latter case observed that "the 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."[615] The term "any form" could be seen as a preemptive factor to block any evolving means that could be used by states to destabilize the territorial integrity and independence of a state, this covers activities such as cyber-attacks, legal warfare and the use of non-state armed groups. The activities of a state on the territory of another state without the latter's consent have been recognized as unlawful by the international tribunals for a long time.

On the other hand, HW through the strategic objectives and employment of its means tends to violate other state's sovereignty during peacetime, is structured to minimize the chances of international military response[616]. The core strategy of hybrid aggressors is to undermine an adversary's ability to defend its sovereignty without the complete commitment of military

[612] Costa Rica claimed that Nicaragua had sent armed forces into Costa Rican territory and dug a channel, while Nicaragua accused Costa Rica of building. A road in the contested area that caused transboundary environmental damage to Nicaragua. See, ICJ Judgment 2015, Rep 1, 2-4, December 16.
[613] ICJ., Certain Activities carried out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Judgement, ICJ Reports 2015, para. 93
[614] PCIJ, Lotus case (France v. Turkey), Judgment, 7 September 1927, series A, No. 1, p. 18
[615] Ibid.
[616] Dayspring S., Toward A Theory of Hybrid Warfare: The Russian Conduct of War During Peace, Naval Postgraduate School, California December 2015, p. v.

force. This puts cyber activities in a very advanced position to be employed by aggressors against the territorial sovereignty of an adversary. As cyberspace has no fixed territorial boundaries as it consists of persistent and low-level intrusions that take place below the threshold of use of force, especially since the violation of the sovereignty of states is typically associated with some physical incursion whether land, sea, or air.[617] However, there is no reasonable justification that would not allow the principle of sovereignty to apply in the cyber context. That was recognized by the UN Group of Governments Experts that noted "State sovereignty, international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and their jurisdiction over ICT infrastructure within their territory."[618] For example, China has developed the ability to disconnect from the internet if attacked but still operate internally on its domestic form of the Internet to protect its territory from any external attacks[619]. China also used this right over the internet in its territory to control what takes place within its borders, mainly the rights of internet users to voice their opinion, which created a dispute between China and Google in 2009 with regards to the compliance with censorship of searches by "Google.cn".[620] The principle of state sovereignty applies to activities conducted by State agents physically present on the territory or beyond the borders of the victim State with a harmful effect on the target state's territory[621]. Similarly, states exercise sovereign control over cyber infrastructure within their territory with an obligation to respect the sovereignty of other states by preventing their cyber infrastructure from being used by others to harm another state[622]. Although the State's physical cyber assets located in its territory are connected to the global Internet, this does not waive a State's territorial sovereignty over those assets and the activities involving them.[623] Multiple declarations including UNGA Resolution 71/73 and NATO Wales Summit Declaration have confirmed that International law applies in cyberspace, however, whether this principle operates as a

[617] Moynihan H., the Application of International Law to State Cyber-attacks Sovereignty and Non-intervention, Chatham House, International Law Program December 2019, p. 13,14.
[618] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, 68th session, 24, June 2013, para. 20, p.8.
[619] Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It, 2010, p. 146.
[620] In January 2010, Google announced that It would no longer comply with censorship of searches by Google.cn and no longer do business within China in response to attacks from Chinese computer servers targeting Gmail accounts of some human-rights activists and Google source code theft. See, Branigan T., Google to end Censorship in China over Cyber Attacks, The Guardian, 12 Jan. 2010.
[621] Moynihan H., Ibid.
[622] Tallinn Manual, Ibid., para 3.
[623] Lotrionte C., State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for balancing Legal Rights, Emory International Law Review, Vol. 26, 2012, p. 851,852.

standalone rule of international law (any breach of this rule gives rise to state responsibility) or not, is still debatable.

To illustrate, the Tallinn Manual took the position that the prohibition on violating the state sovereignty is a substantive primary rule of international law in which it is an internationally wrongful act[624], by which the commentary to Rule 4 stated that "In the cyber context, it is a violation of territorial sovereignty for an organ of a State or others whose conduct may be attributed to the State, to conduct cyber operations while physically present on another State's territory against that State or entities or persons located there. For example, if an agent of one State uses a USB flash drive to introduce malware into cyber infrastructure located in another State, a violation of sovereignty has taken place".[625] On the State level, certain disagreements were identified. For example, the United Kingdom considered that sovereignty is a principle of international law, but does not amount to a standalone primary rule by which cyber operations do not violate the sovereignty of a state, despite whether such attacks may constitute prohibited intervention, use of force, or other internationally wrongful acts.[626] While Russia and China, have emphasized the binding nature of sovereignty. This was reflected in the "Joint Statement on Cooperation in Information Space Development" that was signed by both countries, which states in its first article the following "both countries shall jointly advocate respect to and oppose infringements on every country's sovereignty in information space". A very controversial statement especially since China is considered the world's biggest state sponsor of cyber-attacks[627]. Yet the Chinese National Cyber Security Strategy stresses that " No infringement of sovereignty in cyberspace will be tolerated, the rights of all countries to independently choose their development path, network management method, and internet public policy, as well as to equally participate in international cyberspace governance will be

[624] Schmitt M., Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones on International Law, Chinese Journal of International law, ed. 19, 2018, p. 30,40.
[625] Tallinn Manual 2.0, Ibid. Rule 4. At 19. United States and the Netherlands have taken the position that defensive use of force un the cyber context is permissible under Article 51 even if a cyber-attack by a non-state actor cannot be attributed to another state. See, Secretary General, Developments in the field of information and telecommunications in the context of international security, U.N. Doc. A/66/152, July 15,2011, at 18; Netherlands Government Response to the AIV/CAVV Report on Cyber Warfare, www.aiv-advies.nl/contentsuite/template/aiv/adv/collection_single.asp?id=1942&adv_id=3016&page=regeringsreacties&language=UK.
[626] Corn G. and Taylor R., Sovereignty in the Age of Cyber, American Journal of International Law, 2017, p. 207-208.
[627] Crowdstrike, Observations from the Front Lines of Threat Hunting, October 2018. https://www.crowdstrike.com/resources/reports/observations-from-the-front-lines-of-threat-hunting/

respected".[628] So, states have the right to exercise their sovereign power over cyber infrastructure within their territorial borders (including the satellites, within its jurisdiction) exclusively and independently, as in the non-cyber context. Therefore, if a State exercises its authority whether through State agents, state organs, non-state actors, or proxies if their actions can be attributed to the state under the rules of attribution set out in the ILC's Articles on State Responsibility in another State's territory without the former's consent, that will constitute a violation of state sovereignty.[629]

However, the level of the involvement of states and their organs in the sovereignty of another state is debatable. Some scholars argue that any kind of interference with the State's exclusive internal and external authority, regardless of whether the exercise of authority is manifested through physical presence on the territory of the state or remotely, could violate the State's sovereignty.[630] While others consider that not all exercises of authority carried out without the consent of a territorial state would amount to a violation of sovereignty, such as espionage and the role of state's agents on the territory of another state without being officially disclosed to the territorial authorities. Though the majority of states outlaw acts of espionage under domestic laws, however, most of these activities of intelligence agencies have not been treated by states as internationally unlawful per se.[631] For the present research, it is concluded that the threshold for which activities can be a violation of sovereignty is not established and the assessment has to be made on a case-by-case basis if no other rule of international law applies to the case.

4.1.1. State Sovereignty in Cyber Context

With regards to the violation of sovereignty in the cyber context, the case law assures that a state's sovereignty can be violated without reference to rules of international law dealing with specific areas whether space, air, and the seas. In this matter, Specter has argued that: "whether

[628] The Chinese International Strategy of Cooperation on Cyberspace, 3 January 2017. See, Valjataga A., Tracing opinion Juris in National Cyber Security Strategy Documents, NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), Tallinn 2018, p. 7.

[629] S.S Lotus (France v Turkey), Judgment, 7 September 1927, PCIJ, No.1, p.18. (The PCIJ noted that "first and foremost restrictions imposed by International Law upon 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."

[630] Moynihan H., The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention, Chatham House, 2019, p. 17.

[631] Ibid. p. 17

one chooses to call it sovereignty, or territorial sovereignty, or territorial integrity, or something else entirely, an overwhelming and unavoidable body of treaties, jurisprudence and scholarly opinion stands for the proposition that there is a primary rule of international law that requires one state to refrain from taking public act or exercising authority in the territory of another state, in the absence of consent or another provision on international law to the contrary."[632] The Tallinn Manual 2.0 confirms the former statement in its 4th rule that states the following: " A state must not conduct cyber operations that violate the sovereignty of another state." And to emphasize what would constitute a sovereignty violation in the context of cyber operations following the approach of its experts to treat violations of sovereignty as a primary rule of international law, the Tallinn Manual 2.0 conducted its analysis on two main measures:

- The degree of infringement upon the target State's territorial integrity and that a State's cyber operation that causes physical damage or injury to the territory of another state violates the latter State's territorial sovereignty. Additionally, it includes operations that result in a loss of functionality such as the targeting of cyberinfrastructure or the equipment upon which it relies needs to be repaired or replaced qualifies as a violation but no consensus on the precise threshold for a loss of functionality was achieved among experts[633].
- Whether there has been an interference with or usurpation of inherently governmental functions[634]. Interference mainly is with data or services that are necessary for the exercise of law governmental functions. For example, the conduct of elections would qualify to meet this term[635]. While usurpation covers the exercise of law enforcement functions in another State's territory without justification[636], such violations do not require any damage, injury, or intent to meet the violation of sovereignty criteria.[637]

In this regard, the cyber intrusion can be carried out by an agent of one state while physically present in the territory of another state, as explained before in using a USB flash drive to introduce malware into cyberinfrastructure, or can be conducted remotely from outside the territory of the target state. For example, an agent hacking into and shutting down a state's national power grid from outside the victim state's territory is also considered a violation of

[632] Spector P., In Defense of Sovereignty, in the wake of Tallinn 2.0, American Journal of International law Unbound 2017, vol. 111, pp. 219-223
[633] Schmitt M. and Vihul l., Respect for Sovereignty in Cyberspace, Ibid., p. 1648.
[634] Tallinn Manual, 2.0, Ibid. at 20.
[635] Ibid., para 16.
[636] Ibid. para. 18
[637] Schmitt M. and Vihul l., Respect for Sovereignty in Cyberspace, Ibid. p. 1649.

state sovereignty if the affected server is located on the victim state's territory. And whether the damages are physical or not does not exclude the fact that a violation of the state's sovereignty occurred. But that has an impact on the response options available for the victim State if such an attack was considered an armed attack or not, yet this is will be also based on analysis of each incident separately. For example, in April 2018 one of the Russian intelligence officers (GRU) tried to hack into the Organization for the Prevention of Chemical Weapons (OPCW) systems in the Hague in the Netherlands. The Dutch law enforcement preempted the officer and escorted him out of the country the same day, and was considered an internationally wrongful act, but without specifying in what way[638]. However, in this case, the non-intervention principle does not seem applicable, as such activity did not meet the requirement of coercion[639]. So it is conceivable that a cyber-attack causing physical destruction, fatality, or injury will be considered a use of force. For instance, the Stuxnet virus that targeted Iran's Natanz nuclear facility and caused Iran to replace 1,000 of the 9,000 IR-1 centrifuges at the facility, is a clear example of a cyber-attack potentially qualifying as a use of force [640]. Moreover, the nature of cyber-attacks can be generated in a series of events that only cumulatively meet the threshold for an armed attack, by which if Stuxnet had occurred as a series of attacks rather than a single use of force, it would have qualified to an armed attack, then a well-defined violation of state sovereignty by a remote cyber intrusion[641].

To summarize, the principle of state sovereignty can invoke possible interference by operations that affects the State's exercise of its independent powers and territorial facet by either State agents operating on the territory of another state or by targeting infrastructure in its territory from the territory of another state. Therefore, the principle has legal effects as it applies in the cyber and non-cyber contexts. In practice, any open-ended conception of sovereignty by considering states have discretion as to whether consider respond to potential interference in any kind as a violation of sovereignty or deal with it by diplomatic means might increase the risk of confrontation and escalations in international relations. That is due to the lack of a comprehensive approach in dealing with such operations and the absence of a clear

[638] Statement by the Dutch Minister of Defense "Ank Bijleveld", Government of the Netherlands, Netherlands Defense Intelligence and Security Services disrupts Russian cyber operation targeting OPCW, http://www.defense-aerospace.com/article-view/release/196530/dutch-mod-disrupts-russian-cyber-attacks-on-opcw-in-the-hague.html. October 2018.
[639] Moynihan H., Ibid, p. 18-19
[640] Shubert A., Cyber warfare: A different way to attack Iran's reactors, CNN.com., November 8, 2011, http://www.cnn.com/2011/11/08/tech/iran-stuxnet/
[641] Dinniss H., Cyber Warfare and the Laws of War, Cambridge University Press, 2012, p. 57.

de minimis threshold that varies between each case and each state's interpretation. States tend to avoid framing cyber intrusions as violations of sovereignty not to escalate the situation to possible armed conflict or invoke the defensive use of force. However, it is hard to keep these statements of states in line with the judgments of international courts on the principle of sovereignty, which seem capable of application to all unauthorized exercises of state authority, cyber for instance.[642]

Based on the approach taken by the Tallinn Manual with regards to the de minimis threshold for violations of sovereignty that is based mainly on the severity of effects derived from the rules on use of force, it appears that there is no agreement as to what types of effects would be required under a de minimis threshold, the reason why cyber-attacks conducted by either state actors or NSAs in a hybrid manner is still an evolving challenge to the international law and the lawful use of force. Mainly due to the irregular features of cyberspace by which it is not always easy to consider that cyber operation has a cross-border element that may violate the sovereignty of particular states because perpetrators tend to use different geographical locations and systems, that make a cyber-attack hardly traced. And now there is not enough state practice to support that such limits are customary. Nevertheless, the Tallinn manual notably elaborates on the scope of a state's due diligence obligations in cyberspace in respect to cyber operations which could constitute wrongful acts. Although the due diligence standard is not fully structured, yet it provides good practice in developing a preventive approach and reduces the issues associated with the attribution of cyber activity to a state and the rule recognized that States' obligation to apply due diligence is a rule of international law.

4.1.2. Due Diligence Standard: A Potential Remedy to the Complexity of Cyber Threats

As previously explained, the cyber-attacks in an interconnected world and with more access to cyberspace by private and public persons have increased in volume offering significant challenges to international law in its role to ensure secure, open, and resilient cyberspace. Due Diligence is vital to tackle the complexity of hybrid operations that tend to use cyberspace and non-state armed groups to conduct attacks against other states, exploit the high legal threshold of effective control and inadequacy of overall control, and take advantage of difficulty to trace

[642] Moynihan H., Ibid, p.21. One examples of state's practices in this area is that in 2019 the French government took a sovereigntist approach in stating that any unauthorized cyber intrusions into the French system would constitute a violation of sovereignty. See Roguski P., France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I, Opinio juris, 24 September 2019.

the origin of these cyber-attacks and the uncertain links between the attackers and a state or sponsor.

The standard of due diligence is widely accepted in the field of prevention of transboundary harm in international environmental law[643], and arguably applicable to other potential violations of international law.[644] Although due diligence is not a term that is indicated in the International Law Commission's Articles on State Responsibility, yet it is considered a legal standard of conduct whose content and extent vary according to the applicable primary rule in international law.[645]

International law can impose liability for transboundary harms, but that require a decision on what standard of care should be used to determine whether a state is liable. According to Judge Higgins "the standard by which the duty of care regarding an obligation is to be tested will be determined by reference to the particular requirements of that obligation, and that has not been settled in the law of state responsibility."[646] However, a state is responsible for failing to take, either generally or with respect to the conduct of individuals, duly diligent care or care to such other standard as the particular obligation requires.[647] That reflects the concept of negligence that finds its way into international liability in the form of the standard of due diligence, which requires the state to act with care. Due diligence has emerged as a duty of states to take all necessary measures ensuring that its territory would not cause any harm to other states, which has its roots in the law of neutrality and in the context of the protection of aliens[648]. In this matter, the ICJ in the Corfu Channel case has stated that every State is under an obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States.[649] In addition, the ICJ in its judgment in the "Pulp Mills on the River Uruguay case" illustrated the meaning of a specific treaty obligation that it had qualified as " an obligation to act with due diligence" as follows: " it is an obligation which entails not only the adoption of appropriate rules and measures, but also a certain level of vigilance in their enforcement and the exercise

---

[643] International Law Commission, Commentary on the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, 2001, Report of the ILC on its 53rd Session, p. 392.

[644] Interim Report of the Council of Europe Ad Hoc Advisory Group on Cross-Border Internet to the Steering Committee on the Media and New Communications Services, Incorporating Analysis of Proposals for International and Multi-Stakeholder Cooperation on Cross Border Internet, Strasbourg 2010, p. 17 para 72.

[645] McDonald N., The Role of Due Diligence in International Law, Cambridge University Press for the British Institute of International and Comparative Law, 2019, p. 1044.

[646] Higgins R., Problems and Process: International law and How We Use It, 1995, p. 157.

[647] Ibid.

[648] Work of Grotius or Pufendorf in KA Hessbruegge, The Historical Development of the Doctrines of Attribution and Due Diligence in International Law , New York University Journal of International Law and Politics, 2003, Vol. 265, p. 284-85.

[649] Corfu Channel Case (UK v. Albania), Ibid., 1949, ICJ Rep 4, 22.

of administrative control applicable to public and private operators, such as the monitoring of activities undertaken by such operators…".[650] The due diligence obligation is not only based on the enactment of a law or regulation, but it relates to a certain level of caution in the implementation and enforcement of applicable administrative controls, such as monitoring of activities carried out for protecting the rights of other parties. The International Tribunal for the Law of the Sea "ITLOS" in its advisory opinion, stated that the provision in article 58 and article 62, as well as article 192 UNCLOS, give an obligation to the flag state to take the steps necessary to ensure that every vessel flying its flag is not involved in the illegal activities. Therefore, ITLOS confirmed that this is an obligation of conduct of the flag state and is not an obligation of result and this obligation has been fulfilled if proper due diligence is carried out by the flag state.[651] Due diligence is a standard that describes the threshold of action and effort that a state must demonstrate to fulfill its responsibility.

Therefore, due diligence is achieved and does not incur responsibility on a state just because it failed in preventing a specific event, but if a State failed to take all measures needed, which were within its power, to prevent the event from occurring. So due diligence does not entail a duty of prevention, but rather an obligation of conduct. For example, the ICJ has interpreted the duty to prevent Genocide under Article 1 of the Genocide Convention as an obligation of due diligence of states to employ all means reasonably available to them, to prevent genocide so far as possible.[652] However, the concrete obligations in terms of the standard are resulting from the duty of prevention that is to be determined on a case-by-case basis.

On the other hand, the Due Diligence standard has been established and developed further under LOAC, particularly with regards to the obligation of conduct about preventive and repressive measures that states must undertake in both peacetimes and during an armed conflict. For instance, CA 1 of the GCs and Article 1 of AP1 articulates that states must undertake to respect and to ensure the respect of IHL under all circumstances. In this regard, the Travaux Prepartoires in 1948 shows that the ICRC interpreted the duty to "ensure respect" as an obligation with a due diligence standard, by which the states must do everything in their power to ensure that the humanitarian principles on which the Convention is founded shall be

---

[650] Pulp Mills Case on the River Uruguay (Argentina v Uruguay) , 2010 , Report 14. See also, International Tribunal for the Law of the Sea (ITLOS) (Seabed Chamber), Responsibilities and Obligations of States Sponsoring Persons and Entities with Respect to Activities in the Area (Advisory Opinion), ITLOS Case No. 17, 1 February 2011.

[651] Request for an Advisory Opinion submitted by the Sub-Regional Fisheries Commission, Advisory Opinion, 2 April 2015, ITLOS Reports 2015, para 40.

[652] Application of the Convention on the Prevention and Punishment of the Crime of Genocide "Bosnia and Hezegovina v Serbia and Montenegro", Ibid., 2007, ICJ Rep. 43, p. 221, para. 430.

universally applied.[653] Therefore any violation of LOAC by a state's armed forces entails the state's responsibility not as a breach of a due diligence obligation, but based on the attribution of the conduct of its agents to the state. Also, the due diligence standard in international law is relevant regarding the behavior of NSAs too, by creating a bridge between them and State responsibility.

In the cyber context, as explained before, anonymity is a key factor, however, recognizing a cyber obligation of due diligence might mitigate the attribution dilemma by holding a State responsible for allowing its territory to conduct harmful operations against another state. The United Nations Group of Governmental Experts on Cybersecurity (GGE) in 2015 though did not mention explicitly due diligence standard, has made several mentions of this duty. The GGE maintained that states should seek to ensure that their territory is not used by NSAs to commit and should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. [654] Similarly, the Tallinn Manual 2.0 concluded that the duty of due diligence applies in the cyber context. According to Tallinn Manual, a state breaches its due diligence obligation in the following elements:

- The existence of acts (by NSAs or a Third State) contrary to the rights of a victim State,[655]
- activities conducted from or through the territory of the potentially responsible State (including cyber infrastructure),[656]
- if the activity would have been unlawful if conducted by the potentially responsible State,
- have serious adverse consequences for the victim state,[657]
- concerning which the potentially responsible State has actual or constructive knowledge,
- and upon which the potentially responsible State can act, but fails to take all feasible measures.[658]

[653] ICRC, Draft Revised or New Conventions for the Protection of War Victims, Geneva, May 1948, p. 5.
[654] Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 report, Note from the Secretary-General, A/70/174, July 22, 2015.

[655] Tallinn Manual 2.0, Ibid, commentary to rule 6, para 2 and 15.
[656] Ibid. at 30, rule 6.
[657] Ibid. commentary to rule 6, para 18 and 24.
[658] Ibid commentary to rule 6, para 43; commentary to rule 7, paras 2 and 18.

So as certain features that rely on the harm threshold and knowledge elements are required to trigger due diligence, as highlighted by rules 6 and 7 of the Tallinn manual 2.0, which appears promising and restrictive if framed properly. It is not a substantive provision of international law, but a standard that states must apply to prevent their territory from being used to cause transboundary harm.[659] Rule 6 of the Tallinn Manual states the following: "a State must exercise due diligence in not allowing its territory or cyberinfrastructure under its governmental control to be used for cyber operations that affect the rights and produce serious adverse consequences for other states."[660] It is therefore a position that is derived from the inherent obligations of states to protect each other's rights and their sovereign equality, to which when applied to cyberspace or even attacks originated by NSAs, if the hackers or groups were not identified, then the state that allowed negligently or attentively will be sanctioned because they did not adopt sufficient precautionary measures, by which knowledge is a key factor to due diligence standard. States are required to remedy all transboundary harm that results in serious adverse consequences, though this term was not explained as to what it covers, yet the experts of the Tallinn manual did argue that no "physical damage to objects or injuries to individuals" was required. [661] Also, it attentively linked NSAs' cyberattacks to the due diligence obligation to which their attacks do not violate international law per se (as states are usually held responsible for internationally wrongful acts) but could result in seriously adverse consequences contrary to the target state's rights.[662]

To further clarify, the hybridity in combining the use of modern technology and NSAs masks the operations by covert activities through a multitude of states in low-intensity attacks. For example, if an armed group or proxy actors from state A are using the territory of State B to conduct cyber-attacks against the computer systems of state C, which is often an ordinary scenario in modern conflicts. In this case, the Tallinn Manual concluded that diligence obligations attach to a state through which data only transits (for example a fiber optic cable located within a state), but conceded that transit state responsibility is unlikely to be carried out in practice, in comparison with a state in which specific cyberinfrastructure is set up for malicious purposes.[663] Therefore, state B will responsible for allowing the specific

[659] Ibid. at 30, rule 6.
[660] Ibid., rule 6.
[661] Ibid., at 36-37.
[662] Liu I.Y., The Due Diligence Doctrine under Tallinn Manual 2.0, Computer Law and Security Review 2017, Vol. 33, p. 392
[663] Liu I.Y., Ibid., p. 392

infrastructure used by the group from state A to harm state C. But as a matter of fact, the infrastructure in state B might be originally for peaceful purposes but infiltrated by hackers to launch such attacks. So, a State must have actual knowledge of the harm to be responsible for applying due diligence to prevent transboundary operations. The actual knowledge would be established if the target state could prove that the territorial state had information or detected that a cyberattack was being launched within its territory, which would be extremely difficult for the target state to establish in practice.[664] However, based on the Corfu channel case[665], the drafters of the Tallinn Manual asserted that even if actual knowledge is difficult to demonstrate, the legal obligation to exercise due diligence is not affected, and the manual acknowledged that when governmental infrastructure, rather than private ones, are being compromised, constructive knowledge would be more readily assumed.[666]

Due diligence rule was not favored by multiple states as it puts them under greater responsibility which could be resource-intensive, especially with the lack of opinio Juris in this area. Some scholars argue that it is extremely difficult to prepare a comprehensive and effective defense against the whole panoply of possible unlawful acts.[667] That was reflected on the State level in the UN GGE, as states were only willing to admit that they should exercise due diligence, rather than that they must as the Rule states.[668] The previous is an indication that some states support the desirability of due diligence rule and other states started to consider that it is now a binding principle of cyberspace, such as France and Netherlands.[669] Nonetheless, as explained in this section, international law offers important principles and doctrines to regulate harmful uses of cyberspace by states but is faced with certain obstacles relating to the nature of cyber-attacks and their anonymity. So, due diligence standards may contribute to certain stability in this regard. It also affects the implementation of IHL by strengthening compliance with the LOAC.

Due diligence is an important area for further exploration and development that is necessary to the legal norms applicable to cyberspace, and states must consider this option to become part

---

[664] Kimberley T., State responsibility for International Terrorism, Oxford University Press 2011, p. 68

[665] Corfu Channel Judgment, 1949, Ibid. at 19-20. The ICJ in Corfu case used a series of inferences to determine that the territorial state, Albania, had known of minefield laying within its territory. The court did not require the U.K. to demonstrate Albania's subjective knowledge but better illustrate a category of constructive knowledge.

[666] Liu I.Y., Ibid., p. 393.

[667] Tallinn Manual, Ibid., p. 27, para 7, on the Rule 5 Control of cyber infrastructure.

[668] UN Doc. A/70/174, 13 (c).

[669] Schmitt M., France's Major Statement on International Law and Cyber: An assessment, Just Security, 16 September 2019. See also, Jensen T and Watts S., A cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? Texas Law Review 2017, vol 95, pp. 1555-1557

of public international law after agreeing on certain elements that must be taken into consideration and further State practice or even case law to clarify it. These elements include the level of control of cyberspace activity, by which it could be a regular approach in some states such as China but could be an abomination to others. Furthermore, the technical feasibility and capacity of states to monitor their borders in cyberspace. Moreover, improvements should cover areas such as the threshold on which incidents should be considered as of serious adverse consequences, and what would fall below the de minimis threshold. Likewise, countermeasures should be addressed based on the form of response and how long can it last, otherwise due diligence could become a tool of provocation and the potential means of lawfare that is used to destabilize an order. Also, states must decide and agree on acting preventively based on constructive knowledge that a cyber-attack might stem out from their infrastructure or choose the actual knowledge as a factor. However, all the previous recommendations shall consider that due diligence will not affect the principles of human rights in monitoring the activities that domestically could violate freedom of speech or the right to privacy.

After all, policies at the international level are quite relevant and important for the success of due diligence in cyberspace. For example, a report by the Group of Governmental Experts on Advancing responsible State behavior in cyberspace in the context of International Security in May 2021[670], was a step forward in promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security. One of the major steps in this report is the acknowledgment that IHL applies to cyber operations during an armed conflict. Though it did not solve all issues of cyber-only exchange as armed conflicts, whether data is an "object" that an operation that targets civilian data for destruction or deletion violates IHL or not. Nonetheless, the report has treated due diligence as a voluntary non-binding norm of responsible state behavior, by which it adopted many of the same criteria highlighted by the Tallinn Manual 2.0 experts which will ease its path towards rule status. Similarly through the resolution 73/28, the General Assembly of the United Nations established an Open-Ended Working Group (OEWG) that adopted by consensus across all UN members the following: "states reaffirmed that norm does not replace or alter States' obligations or rights under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible state behavior in the use

[670] Report of the Group of Governmental Experts on Advancing responsible State Behavior in Cyberspace in the Context of International Security, GGE, 28 May 2021.

of ICTs."[671] All the previous are important for future due diligence status, which will require to be enforced in international relations to establish the necessary institutional structures guaranteeing that the norm is applied effectively. States should further develop the use of cyber defense systems, especially at the regional and international levels by taking data security into account at the design stage of any system architecture. Fundamentally, due diligence as its current non-binding status must apply between individual states as well between states and private companies, against modern threats, such as hybrid warfare amid evolving dual-use technology (civilian and military actors, or public and private actors). Due diligence is in line with what international law is about, as the latter imposes a negative duty on states to refrain from attacks, and not only positive duty to prevent others from launching attacks. Therefore, states are subject to the due diligence standard in preventing transboundary cyber harm, especially from non-state source. And are subjects to absolute liability for refraining from causing harm through attacks themselves.

At the same time, the attribution capabilities of states have developed, and cooperation between states in this field is allowing states with lesser capabilities to have the necessary data and information from other states or the private sector. Therefore, attribution as much as it creates a challenge to the law yet is a technical matter that will be of less importance in the future. But to sum up, the due diligence standard maintains and frames the responsibility of states regarding actions carried out on their territory and can play an important role in preventing and cracking down cyber activities within the state's territory that target other states' territory.

4.2. Legal Nature of the Non-Intervention and Non-Interference Principle and Elements of their Scope

In international law, the principles of non-intervention and non-interference include the prohibition of the threat or use of force against the territorial integrity or political independence of any state, as articulated in Article 2(4) of the UN Charter. These principles affirm that states should not intervene in the internal affairs of other states. Nonetheless, exceptions on the use of force in international relations, such as self-defense, do not infringe the principle of non-intervention. Similarly, Article 2(7) of the UN Charter states that nothing shall authorize the UN to intervene in matters which are essentially within the domestic jurisdiction of any state, but this principle shall not prejudice the application of enforcement measures under Chapter VII. Therefore, operations that are authorized by the UNSC under Chapter VII of the Charter,

[671] OEGW Final Substantive Report, UN Doc A/AC.290/2021/CRP.2, 10 March 2021, para. 54

do not violate the principles. Both principles are considered to constitute a classic manifestation of the doctrine of the fundamental rights of states. Non-intervention and non-interference are two terms that seem to be interchangeable, but the latter suggests a wider prohibition by which interference must be a coercive or dictatorial effect of depriving the state intervened against of control over the matter in question. Therefore, simple interference that lacks coercive means is not intervention. Also, intervention with the consent of the State being intervened in (intervention by invitation) is not precluded. However, when non-intervention is breached using force, such actopns are also violating the requirement of non-interference.

Before the 19th century, the intervention was an ordinary policy by states and was used frequently to enforce impartial and just rules. However, Emer de Vattel's "Droit des Gens of 1758" was the first to formulate such a principle and his book was one of the most influential pieces of literature on the Law of Nations in the 18th century, has concluded that: "No foreign power has a right to interfere in affairs being solely a national concern."[672] In case of disputes, E. Vattel stated that: "it belongs to the nation alone to judge and determine them conformably to its political constitution."[673] His explanation fits with the nature of sovereignty and the right of states to regulate their affairs, even the evolution in warfare that followed and the development of the applicable laws, did not affect the well-established position of the principle of non-intervention as part of the international law in contemporary conflicts. After WW II the law of intervention developed, according to Oppenheim the principle is the corollary of every state's right to sovereignty, territorial integrity, and political independence.[674] And then came the UN Charter that emphasized the cooperation between states to slightly allow the states to intervene in the affairs of other states without the use of force, which led later to the development of indirect intervention through political, economic, and diplomatic means.[675] The collective security model reflected in the UN Charter was established to deter state-to-state aggression experienced in the two world wars of the twentieth century. Still, it does not explicitly address the particularities of a foreign state's military response to attacks from a non-state actor[676]. As explained before, the charter framework is at least theoretically sufficient to address hybrid measures short of the use of force. However, the contours of what constitutes

[672] De Vattel E., The Law of Nations, Or, Principles of the Law of Nature, applied to the Conduct and Affairs of Nations and Sovereigns 1797, Liberty Fund, Indianapolis 2008, Book I, Ch III, para. 37.
[673] Ibid., para. 36.
[674] Oppenheim L., Oppenheim's International Law, 1996, Vol. 1, p. 428.
[675] Rattan J., Changing Dimensions of Intervention Under International Law: A Critical Analysis, Sage Open, June 2019, p. 2.
[676] Johnson, D., the Problem of the Terror Non-State: Rescuing International Law from ISIS and Boko Haram, Brooklyn Law Review, Vol. 84, Issue 2, Article 4, 1-1-2019, p. 497.

coercive interference have remained murky.[677] Whilst, HW mainly relies on indirect involvement in the conflict, by using proxy fighters and conducting operations at a level of intensity that circumvents the relevant legal thresholds, by that impeding the target state's ability to use force in its defense. And when intervention becomes unavoidable, actors will seek to distance themselves by the use of proxy forces, cyber-attacks, as well as covert and clandestine methods.

Nonetheless, even electoral interference of coercive effect can be categorized as internationally wrongful acts in the sense they violate both the principle of sovereignty and non-intervention, enabling the targeted state to use countermeasures in line with the Draft Articles on State Responsibility. Still, a response can be established legally if the measures taken are proportional and aimed at bringing the aggressor back into line[678]. Therefore, the principle of non-intervention, which is a core principle of international law, plays an important role in countering and regulating the frontiers of HW

However, following the historical development of the use of force in international relations, particularly the codification of UN charter by the formalization of the non-intervention principle, incidents such as direct intervention for changing regimes did not disappear but turned to more of a covert nature, unless policymakers locate a legal justification for violating the prohibition against intervention. For example, in 1960 President Eisenhauer authorized a covert operation plan in the Bay of Pigs in Cuba to overthrow Fidel Castro by infiltrating Cuba and starting an uprising movement. An operation that continued after President Kennedy was elected has failed but it was clear that in large part of it was to avoid openly violating America's non-intervention commitments.[679] And while interventions are still an option for states in many incidents, it is seen to be more covert as a result of how international law shapes the behavior of states. Hidden violations demonstrate a certain sensitivity to how others will react to blatantly illegal actions and a subsequent effort to minimize the visibility of such acts as a

[677] Farer T., Political and Economic Coercion in Contemporary International Law, American Journal of International Law, 1985, pp. 405-13.

[678] Sorensen H. and Back-Nyemann D., Going Beyond Resilience: A Revitalized Approach to Countering Hybrid Threats, Strategic Analysis, Hybrid COE November 2018, p. 4-5

[679] Poznansky M., The United Nations and the Accidental Rise of Covert Intervention, Lawfare Blog, June 2020. In this context, a Memo of Admiral Arleigh Burke, the chief of U.S. naval operations in 1960, noted that that: "the U.S. has the capability to seize Cuba by direct military actions, but in doing so it would prove that the U.S. is not willing to abide by its treaties if U.S. interests dictate otherwise." He also added that: "Such actions will lead to charges of aggression against the U.S., both in the OAS and in the United Nations, with the resulting possibility of UN and OAS action against the U.S.". see, Letter from the Chief of Naval Operations (Burke) to the United Secretary of State for Political Affairs, Washington 1960 Foreign Relations of the United States, 1958-1960, Cuba, Vol. VI.

result.[680] Therefore, understanding how the principle of non-intervention in the internal affairs of other states has transformed the actions taken by states to use the law as a means to justify such actions in a covert manner, that has led to the rising of new exceptions to the principle of non-intervention, such as the Responsibility to Protect (R2P) to pursue self-interested interventions under the guise of humanitarian actions.[681]

In this context, Article 2(7) of the UN Charter states that: "the UN has no authority to intervene in matters which are within the domestic jurisdiction of any state, while this principle shall not prejudice the application of enforcement measures under Chapter VII of the Charter[682]." Further, Resolution 2625 on the Friendly Relations Declaration of 1970 concluded that: "No state or group of states has the right to intervene, directly or indirectly, for any reason whatever, in the internal and external affairs of any other state. Consequently, armed intervention and all other forms of interference or attempted threats against the personality of the state or its political, economic and cultural elements, violate international law." Also, any support or sponsoring of armed activities or groups directed towards the violent overthrow of the regime of another state or interference in civil strife in another state is considered a breach of the non-intervention principle[683]. By which the development of the non-intervention principle has made it become a binding principle of international law and of a jus cogens nature. The principle is then an inter-state doctrine and does not apply to intervention by NSAs unless their activities can be attributed to a state under the rules of attribution in international law.

Nevertheless, what seemed to be unclear is the nature of intervention that shall be prohibited under the principle of non-intervention. In this manner, the ICJ in the Nicaragua case 1986 determined that: "a prohibited intervention must accordingly be one bearing on matters in which each state permitted, by the principle of state sovereignty, decide freely. So, the element of coercion defines and indeed forms the very essence of prohibited intervention."[684] Also, the

---

[680] Poznanksy m., Ibid.
[681] Ibid.
[682] UN Charter, Chapter I, Article 2/7, full text: "nothing contained in the present Charter shall authorize the United Nations to intervene in matters which are essentially within the domestic jurisdiction of any state or shall require the Members to submit such matters to settlement under the present Charter; but this principle shall not prejudice the application of enforcement measures under Chapter VII."
[683] UN General Assembly resolution 2625 (XXV) on Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations
[684] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment of ICJ 1986, Rep 14, para 205. See also ICJ, Armed Activities on the Territory of the Congo (DRC v Uganda) ICJ Reports 2005, para. 164. "the Court noted that Nicaragua had "made it clear that the principle of

court concluded that "intervention is wrongful when it uses methods of coercion concerning such choices, which must remain free ones."[685] The ICJ in this previous statement highlighted the interstate doctrine by which it concerns a state-to-state relation and that prohibition of intervention is an issue that a state should be permitted to decide freely. Besides, it tried to fill the gap of what constitutes a prohibited intervention by limiting it to coercive methods. According to the ICJ in the Nicaragua case, while examining coercion in international law, it stated that: "Nicaragua complained that the U.S. had two main objectives: First to overthrow of the government of Nicaragua and second, to coerce the government of Nicaragua into the acceptance of the United States policies."[686]. Therefore, it established that any use of force or threat to coerce a state to compel with the consent of the coercer would amount to prohibited intervention and unacceptable behavior. Likewise, Article 51 of the Vienna Convention on the Law of treaties indicated that: "the expression of a state's consent to be bound by a treaty which has been procured by the coercion of its represented through acts or threats direct against him shall be without any legal effect".[687] Nevertheless, according to Steven Wheatley, the non-intervention principle prohibits the deliberate and targeted actions of one state (A) aimed at interfering in the domestic political affairs of another state (B), where the behavior of state (A) is coercive and the actions cannot be justified as a lawful countermeasure, or on some other recognized ground under international law[688]. Nonetheless, the principle of non-intervention is not absolute, and in exceptional cases, such intervention is permitted through either direct military interventions, or indirect (economic, subversive, diplomatic), a state can intervene under self-defense, or through collective action under the Chapter VII of the UN Charter. And the non-intervention principle, concerning non-forcible interventions, is related to the element of sovereignty under which states are entitled to exercise their state powers free from interference from other states.[689] And the main difference between the violation of the non-intervention principle and other breaches of sovereignty is the element of coercion.

---

non-intervention prohibits a State "to intervene, directly or indirectly, with or without armed force, in support of the internal opposition within a State"

[685] Military and Paramilitary Activities in and against Nicaragua, Ibid. para. 292(3)

[686] Ibid. para. 239 see also Ibid para. 241, by which the court stated that: "The United States intended, by its support of the contras, to coerce the Government of Nicaragua in respect of matters in which each state is permitted to decide freely. "

[687] Vienna Convention on the Law of Treaties, United Nations May 1969, entered into force 27 January 1980, Treaty series, Vol. 1155., art. 51

[688] Wheatley S., Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber Operations Targeting Democracy, Presented at Conference on "New technologies: New Challenges for Democracy and international Law", University of Cambridge, March 2019, p. 11.

[689] The Friendly Relations Declaration provides that, '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'

However, many questions regarding what is considered a coercive intervention, or if intervening in cases of assistance to peoples seeking exercise the right of self-determination or in cases of Humanitarian intervention or protection of nationals in other states, were left unanswered and have opened the door for such justifications to interfere or justify the use of force in the era of HW. Coercion draws the line between minor interferences and unfriendly acts on one hand, and intervention sufficient to breach the prohibition on non-intervention, on the other hand. Otherwise, any act that affects another state would fall within the prohibition. Furthermore, certain factors found in the international law sources can help in identifying coercion, such as elements of pressure and the benefit for the perpetrating state from actions coerced on the target state.

4.2.1. Elements of Coercion

As explained before, the principle of non-intervention is related to State sovereignty and prohibits mainly dictatorial or coercive activity which is unlawful and engages the responsibility of the State which conducts it to the extent that the acts concerned can be attributed to a particular state or states. One of the main elements that identify coercion in international relations is the application of pressure to deprive the target state of control of its state function. The degree of pressure varies in each case based on the facts and in many instances hardly quantified, however it should have a certain magnitude to apply.[690] According to Oppenheim, for interference to constitute intervention, it must be forcible or dictatorial, or otherwise coercive, in effect depriving the state intervened against control over the matter in question.[691] So, the element of pressure or compulsion on the part of coercing state is one of the requirements for coercion, otherwise, it would be not differentiated from mere attempts of influence. And only a certain magnitude of pressure qualifies as coercive, by which pressure that could be reasonably resisted does not qualify as such. In applying the pressure factor to the cyber context, the Tallinn manual has considered that states may not intervene, including by cyber means, in the internal or external affairs of another state. The rule mainly targets coercive intervention by cyber tools, rather than mere interference that lacks the requisite of coerciveness to rise to the level of intervention. Therefore, disinformation interference that has no physical damage or coercive ends would be purely unlawful interference but not

[690] Jamnejad and Wood, Ibid. p. 348.
[691] Oppenheim L., Oppenheim's International Law, Ibid., p. 432.

intervention. For example, if an operation that targeted the infrastructure of an election campaign caused physical damages or led to the death of a candidate, then it will be considered unlawful election intervention. [692]

On the other hand, hybrid adversaries tend to use a combination of political and military pressure to influence an outcome in a matter reserved to the targeted sovereign state. For example, Russia was able to use both coercive and escalators tools on one hand, and compensatory and de-escalatory tools on the other to pressure the pro-western government in Kyiv. Russia has offered loans and decreased gas prices, at the same time canceled loans and decreased the supply of gas through its proxy companies "Gazprom" and "Gazprom bank", by using synchronized and escalation patterns before the Minsk agreement [693]. While the power of threat is predicated on the fact that the target knows that it is being coerced and will suffer consequences if it does not respond as the coercer wishes[694]. Nonetheless, in the example provided before, hybrid adversaries (Russia in this case) tends to identify the vulnerabilities to enforce their coercive pressure, at the same time keep the situation in ambiguity by which Ukraine was generally aware of the risk associated with the energy and economic deals with Russia, but was unable to realize how these contracts were designed in premeditated fashion as baits that would lead to further strategic entrapment that would allow Russia to use them with a pure adversarial intent should the need arise.[695]

In addition, coercion must be directed at securing a benefit for the perpetrating state. So another element that is corresponding to the pressure factor is that coercion must be directed at securing a benefit for the perpetrating state. According to the Friendly Relations Declaration: "No State may use or encourage the use of economic, political or any other type of measures to coerce another State to obtain from it the subordination of the exercise of its sovereign rights and to secure from it advantages of any kind."[696] The coercive intervention can be direct and indirect while attempting to compel an outcome or conduct for a matter reserved to the target state. The indirectness of such outcome was determined by the ICJ in the Nicaragua case by affirming that the US funding of the contras constituted intervention, notwithstanding that a

[692] Tallinn Manual, Ibid. rule 66.
[693] MCDC Countering Hybrid Warfare Project: understanding Hybrid Warfare, January 2017, p.16-17.
[694] Moynihan H., Ibid. p. 28-29.
[695] MCDC Countering Hybrid Warfare Project: understanding Hybrid Warfare, Ibid. p. 17.
[696] United Nations General Assembly Resolution 2625, The Declaration on Principles of International Law concerning Friendly Relations and Co-operation among states., 24 October 1970.

series of intervening events were required after the US transfer of funds took place and before coercion of the Sandinista regime of Nicaragua occurred.[697] Contemporary hybrid operations are relevant to the previous statement, for instance, cyber operations conducted with unclear intent such as investing in foreign critical infrastructure or are not readily definable as hostile and aggressive actions such as instigating non-violent protest. Such activities are at the core of synchronization escalations tailored by hybrid adversaries to secure their benefits such as the ability to use coercion while staying below the target's detection and response threshold, to be used indirectly in simultaneously escalating and de-escalating a future crisis. The ambiguity of operations switching between escalation and de-escalation is a challenging method to the principle of non-intervention while examining its coercive elements and the confusion it creates as to whether it can interplay with interference, rather than crossing the thresholds that can lead to cumulative and non-linear effects.

4.2.2. Coercive Intervention in Hybrid Cyberspace

Coercion in cyber context was examined by the experts in Tallinn Manual through rules that apply to relations between states and only bans coercive interference, defining coercion as: "an affirmative act designed to deprive another state of its freedom of choice, that is, to force that state to involuntarily act or refrain from acting in a particular way."[698] The manual gave examples such as the use by one state of a DDOS operation to coerce a government into reversing a decision about the official language after a referendum.[699] However, the majority of experts in the manual were in favor of the fact that coercive requirement is satisfied when an act has the effect of depriving the state of control over the manner in question.[700] The Tallinn Manual has therefore defined coercion to support a broader understanding of coercion that includes acts designed to deprive the state's freedom of choice to act involuntarily or involuntarily refrained from acting in a particular way. That has an important impact on the covert cyber operations that aim to disrupt or undermine the exercise of another state's sovereign functions with the harmful effects that will ensue within the target state, which is the outcome cyber adversary seeks to compel.

As explained before, the non-intervention principle relies on a causal nexus between the coercive behavior and the deprivation of the victim state's authority concerning the exercise of

[697] ICJ, Nicaragua case, Ibid. para. 205.
[698] Para 18 commentary to Rule 66 of the Tallinn Manual 2.0.
[699] Ibid. para 9 of the commentary to Rule 66.
[700] Ibid. para 19 of the commentary to Rule 66.

its state functions on the other. In the same context, the group of experts has equated the concept of state sovereignty concerning the non-intervention with what is known as *Domaine Reserve',* which describes the areas of State activity that are internal or domestic affairs of a State within its domestic jurisdiction or competence.[701] Therefore, based on this characterization, state-sponsored attacks targeting individuals or companies will not engage the non-intervention principle unless these attacks had a direct effect on the state's exclusive exercise of its independent sovereign functions. For instance, the United Kingdom, the US, and Australia stated that the WannaCry ransomware attributed to North Korean actors (known as Lazarus Group) in December 2017[702], was a criminal use of cyberspace rather than a violation of international law, as the attack targeted private institutes and did not affect the ability of those states to exercise inherently its sovereign power. [703]

On the other hand, the Tallinn manual through the majority of its group of experts has concluded that States' actual knowledge that it has been coerced as a necessary precondition was not required for the violation, but the intent to coerce is required. [704] Therefore, since actual harm is not a prerequisite for the non-intervention principle to be engaged, so the actual coercion is not required to succeed to be unlawful, then states are not required to know about the behavior especially if the act did not reach its goal, so the coercive behavior is in itself enough. So, the cyber-attacks in its relation to the non-intervention principle has different understanding when it comes to the targeted sector, this was reflected in the EU's recent restrictive measures against the cyber-attacks that considered these attacks as a threat to member states when affecting information systems relating to, inter alia:

- "Critical infrastructure, including submarine cables and objects launched into outer space, which is essential for the maintenance of vital functions of society, or the health, safety, security and economic or social well-being of people;

[701] Moynihan H., Ibid. p. 33-34.

[702] WannaCry Ransomware attack in 2017 was a crypto-worm that targeted computers running the Microsoft Windows operating systems by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. The incident impacted 300,000 computers in 150 countries. And in December 2017, the U.S., UK and Australia formally asserted that North Korea was behind the attack. See, Bossert Th., It's Official: North Korea is Behind WannaCry." The Wall Street Journal, 18 December 2017. See more about the WannaCry Ransomware, Savita M. and Manisha P., A brief study of WannaCry threat: Ransomware attack 2017, International Journal of Advanced Research in Computer Science.

[703] Statement of the Foreign Office Minister, Lord Ahmad of Wimbledon, Foreign Office Minister condemns North Korean actor for WannaCry attacks, December 2017. https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks

[704] Tallinn Manual 2.0, ibid, at 321

- Services necessary for the maintenance of essential social and/or economic activities, such as energy, transport, banking, financial market infrastructures, health, digital infrastructure, and drinking water supply and distribution
- Critical state functions, in particular areas of defense, governance, and functioning of institutions, including for public elections or the voting process, the functioning of economic and civil infrastructure, internal security, and external relations including diplomatic missions.
- The storage of classified information and government response teams."[705]

Based on the previous analysis the Stuxnet operation[706] has met all requirements for qualifying as coercive cyber intervention based on the coerciveness that aimed at preventing Iran from pursuing a particular course of action, and it was conducted by states and not by individuals or autonomous hackers. Also, it targeted a critical infrastructure that is vital to Iran but maintained a certain level of intensity below the threshold of an armed conflict as it did not result in physical or human casualties. Although the Iranian Government did not consider it as a use of force or armed attack. Yet, it has reached this level especially that it disrupted a critical infrastructure and coercively interfered with a State's chosen domestic policy, despite whether it was a legal course of action or not to prevent another country from carrying out nuclear research that is claimed to be for peaceful purposes. And whether the Stuxnet attack was a countermeasure taken by a particular state to compel Iran from its actions that are acting in violation of the treaty on the non-Proliferation of Nuclear Weapons regime to which it is a party.[707] However, taking into account the necessity principle and the availability of alternative means to resolve any dispute peacefully, this attack is a covert operation that violated the principle of non-intervention.

Furthermore, the cyber intervention prohibition has had many shapes in recent years, but what was challenging are those that targeted elections in the U.S. after the American Intelligence agencies have concluded with high confidence that Russia acted covertly in the U.S. elections

[705] EU Council decision (CFSP) 7299/19, Ibid, Article1, para 4.
[706] The seeds for the Stuxnet attack were apparently sown well before 2010. The worm was first detected in 2008, when it infected networks around the world, it did no damage to most systems. At first, it was assumed that the attack, which appeared to target nuclear facilities in Iran, was not successful. Yet, in the fall of 2010, reports spread that Iran's uranium enriching capabilities had been diminished. Stuxnet is the first computer virus known to be capable of specifically targeting and destroying industrial systems such as nuclear facilities and power grids.
[707] Treaty on the Non-proliferation of Nuclear Weapons of 1 July 1968, 729 U.N.T.S., p. 161. (entered into force on 5 March 1970)

to promote Donald Trump's campaign[708]. Similarly, cyber-attacks in Europe that targeted the elections in Ukraine, Bulgaria, Estonia, Germany, and France were investigators who considered that these cyber-attacks are attributed to suspected Russian hackers.[709] But the problem of attribution and definite evidence that links a group to a state is challenging though coerce intentions have been identified, which is another reason to promote and develop the due diligence principle to impose stricter rules on the responsibility of states in cyberspace.

To conclude, the right to non-interference and non-intervention is well established in international law and applicable to cyber activities and cyber actors (states and non-state), as long as states are the primary actors in the international system, especially if states are transparent about how international law applies to their cyber activities in theory and practice. But with no clear agreement on the criteria for its application, it will be left for the states themselves to decide what could be considered as a coercive intervention and what measures can be taken. Moreover, the target state will need to assess whether it has been the victim of an attempt by another state to deprive it of its independent will to exercise its sovereign rights by proving if there is evidence of the application of pressure by the adversary. Also, cyber intrusions that target or affect critical state infrastructure, will be coercive as such attacks will have a practical effect on the free will of the target state to exercise its sovereign functions over such infrastructure (Stuxnet case is an example). That will require also cooperation between the public and private sector in the context of cybersecurity with the rise of unconventional or low-intensity threats that featured inconclusive evidence of foreign involvement or hostile action being covertly structured to conceal or obscure any participation and responses. Nevertheless, it is important to differentiate between cyber intervention and other cyber activities that do not constitute intervention as there are many areas of activity that are a legitimate concern of the international community.

[708] Russian Hackers Acted to Aid Trump in Election, U.S. says, The New York Times, December 2016, https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?rref_collection%2Fnewseventcollection%2Frussian-election-hacking&action_click&contentCollection_politics&region_rank&module_package&version_highlights&contentPlacement=4&pgtype_collection

[709] Dorell O., Russia Engineered Election hacks and meddling in Europe. https://eu.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/

III- International Humanitarian Law and Hybrid Warfare

Armed conflicts are not illimitable, but bounded due to the efforts of scholars, theorists, and humanitarians throughout history that developed legal regimes to minimalize the harm of the use of force and the disastrous impact of armed conflicts.[710] These borderlines are developed to ensure the respect of human dignity and alleviate human suffering during an armed conflict. International Humanitarian Law (IHL) (also known as Jus in Bello or the Law of Armed Conflict "LOAC"), is the law that applies in armed hostilities through a set of rules that seek to limit the effects of armed conflict. This legal regime, a primary branch of international law, has originated in customary practices of armies and developed over the ages on all continents.

So in addition to conventional law as the main source of IHL, customary IHL is of particular importance as states that have not ratified IHL treaties, are still bound by customary law. Moreover, as there is less conventional law governing NIACs, customary law becomes vital to fill in gaps in the written law. The customary nature of conventions and treaties, which is reinforced by Article 1 of the GC, which removed the imposition of reciprocity when signing treaties, compels states to comply with IHL and its obligations. However, the rules of IHL are also applicable to armed conflicts between a State and armed opposition groups or between such groups, so they apply to all parties of the conflict. Some provisions in the Hague and GCs were reflections of existing customary law, therefore they are binding on all states regardless of ratification, and also on armed opposition groups in the case of NIACs. The reason why the application of customary international law is of high significance to NIACs, as treaty law has remained limited in some areas of such conflicts.

IHL can also be found in certain non-binding instruments, known as soft law that although may appear to be legal in nature, yet are not legally binding and cannot be enforced against the parties. One of the examples of soft law that supports the IHL treaties and customary international humanitarian law is the 2008 Montreux Document on pertinent international legal obligations and good practices for states related to operations of private military and security companies (PMSCs) during armed conflict[711]. The document details the legal obligations of

[710] Certain types of armed conflicts have been considered unlawful and have subsequently decline in number and even disappeared. Such as, wars to collect debts, wars of conquest, prohibition of targeting civilians during conflict or abusing prisoners. See, O'Connel M., What is War, An investigation in the wake of 9/11. Ibid. p.3

[711] For more information about the document, see https://www.icrc.org/en/publication/0996-montreux-document-private-military-and-security-companies and https://www.montreuxdocument.org/about/montreux-document.html

states with regards to PMSCs and their activities during a conflict and provides suggestions for best practices in how to implement those obligations. The role of soft law in such circumstances is highly relevant to contemporary conflicts, as states employ PMSCs to perform combat or combat-related operations, and that has increased in modern conflicts in terms of the number of conflicts they have been employed, and the range of tasks assigned to them. States, therefore, are required to make sure that PMSCs act in accordance with IHL and are familiar with its rules.

For IHL to apply to a situation of violence, it must involve an armed conflict by which that can be analyzed from different perspectives. Firstly, the temporal scope as IHL applies from the moment the armed conflict breaks even if parties of the conflict do not acknowledge the state of war. Secondly, material scope as different sets of rules apply to IAC and NIAC therefore the material scope is important to identify the nature of the conflict. And thirdly, the geographical scope, as IHL applies to the entire territory of the State(s) involved in the conflict, regardless of where the fighting is taking place. The preceding underlines the main difference between IHL that regulates the conduct of parties engaged in an armed conflict, and the Jus ad Bellum set out in the UN Charter that regulates whether a State may rightfully resort to armed force in its international relationships. By which the provisions of humanitarian assistance apply in cases of occupation, IACs, NIACs, and the event of natural or man-made disasters. Its legal framework serves as a vital tool to address such situations, advocate and achieve the protection of affected civilian populations.

Moreover, the IHL is concerned with the protection of non-combatants, and the behavior of the states and combatants during an armed conflict. IHL endeavors to minimize unnecessary harm throughout the armed conflict by establishing rules of the proper conduct of hostilities for humanitarian reasons. That includes, but is not limited to, protecting persons who are not or no longer participating in hostilities (hors de combat, which includes civilians, medical and humanitarian workers), prisoners of war (POW), limit casualties, and the appalling impact of armed conflicts by regulating the means and methods of warfare, seek to protect persons and property through outlining the rights and duties of states and NSAs during an armed conflict.

On the other hand, HW with no universally recognized definition combined with the increase of NIACs, are seen to be evolving in the contemporary scene, certain challenges to the applicability of IHL were noticed. HW in armed conflicts is not a new phenomenon, but their

multi-dimensional features fall short of all traditional classification of conflicts and rather combine their distinct characters in a single form creating a legal grey area. Besides, NSAs have evolved in power, involvement, and influence leading to uncertainties regarding the classification of armed conflict especially since some states deny their participation in armed violence, but rather argue that they are engaged in counter-terrorism operations not governed by IHL.[712]

Likewise, present-day NSAs have blurred the line of distinction between civilians and combatants, by upgrading their ability to establish an autonomous status that consists of State structure, deploying modern weapon systems ranging from high-tech arsenals and self-directed artilleries, and invulnerable ability to craft covert operations. At the same time, operating in urbanized territories where civilians and armed actors intermingle. Additionally, the classification and threshold of armed conflicts, whether IAC or NIAC, is flexible, especially with the additional rules provided by the APs to the GCs 1949. Though these rules define the field of application and do not extend to the entire law of armed conflicts, yet uncertainties and different substantive regulations especially with regards to the armed conflicts of both types of conflicts are of significant relevance to the legal gray area in contemporary conflicts.[713] Therefore, the conditions for the existence of a NIAC in terms of sufficient level of organization for the NSA, intensity of hostilities, and geographic scope of the NIAC remain a source of legal uncertainty.

The challenge in identifying the nature of an armed conflict (IAC or NIAC) was not created by HW but rather exploited by it. Hybrid adversaries have used the necessary means to take advantage of the gap between the two systems on one side, and the possible convergence on the other. According to Cassese, the two bodies of international law have converged with the result that internal strife is now governed to a large extent by the rules and principles which had traditionally only applied to IACs.[714] Similarly, the ICRC has taken the position that the insufficiency concerning content and coverage of treaty law applicable in NIACs should be

[712] Classification of Armed Conflicts, RULAC, Geneva Academy, online platform (last updated 21st of April 2017). https://www.rulac.org/classification#collapse2accord. Important to note, that States also tend to apply IHL to situations that do not amount to an armed conflict, because the rules governing use of force and detention of individuals for security reasons are generally less restrictive under IHL than under IHRL.

[713] The 1949 GCs and the 1977 Protocols contain around 600 articles of which on CA 3 to the 1949 GCs and the 28 articles of the AP II apply to NIACs. See, Boelaert-Siominen S., "Grave Breaches, Universal Jurisdiction and Internal Armed Conflict: Is Customary law moving towards a uniform enforcement mechanism for all armed conflicts?" Journal of Conflict and Security Law 2000, Vol. 5, at. 63.

[714] Moir L., The Law of Internal Armed Conflict, "Memorandum of 22 March 1996 to the Preparatory Committee for the Establishment of the ICC", Cambridge University Press 2000, p. 51.

addressed by analysis of custom and not the promulgation of further treat-based law.[715] But, what seems as convergence to erode the gap between the two legal regimes, is not in place yet. The ICTY in the Tadic appeal trial considered that the 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.[716] Mainly, the distinction between IAC and NIAC in a hybrid warfare scenario depends on the evidence of a state attribution to the conflict. State attribution is highly challenging in modern conflict due to state denial policy and covert operations, adding to this evidential legal uncertainty, the ICJ and ICTY understanding of whether applying a high degree of "effective control" or a lesser degree of "overall control" would highlight the challenges imposed to IHL from Hybrid adversaries.

Furthermore, the means and methods used by hybrid adversaries complicate the attribution to a particular type of armed conflict and the implementation of IHL. For example, collateral cyber activities which are inherently trans-border aggravate any approach to classification based on geographical factors. Therefore, cyber-attacks are very crucial once deployed in an armed conflict and raise questions about the fundamental principles of IHL and their full implementation in certain fields. From a humanitarian perspective, the challenge of cyber operations stems from the digitalization on which cyberspace is built, such digitalization ensures anonymity that complicates the attribution of conduct. And while IHL relies on the attribution of responsibility to individuals and parties to conflicts, major difficulties arise. For this chapter, cyber activities will be considered as those designed, intended, or used to cause injury or damage to an adverse party in an armed conflict, by that analysis will exclude cyber activities that fall below this threshold, such as espionage or financial hacks. In this regard, comparing cyber-attacks to kinetic operations and the possible collateral effect on civilians can be challenging due to the interconnected and dynamic nature of target systems and networks. So cyber-attacks on specific systems may have various repercussions on various other systems despite where they are located. Cyber operations conducted by state actors or NSAs that have similar effects to classic kinetic operations (destruction of civilian or military assets or cause

[715] Henckaerts J-M., The Conduct of Hostilities: Target selection, proportionality and precautionary measures under international humanitarian law", in the Netherlands Red Cross, Protecting Civilians in 21st-Century Warfare: Target Selection, Proportionality and Precautionary Measures in Law and Practice, 8 December 2000, p. 11.

[716] Prosecutor v Tadic, Decision on the Defense Motion for Interlocutory Appeal on Jurisdictions, 2 October 1995, para 128.

the death or injury of soldiers or civilians) are governed by IHL if occurred during an armed conflict.[717] So, states should use the existing processes developed for the purpose of kinetic operations as a general frame of reference and adapt them to account for the challenges posed by cyber operations. However, if such attacks did not result in any physical destruction or loss of lives, or conducted by civilian hackers, it remains unclear what is the status of such actors (combatants, civilians, or civilians directly participating in hostilities). In particular that states tend to blur the functions of the various organizations that can be involved in the conduct of cyber operations, as such operations involve cyber intelligence, private sectors, and private individuals. So, procedures must comply with IHL and states must put in place measures to spare the civilian population and objects.

Similarly, according to Tallinn Manual, the 2008 conflict between Georgia and Russia consisted of cyber operations that were launched by civilians and took place on belligerent territory during an armed conflict, therefore there was no doubt that IHL applied. However, the challenging legal question is whether cyber operations alone can qualify as armed conflicts to which IHL applies if there is no armed conflict in the first place. Moreover, the simple combination of a variety of actors to a single battlefield with the possibility of its extraterritorial effect that might spill over the territory of another state, with operations that combines a level of intensity that crosses the thresholds of one type of conflict and could stay below the threshold of another, is problematic by which it changes the nature of the conflict from a NIAC to an IAC or establish them both in parallel.

In this chapter, two main topics will be addressed, the distinction between NIAC and IAC, and the distinction between civilians and combatants in the context of HW. In doing so, the analysis will focus on the classification of hybrid armed conflicts and will highlight a general understanding of how to classify a conflict and identify its parties. Hence, selected situations will be examined in the light of IHL such as the annexation of Crimea that is relevant because it will examine the confusion created by annexation that did not meet the level of violence. Another scenario is the NIAC involving ISIS in Syria that reflects the role of NSAs in classifying a conflict that involves the territory of multiple States. Moreover, further examination will cover NSAs in NIACs and the geographic limitation of IHL with regards to cyber operations, and assess the spill-over conflicts and their impact on the classification paradigm. Also, HW, as explained before, creates confusion and flourishes in co-existing

[717] Tallinn Manual 2.0, Ibid, Rule 82, para 16.

conflicts. So, an examination of such types of conflicts is required and fits the challenging nature of hybridity that blurs the line of distinction between both classical categorizations.

Last but not least, selected issues related to principles of distinction will be addressed. Notably, analyzing this principle in the context of cyber operations is highly relevant to contemporary conflicts. In doing so, the distinction between civilian object and military objectives will be addressed in the cyber context, particularly the problems that arise with regards to dual-use infrastructure. And finally, will also examine in detail the problem of direct participation in hostilities under IHL. In that event, analyzing civilians' participation in hostilities through cyber means will require looking through the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities that was published in 2009, and Tallinn Manual experts' opinion on this matter.

1. International Humanitarian Law: Background

The law of armed conflict comprises the Geneva Conventions, the Hague Conventions, and several other treaties and laws, by which it was developed in an attempt to mitigate the atrocities of armed conflicts. However, means and methods of warfare have always been subject to certain principles and customs that are reflected in rules of international customary law, rules of ancient civilization, and religions. That has also been the case with regards to the classification of armed conflicts. For example, Christianity distinguished between external and internal wars to ensure that heretics and heathens do not benefit from the same treatment, which Christians are entitled to.[718] Also, Islamic rules have set different obligations and methods towards the adversary and differentiated between wars against unbelievers and wars against fellow Muslims.[719] Nevertheless, as the codification of the IHL started in the 19th century, that was strongly influenced by the Lieber Code of 1863[720], written to govern the conduct of Union forces during the American Civil War as the first example of the codification of the laws of war. The codification was striking a careful balance between humanitarian concern and

[718] Ibid. p, 40
[719] Ibid.
[720] Francis Lieber was the drafter of the first regulations on battlefield conduct through his publication "On Liberty and Self Government" in 1853, that triggered his desire to compile the customary rules of warfare. Later on, his Lieber Code was a great achievement that proposed a code of regulations for armies in field. These regulations have been developed into four principles of LOAC: the principle of distinction, military necessity, unnecessary suffering and proportionality. See, Schwarzenberger g., International Law: As Applied by International Courts and Tribunals, The Law of Armed Conflicts, Cambridge University Press 2004, p. 50.

military requirements of States. It is important to note that the ICRC[721]; was founded in 1863 at the initiative of Henry Dunant who witnessed and helped in easing the suffering of wounded soldiers at the battle of Solferino in 1859 and then lobbied political leaders to take more action to protect war victims; had an important role in such maturity. Henry Dunant campaigned for this cause and by August 1864, delegates from dozen countries adopted the first Geneva Convention (Hereinafter GC) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the field, which framed these inputs in a legal form and made it compulsory for armies to care for all wounded soldiers on both sides of the conflict.[722]

In parallel, the Hague Convention was a series of international treaties issued from international conferences held at The Hague in the Netherlands in 1899 and 1907. Although the first conference failed, yet it did adopt conventions defining the conditions of a state of belligerency and other customs relating to the war on land and sea. The convention focused on the prohibition to warring parties to use certain means and methods of warfare, and concerning issues such as the pacific settlement of international disputes and the laws and customs of war. That Hague convention is considered one of the two main treaty sources of IHL that was later amended and extended by the GCs. So, IHL splits into two different groups, the Geneva Law that deals with protected person and demands humane treatment, and the Hague law that deals with means and methods of warfare that limits the type of weapons, facilities, or strategy used within an armed conflict.

The process of establishing the rules of IHL has changed decisively after WWII and steered to the conclusion of three additional GCs for the protection of the victims of war as follows: (a) the second GC for the Amelioration of the condition of wounded, sick, and shipwrecked members of armed forces at sea, that came as a successor of the Hague convention 1907; (b)the third GC 1929 relative to the treatment of Prisoners of war; and (c) the fourth GC relative to the protection of civilian persons in time of war 1949.[723] With the four conventions revised and adopted, the whole set was referred to as the "GCs 1949" and ratified in whole or with

[721] ICRC is an independent, neutral and intermediate institution between parties to a conflict. ICRC acts as the guardian of the GCs and work on protecting the victims of hostilities and use its offices as hospitals and safe zones. Otherwise, the detaining power or state shall offer such service. See article 10 of the GCs 1949.
[722] ICRC Article on: Founding and early years of the ICRC (1863-1914), 12 May 2010. https://www.icrc.org/en/document/founding-and-early-years-icrc-1863-1914
[723] Jean Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law, vol. I, ICRC 2009, p. xxxii. See also, the GCs of 1949 and Additional Protocols, and their Commentaries, ICRC database. https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp

reservations by 196 countries to date, and they were considered the foundational treaties of the modern law of armed conflict or IHL.

Given that, the GCs have brought two fundamental changes, first in replacing the term "War" with "Armed Conflict", ensuring the applicability of IHL to an armed conflict regardless of whether it was declared or not. Second, the acknowledgment and extension of IHL to NIACs. This development was not seen as a novel step towards creating new types of conflicts that existed long before 1949, but it was the first time that international law codifies minimal rules to be respected during NIACs.[724] The various treaties of GCs deal mainly with the fate of persons who have ceased to fight or have fallen into the power of the adversary.

Correspondingly, armed conflicts are either international or internal. CA 2 of the GCs states that an IAC is a declared war or any other armed conflict which may arise between two or more States.[725] While CA 3 of the GCs applies to armed conflicts not of an international character occurring in the territory of one of the High Contracting Parties.[726] However, due to the development of new weapons, the decolonization after WWII that increased the numbers of states with new emerging humanitarian needs, and the evolving nature of NIACs, a diplomatic conference was held between 1974 and 1977 that drew APs to the GCs with great influence on the scope of applicability of IHL. By which the two branches of law covered in the Hauge and GCs were further developed by the first two APs to the GCs. To point out, the AP I apply to situations of declared war and armed conflicts between high contracting parties, including conflicts against colonial domination, alien occupation, and against racist regimes in the exercise of people's right of self-determination, as enshrined in the UN Charter and the Declaration on Principles of International law concerning Friendly Relations and cooperation among states under the UN Charter.[727] While the AP II of 1977, which supplements and develops CA 3 of the GCs, applies to armed conflicts between regular armed forces and dissident armed forces or other organized armed groups which are under responsible command, exercise a certain control over a part of the territory as to enable them to carry out sustained, concerted military operations and implement this protocol. A threshold that is higher than the one provided in CA 3 of the GCs with regards to NIACs, by which the key distinguishing factor

[724] The ICRC in 1948 has recommended to extend the GCs entirely to NIACs, but that was rejected by most states. Therefore, the agreement was to incorporate a single provision (CA 3) into the four GCs, which would be applicable in the case of armed conflict not of an International character occurring in the territory of one of the high contracting parties. See, Edlinger K., Ibid. p. 41

[725] Geneva Conventions 1949, CA 2, Ibid. and see Article 1 section 4 of the AP I.

[726] Geneva Conventions 1949, CA 3, Ibid., and see Article 1 section 1 of the AP II.

[727] AP I to the Geneva Conventions of 1949, Ibid., Article 1(4). See also, Edlinger K., Ibid. p. 42.

between the two regimes is that Article 1 of the AP II requires armed groups to have the ability to control territory. And finally, came AP III of 2005 relating to an additional distinctive emblem (the red crystal).[728]

The GCs and their APs have enjoyed universal ratification, frequent reaffirmation, and widespread integration into domestic law and military doctrine. Relatedly, numerous international treaties emerged, that is thought to reflect customary IHL, were binding to all states and parties to a conflict, and played a significant role in the continuous effort to alleviate the effects of armed conflicts. These treaties include but are not limited to the following, The 1954 Convention for the Protection of Cultural Property in the event of Armed conflict and its two protocols;[729] The 1972 Biological Weapons Convention;[730] The 1980 Convention on Conventional Weapons and its five protocols;[731] The 1993 Convention on Chemical Weapons;[732] The 1997 Ottawa Convention on anti-personnel mines;[733] The 2000 Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict;[734] The 2006 International Convention for the Protection of All Persons from Enforced Disappearance;[735] and The 2008 Convention on Cluster Munitions (CCM).[736]

1.1. Basic Principles of International Humanitarian Law

Additionally, justice in armed conflict is distinct from just war in jus ad Bellum, by which if the state lacks just cause of war, it may fight justly once an armed conflict occurs. That is based

[728] ICRC Article on: Founding and early years of the ICRC (1863-1914), Ibid.
[729] Convention for the Protection of Cultural Property in the event of Armed Conflict with Regulations for the Execution of the Convention 1954, The Hague, 14 May 1954. "it is the first international treaty with a world-wide vocation focusing exclusively on the protection of cultural heritage in the event of armed conflict."
[730] Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological and Toxin Weapons and on their Destruction, opened for signature at London, Moscow and Washington, 10 April 1972 (entry in force 1975). "The convention was the first multilateral disarmament treaty banning an entire category of weapons."
[731] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be excessively Injurious or to have Indiscriminate Effects, Geneva, 10 October 1980.
[732] Convention on the Prohibition of the Development, Production, Stockpiling and use of Chemical Weapons and on their Destruction, Paris 13 January 1993 (entry in force April 1997).
[733] Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, 18 September 1997 (entry in force March 1999).
[734] Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, 25 May 2000 (entry in force February 2002).
[735] UN General Assembly, International Convention for the Protection of All Persons from Enforced Disappearance, 20 December 2006, available at: https://www.refworld.org/docid/47fdfaeb0.html (accessed 11 February 2021).
[736] The Convention on Cluster Munitions was concluded by the Dublin Diplomatic Conference at Dublin on 30 May 2008. "The Convention on Cluster Munitions is a humanitarian imperative-driven legal instrument which prohibits all use, production, transfer and stockpiling of cluster munitions."

on the morally exceptional character of armed conflict reflected in the principles of IHL. The morally exceptional nature of warfare means that its main goal is to reach a peaceful conclusion with fewer costs that is the main fundamental idea behind the doctrine of humanitarianism that balances the military necessity and humanitarian concerns for all victims of warfare.[737]

First, the *Principle of Distinction* requires the parties of armed conflict to distinguish, at all times and under all circumstances, between combatants and military objectives on the one hand and civilian objects on the other. Such right is exempted in case civilians took part in hostilities[738]. This principle was first outlined in the St. Petersburg declaration, stating that: "the only legitimate object which states should endeavor to accomplish during war is to weaken the military forces of the enemy"[739]. According to the Kassem case in 1969, Israel's Military Court at Ramallah recognized the immunity of civilians from direct attack as one of the basic rules of international humanitarian law[740]. The principle is then merely understood as a clear distinction of military targets from the civilian environment, by which it should assure that military operations shall target only military targets (combatants and military objectives). This principle also prohibits indiscriminate attacks under AP I article 51(4), that are incapable of distinguishing between civilians or civilian objects and military objectives, or that occur where the effects of the attack cannot be limited as required by IHL.

Second, the *Principle of Necessity and Proportionality* by following the rule that a belligerent can only apply the amount and kind of force necessary to defeat the enemy, without causing loss of civilian life by excessive attacks[741]. And every feasible precaution by belligerent must be taken to avoid civilian causalities.[742] This is not easily assessed especially since the military commander must act reasonably in the circumstances prevailing at the time using the knowledge they have acquired in fulfillment of their obligation to take precautions in attack. So the lawfulness of such attacks does not depend solely on the outcome but must include the knowledge factor of the commander.

Third, the *Principle of Humane Treatment* requires that civilians are always treated humanely, prohibiting by that any violence to life and person including torture or cruel treatment[743]. This

[737] Crowe J., and Westond-Scheuber K., Principles of International Humanitarian Law, 2013, p. 2.
[738] See, AP I, Arts 48, 51-52, 57; AP II, Arts. 13-16.
[739] St. Petersburg Declaration, preamble, cited in Vol. II, Ch. 1, p. 83.
[740] ICRC, Customary IHL, Israel "Practice relating to Rule 106.", Conditions for Prisoner of War Status, Section A, Chapter III.
[741] See, AP I, Arts. 35, 51(5).
[742] See, AP I , Arts. 57,58.
[743] ICRC, Geneva Convention IV, Art. 27, see also CA 3 of Geneva conventions 1949.

rule has been established by state practice as a norm of customary international law and is applicable in both IACs and NIACs. For example, treating the prisoners of war humanely was recognized in the Lieber Code[744], and Hague regulations[745]. Humane treatment is an overarching concept, yet according to CIHL rules, it includes but is not limited to certain categories of persons: the wonder, sick and shipwrecked, persons deprived of their liberty, displaced person, women, children.[746]

Fourth, the *Principle of non-discrimination* requires that all protected persons shall be treated equally by parties to the conflict without any distinction based on religion, race, sex, or political opinion[747] . Besides, preferential treatment is given to women and children during an armed conflict requiring that children under 18 must not take part in hostilities[748]. As seen the principles provide general protection for civilians and civilian objects and apply only to military operations that qualify as attacks defined under IHL.[749]

Therefore, once a situation is classified as an armed conflict, IHL directly comes into force through a set of rules that applies to the belligerent behavior, protection of non-combatants including civilians and their properties, as well as the respect of the environment. So, the 1949 GCs established the modern distinction between types of conflicts.[750] However, due to the transformation of international relations, the nature of armed conflicts, and the dividing line between war and peace that have been blurred with the evolving features of warfare, specifically in the era of HW, the IHL has been facing significant challenges that need to be addressed. Nonetheless, the notion of responsibility is an essential part of the implementation and respect for the law and its basic principles. The reason why IHL provides several obligations that trigger the international responsibility of states in case of violations.

---

[744] Liber Code, Article 76, Vol II, Chapter 32, p. 215.
[745] Hague Regulations, Article 4(2), p. 206.
[746] IHL Database, Customary IHL , Chapter 33-34. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter33
[747] See, AP I , art. 75(1). also, common art 3 GC. IV Art 27.
[748] ICRC, Geneva convention IV, art. 24, 27. see also, AP I Arts. 76-78, AP II Art 4 (3).
[749] The notion attack under IHL, defined in article 49 of the 1977 AP I, is different from and should not be confused with the notion attack under article 51 of UN Charter. Specific cyber operation or type of cyber operations for instance that amounts to an attack under IHL, does not necessarily mean that it would qualify as an armed attack under the UN Charter. See, ICRC Report on Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict, ICRC Expert Meeting 21-22 January, 2021, p. 41.
[750] Eve La Haye, War Crimes in Internal Armed Conflicts, Cambridge Studies in International and Comparative Law, Cambridge 2008, p.5.

1.2. Responsibilities and Violations of States under International Humanitarian Law

A State is responsible for violations of international humanitarian law attributed to it. State practice establishes this rule as a norm of customary international law applicable to violations committed in both IACs and NIACs. Equally important, is the responsibility of states for violating IHL by which to determine such violation, the conduct of individuals or groups must be attributable to the state, even if the state did not authorize the violation, it still holds responsibility. States also may be responsible for the wrongful acts of NSAs over which they exercise effective control. This is similar to the attribution discussed in the previous chapter, nonetheless, the difference is that such violation occurs in an armed conflict. One of the challenges that surround such responsibility is that usually, it is a matter for diplomatic discussion by which in an ongoing armed conflict, parties of the conflict are not conducive to such dialogue.[751] Nonetheless, once such violations occur and attribution has been determined, the state will be held responsible for violations of IHL. Consequences can include UNSC sanctions, such as arms embargoes, financial sanctions or travel bans, or even the use of force against that state. State responsibility for failing to respect obligations under IHL can be triggered before the ICJ by other states suffering damages related to such violations and can lead to compensation. In addition, if a State failed to prosecute perpetrators of war crimes, crimes against humanity, and genocides at the national level may in certain circumstances trigger the competence of the ICC. The court jurisdiction is established by the State ratification of the ICC statute or by the binding decision of the UNSC when the state is unwilling or unable to prosecute alleged offenders.[752]

States must undertake to respect and ensure respect for the GCs in all circumstances.[753] The responsibility of states is confirmed in both treaty and customary IHL. A study published by ICRC in 2005 highlighted the rules of customary IHL and drew the following obligations on states in connection with their actions in IAC and NIAC.[754]

A State is responsible for violations of international humanitarian law attributable to it, including:

- Violations committed by its organs, including its armed forces;

[751] International Humanitarian Law: A Handbook for Commonwealth Parliamentarians, Commonwealth Parliamentary Association (CPA), September 2019, p. 30.
[752] Rome Statute of the International Criminal Court (hereinafter Rome Statute), 17 July 1998, 2187 U.N.T.S, entered into force 1 July 2002, Article 17.
[753] Geneva Conventions I – IV, Article 1. See also, AP I, Article 1 and Article 80..
[754] Henckaerts, Jean-Marie, and Louise Doswald-Beck, eds. Customary International Law . Vol. 1, The Rules . Cambridge: Cambridge University Press, 2005, part 6.

- Violations committed by persons or entities it empowered to exercise elements of governmental authority;
- Violations committed by persons or groups acting in fact on its instructions, or under its direction or control;
- Violations committed by private persons or groups that it acknowledges and adopts as its own conduct (Rule 149).

In addition, a State responsible for violations of international humanitarian law in the context of an international or a non-international armed conflict is required to make full reparation for the loss or injury caused (Rule 150). Moreover, states must investigate war crimes allegedly committed by their nationals or armed forces, or on their territory, and, if appropriate, prosecute the suspects. They must also investigate other war crimes over which they have jurisdiction and, if appropriate, prosecute the suspects (Rule 158). Finally, states must make every effort to cooperate, to the extent possible, with each other to facilitate the investigation of war crimes and the prosecution of the suspects (Rule 161).

The ICJ has held in several cases that the conduct of a State organ always triggers the responsibility of that state, without having to prove that this group acted under the State's orders or acted in contrary to the instructions given. For example, in the Armed Activities on the territory of the Congo case, the ICJ affirmed that "according to a well-established rule of international law, which is of customary character, the conduct of any organ of a State must be regarded as an act of that State." [755] In the same case, the ICJ held that it was also irrelevant for the attribution of their conduct to Uganda whether the UPDF soldiers acted contrary to the instructions given or exceeded their authority. The court asserted that "according to a well-established rule of a customary nature, as reflected in Article 3 of the Fourth Hague Convention respecting the Laws and Customs of War on Land of 1907 as well as in Article 91 of Protocol I Additional to the Geneva Conventions of 1949, a party to an armed conflict shall be responsible for all acts by persons forming part of its armed forces"[756]. Therefore, while states will be responsible for violations attributable to it, the individuals who commit such violations will be prosecuted based on the gravity of the offense or crime. In which violations of IHL are not necessarily war crimes, as the GCs require states to criminalize certain serious violations of IHL, known as grave breaches. The judicial enforcement of IHL relies on national courts, which was foreseen by the GC 1949 which imposed an obligation of states to incorporate the

[755] Armed Activities on the Territory of the Congo [Democratic Republic of the Congo v. Uganda], Judgment, ICJ Reports 2005, p. 168, para. 213
[756] Ibid., para 214.

relevant rules of IHL into domestic legislation, to enforce international law governing armed conflicts through national courts.[757] By which the jurisdiction of the main permanent international courts, ICC that is competent to determine individual criminal responsibility for war crimes, and ICJ that is competent to determine State responsibility for IHL violations in armed conflicts and to render advisory opinions on such cases, are restricted by State sovereignty as laid down in Article 2(7) of the UN Charter-based on the domestic jurisdiction, that does not create an obstacle to the judicial enforcement of international law, rather it endows national courts with a special role in enforcing international law.[758]

Similarly, AP II related to violations of IHL in NIACs, CA 3 and AP II of the GCs did not mention the possibility of criminal prosecution for violations. Yet, it is generally accepted that individual criminal responsibility arises for certain serious violations of IHL, regardless of whether they are committed in an IAC or NIAC.[759] For the national courts to have such jurisdiction that involves cases that violate IHL in NIAC or IAC, the rule of law requires courts to be independent, impartial, accessible, and able to provide effective and equal enforcement of the law. That is assessed based on structural conditions that empower courts to enforce IHL and functional conditions that refer to the court's de facto enforcement of IHL.[760] That is of high interest to the international community to ensure that national courts are equipped and well placed to perform the role within the domestic legal order.

Nonetheless, in practice violations of IHL might be hardly detected as the areas of conflict zones are often inaccessible, destruction of physical evidence, and deliberate spread of misinformation about the actual conduct by belligerents. However, AP I of the GCs has established the International Humanitarian Fact-Finding Commission (IHFFC)[761], which consists of an expert body to respond to incidents concerning IHL during an armed conflict. But that will rely on the consent of the parties to a conflict that needs to accept the authority of the Commission by depositing an "Article 90" declaration.[762] Also, other UN mechanisms play a vital role in fact-findings such as the special rapporteurs, independent experts, and working groups established under the IN Human Rights Council's special procedures.

---

[757] See, Common paragraph 1 of articles 49,50,129,146 to the four GCs 1949. Also, Article 85(1) of the AP I to the GCs 1949.
[758] Weill S., Building respect for IHL through National Courts, ICRC review, 2014, vol. 96, p. 860-861.
[759] [759] International Humanitarian Law: A Handbook for Commonwealth Parliamentarians, Ibid. p. 32.
[760] Weill S., p. 862.
[761] AP I of the GC 1949, Ibid. Article 90.
[762] International Humanitarian Law: A Handbook for Commonwealth Parliamentarians, Ibid. p. 30-31.

Consequently, the distinction between peacetime and wartime is fundamental for the application of different legal regimes, thus it is vaguer in contemporary conflicts. For example, according to Marco Sassolli, the victims of IHL violations often have no other remedy than to try and trigger a procedure before a human rights body, however, such bodies sometimes neglect the specificities of IHL and armed conflicts.[763] This brings us to the role of both the IHL and IHRL in promoting the protection of individuals and the reason why they both interplay although they do not occupy the same space at the same time. Both bodies of rules are considered to be complementary, but they can contradict too due to the expansion of IHL to cover NIACs and the increased application of IHRL to conflict situations that led to co-application by reinforcing one another, at the same time generated a normative tension that requires a certain form of regulation.

1.3. The Relationship between IHL and IHRL

First, both bodies of law have similarities in the strive to protect the lives, health, and dignity of individuals. But these two branches of public international law have developed separately through different treaties and have a different scope of application. The Human Rights law originally was a matter of constitutional law, an internal relation between government and its citizens, but after WW II it became a body of international law. IHRL is a law crystallized by the adoption of the Universal Declaration of Human Rights 1948 (UDHR), with sets of international rules established by treaties, customary rules, and soft law principles forming the IHRL that operates at all times.[764] On the other hand, IHL that developed from the pre-charter Hague and Geneva law is traditionally based on the humane expectations between states at war as civilized behavior and developed to regulate inter-state relations reflecting their common interest in minimizing the devastating impacts of armed conflicts and limited to the territories involved.[765] Comparably, IHRL developed in post-1945 focusing on the legal relations between governments and individual rights holders, finds its roots in the International Covenants on Civil, Political Rights, and Economic, Social and Cultural Rights of 1966

[763] Application of International Humanitarian Law and International Human Rights Law in an Armed Conflict, Conference by the International Institute of Humanitarian Law, San Remo - Italy 2019, p. 8.
[764] Droege C., The Interplay between International Humanitarian Law and International Human Rights Law in situations of Armed Conflict, International Law Forum, University of Jerusalem, ICRC, 26\12\2007, p. 313.
[765] Meron Th., On the Inadequate Reach of Humanitarian and Human Rights Law and the Need for a New Instrument, 77 AM. J. INT'L L. 554, 592 (1983).

(ICESCR).[766] This body of law applies in the situation of peace and war alike "lex generalis", while IHL applies during an armed conflict "lex specialis". In this respect, IHRL appears to be more protective than IHL, but its rules may not be realistic in an armed conflict.[767] So, although both have different origins and rules, yet there has been convergence and interplay from the adoption of the UDHR in 1948 that have influenced the codification of GC 1949 and its APs.[768]

To clarify, the "lex specialis" under international law is a situation governed by a specific rule which makes it deviate from the general rule "lex generlis". When the two principles coincide, then the complementarity and mutual reinforcement are reflected, however, when they are not completely compatible, it is the interpretation principle of "lex specialis" that is invoked and the norm that is best tailored to the situation prevails. Such principle is reflected in the writings of Hugo Grotius that considered any conflicting between special and general rules, the former is more effective. Also, the advisory opinion of the ICJ in the Nuclear weapons case has noted that the two sets of norms, IHL and IHRL, should be interpreted in harmony on the principle of systemic integration.[769] Similarly, in the advisory opinion in the Wall case, the ICJ has noted that in matters that relate to both IHL and IHRL, both will be taken into consideration.[770] In other words, under certain circumstances, the specific rules of human rights law are applied by reference to IHL standards, and the closer the situation is to the battlefield, the more IHL will take precedence, and vice versa. So, the ICJ has defined an exclusive framework of these rights regarding their applicability in distinct circumstances but also acknowledged that when in situations where both IHL and IHRL apply simultaneously, the doctrine of lex specialis applies. Therefore, it is accepted that IHRL continues to apply to states both in times of peace and

[766] ICRC, International Humanitarian Law and International Human Rights Law "Similarities and Differences", Advisory services 2003.
[767] Application of International Humanitarian Law and International Human Rights Law in an Armed Conflict, Ibid. p. 8.
[768] See, for example, AP I, art. 54, para. 1, on the prohibition of civilian starvation
[769] ICJ, Advisory opinion on the Legality of the threat or Use of Nuclear Weapons, Ibid. para. 25. See also, Milanovic M., The Lost Origins of Lex Specialis: Rethinking the relationship between Human Rights and International Humanitarian law, Ohlin Ed., in Theoretical Boundaries of Armed Conflict and Human rights, ASIL Studies in International Legal Theory, Cambridge University Press 2016, p. 78.
[770] ICJ, Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory opinion 2004, para. 105. The court stated that "the protection of the International Covenant on Civil and Political Rights does not cease in time of war, except by operation of Article 4 of the Covenant whereby certain provisions may be derogated from in a time of national emergency." It also added that: "the test of what is an arbitrary deprivation of life fails to be determined by the applicable lex specialis, namely, the law applicable in armed conflict which is designed to regulate the conduct of hostilities". The court, concerning the relationship between IHL and IHRL, has stated that there are three possible situations: "some rights may be exclusively matters of international humanitarian law; others may be exclusively matters of human rights law, yet others may be a matter of both branches of international law."

armed conflict unless the state has derogated from the relevant human right if that derogation is lawful.

However, it will be challenging to determine which conflicting rule constitutes the "lex specialis" in every specific situation. For instance, the ECHR in Hassan v. the United Kingdom case, concerning the capture of the applicant's brother by British armed forces and his detention at Camp Bucca in Iraq, considered that both IHL and European Convention of Human Rights provide safeguards from arbitrary detention in time of armed conflict and that the grounds of permitted deprivation of liberty set out in Article 5 requires that both laws should be accommodated, as far as possible, with the taking of POW and the detention of civilians who pose a risk to security, under the third and fourth GCs.[771]

Moreover, states are allowed to suspend certain human rights provisions for emergencies, which trigger misconception to exempt such rights in armed conflicts, even though international law is clear that such derogations do not involve international obligations of states towards others, such as discrimination solely on the ground of race, color, sex, religion[772]. Therefore, if derogation clauses exist, suspension of certain rights applies, but that does suspend the limit of other rights which makes human rights apply even in armed conflict but in a modified manner. On the other hand, the right of derogation does not apply to IHL, as its rules are only applicable during armed conflicts[773], which makes IHL unsuspended with the only exception of Article 5 to the fourth Geneva Convention[774]. Derogation from the right to life under human rights laws are strictly limited to exceptional circumstances and can be invoked only in time of war or other public emergency threatening the life[775], while killing is allowed in a less limited circumstances in wartime under the IHL.

IHRL and IHL are traditionally two separate branches in law, yet the development and practices showed not only common features but also common integration in practice. One of the finest examples of this co-application is the "Guiding Principles for Internally Displaced Persons" that bring together existing human rights and humanitarian law alongside the

[771] European Court of Human Rights (ECHR), case of Hassan v. The United Kingdom, Judgment 16 September 2014, para. 104.
[772] Ibid. p. 318.
[773] ICRC, What is the difference between Humanitarian Law and Human Rights Law? Resource Centre 2004, www.icrc.org.
[774] ICRC, Convention (IV) relative to the protection of Civilian Persons in Time of War, Geneva,12 August 1949, Art.5.
[775] ECHR, Guide on Article 15 of the European Convention on Human Rights, Derogation in time of emergency, Article 15, para 2. (Updated on 31 December 2021)

framework for refugee law[776]. Numerous treaties were established based on such cooperation, such as "the Convention on the Rights of the Child of 1989[777], the Rome Statute of the International Criminal Court[778], the Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict 2000[779], the Basic Principles and Guidelines on the Right to a Remedy and Reparation for Victims of Gross Violations of International Human Rights Law and Serious Violations of IHL[780].

On the other hand, the two bodies of laws contradict. For example, the IHL success depends on discretion and neutrality, while IHRL deals with accountability and/or responsibility. At the same time, the IHRL binds only states within the territory of that state or when people are subject to the state's jurisdiction. In other words, IHRL governs the relationship between a State and persons within its territory or jurisdiction across a wide spectrum of conduct, while IHL that governs NIACs applies to both states and NSAs.[781] That does not mean that both states and NSAs are equal under domestic law, as NSAs are bound by such law and will be prosecuted for any crimes or violations. IHL's main concern is protecting those who are no longer part of hostilities, while IHRL aims to protect everyone during peacetime from arbitrary behavior by their governments, so IHRL does not deal with the conduct of hostilities.[782] As well, the applicability of IHRL to NSAs can face restrictions due to the challenging factor of full compliance based on the fact that NSAs cannot perform government-like functions on which the implementation of human rights norms is premised. Also, the extraterritorial application of IHRL arises under two conditions. Firstly, when an individual is under the authority and control of the agents of the state in question, for example when a state's armed forces detain people outside that state's territory. Secondly, where the state has effective control of an area outside its borders, such as during a military occupation. So even if a state is involved in an armed conflict overseas, it will have obligations under both IHL and IHRL.[783] Therefore, it is generally accepted that the IHRL applies in armed conflicts, but whether and to what extent it applies extraterritorially and if it addresses NSAs, is still controversial. For

[776] Overlapping Areas of Law: "Towards a Comprehensive Legal Framework", www.gsdrc.org
[777] Convention on the Rights of the Child of 1989, art. 38, Nov. 20, 1989.
[778] Rome Statute of the International Criminal Court, July 1, 2002.
[779] Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict 2000, Nov. 20, 1989.
[780] United Nations, General Assembly Resolution 60/147, 16 December, 2005.
[781] ICRC, 31st International Conference of the Red Cross and Red Crescent, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Geneva October 2011, p.14
[782] What is the difference between Humanitarian law and Human Rights Law? Ibid.
[783] International Humanitarian Law: A Handbook for Commonwealth Parliamentarians, Ibid., p. 54-55.

example, the rise of NSAs involved in terrorist operations that are undertaken in the context of NIACs led to certain misconceptions in the application of IHL and IHRL. Taking into consideration that some states consider that such operations are armed conflicts of terroristic and unlawful nature that require the applicability of IHL. While other states believe that such applicability of IHL can give legitimacy to NSAs. This creates a blurring effect on the lines between armed conflict and terrorism challenging the application and integration of IHL. The challenging aspect lies mainly in the lack of comprehensive and harmonized response from states and the UN that has resulted in the establishment of new and expansion of existing counter-terrorism measures.[784] States showed a tendency to deny the application of IHL in favor of counter-terrorism regulations, particularly in the prosecution of genocide, crimes against humanity, and war crimes. That has produced inconsistencies in the identification and prosecution of war crimes that undermine the shared goal of human rights and humanitarian law in preventing unlawful conduct in armed conflict.[785] By which undermining one body of legal norms has significant consequences and implications for the effectiveness of the other.

Besides, the parallel approach of both IHL and IHRL with regards to the complexity of situations that might involve armed operations such as rebellions within an armed conflict, and internal disturbance such as protests that fall within law enforcement, is problematic because the co-application might simply become a cumulative application, whereby states are required to comply with the most demanding legal norm. The evolving interest in co-application of both bodies of law is because IHL has only the ICRC as an international monitoring body, while IHRL has developed courts, commissions, and committees that are involved in armed conflicts and crimes violating the principles of international law. This means that many incidents which occur during an armed conflict are currently being considered by IHRL bodies such as the ECHR. Similarly, the emerging and evolving role of ICC that was created by the 1998 Rome Statute to try cases relating to IHL to repress inter alia war crimes, has pushed further towards regulating the legal relationship between IHL and IHRL because the ICCs enforce international criminal law that in return enforces the norms of both bodies of the law creating specific criminal prohibitions.[786] For example, the ICTY had the mandate to prosecute persons

[784] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 32IC/15/11, 2015, p. 17.
[785] Report of the Special Rapporteur "Fionnuala Ni Aolain" on the promotion and protection of human rights and fundamental freedoms while countering terrorism General Assembly, 3 September 2020, 75th session, p. 11-12.
[786] Ibid., p. 8.

responsible for grave violations of international law. The grave breaches that are set in the GC of 1949 are similarly reproduced in Article 2 of the ICTY statute stating that the court shall have the power to prosecute persons committing or ordering to be committed grave breaches of the GCs namely the acts against persons or property protected under the provision of the relevant GC of 1949.[787] In addition, the implementation procedure of IHRL and IHL rests on States, by which the implementation of IHL requires states' procedures with the key role of ICRC as a monitoring body in ensuring respect for the Humanitarian rules.

To sum up, IHRL had played a very important role in filling the international legal gap identified before its dramatic development. It is majorly in NIACs that was expressed in CA 3 of the GC 1949, by which the assumption was that unless IHL norms apply to such conflicts, states activities were unrestrained by international law. But with the development of IHRL, this assumption is no longer valid.

It has been concluded that, despite the differences between those two branches of international law starting from origin up to the fundamental differences in implementation, it has been noticed that they both work in parallel application filling the normative gaps in the protection of individuals, mainly in the right to life, the prohibition of torture and enhances possibilities of accountability for law-violations and remedy for victims. However, the "lex specialis" rule introduced by the Nuclear Weapons advisory opinion, may not be as effective as desired. In which the concept of hybrid adversaries and conflicts of hybrid nature involving non-state armed groups or cyber militias can create a gap, yet that can lead in the future to the adoption of the more developed co-application rule as seen in the "Hassan v. UK" ECtHR case in which the court stressed that "even in situations of international armed conflict, the safeguards under the convention continue to apply, albeit interpreted against the background of the provisions of international humanitarian law". This approach was also adopted at a national level by the Israeli Supreme court that considered a civilian taking a direct part in hostilities cannot be attacked at such time if a less harmful means can be employed.[788] The judgment takes into consideration the complexity of the conflict and the obligations of the State of Israel relating to the residents of the Gaza strip, that derives from the state of armed conflict that exists

[787] Statute of the ICTY for the Prosecution of persons responsible for serious violations of IHL committed in the territory of the former Yugoslavia since 1991, U.N. doc S/25704 at 36, annex 1993 and S/25704/Add.1 1993, adopted by Security Council on 25 May 1993, article 2.
[788] Public Committee against torture in Israel v. Government of Israel (targeting killing case), HCJ 769/02, IsrSC 2006, para 40.

between Israel and Hamas organization that controls the strip and from the degree of control exercised by Israel over the border crossing. Another example can be found in the International Commission of Inquiry on the Gaza border protests[789] (that do not reach the threshold of armed attacks), the commission found that even if an armed conflict is occurring and demonstration was organized (including militants), then IHRL rules involving law enforcement prevail over IHL rules, setting the bar of the use of lethal force against demonstrators in prohibiting the targeting of individuals in the crowd if based purely on their membership in an armed group.

2. Applicability of Jus in Bello to Hybrid Warfare

In the previous chapter, the complexity of HW means and tools to the legality of the threat or use of force in international relations was highlighted. It acknowledged the challenging nature of hybrid adversaries, particularly the attribution problem to state responsibility and the threshold of these operations. However, in this chapter discussions will focus on armed conflicts, whether IAC and NIAC or even the internationalization of a NIAC as a result of a third State military intervention on the side of the rebels concerning HW. Additionally, will portray the impact of cyber operations, hybrid non-state groups or adversaries in light of the IHL (customary and treaty), its basic principles, legal framework, challenges imposed, and possible remedies.

Various elements should be taken into consideration while addressing the challenges of HW to IHL. First of all, the novelty of certain phenomena such as cyber-attacks to IHL that had changed the way armed conflicts are conducted especially since the current legal norms emerged at times where new technological means were not in the horizon. Secondly, difficulty in distinguishing between civilians and combatants, the ambiguity of conflict classification that is the main rule to determine the applicable law and highly challenged by the hybrid nature of contemporary conflicts, and the fusion of direct and indirect approaches to warfighting. The previous are relevant to the legal complexity created by HW, as traditional international law is based on binaries such as the distinction between war and peace to know what legal framework is applicable internationally and nationally, and once an armed conflict is confirmed it is important to determine the legal character of the conflict as to whether it is international or not.

[789] Report of the detailed findings of the independent international Commission of inquiry on the protests in the Occupied Palestinian Territory, A/HRC/40/CRP.2, 18 March 2019, para. 106

Finally, the impact of HW on the principles of distinction, proportionality, and the prevention of unnecessary suffering, in line with the general rules governing the conduct of hostilities. While the LOAC is based on a subtle equilibrium between principles of necessity and humanitarian consideration to ensure that the force applied on the battlefield allows the accomplishment of the mission whole taking appropriate humanitarian considerations into account,[790] the emerging complexity of the modern battlefield is undermining the confidence in LOAC and its ability to regulate hybrid operations.

In the same sense, hybrid operations are quite fertile in fragile or failed states due to the strong correlation between state fragility and conflict. According to the World Bank, fragile states share a common fragility in two particular aspects: "state policies and institutions are weak in these countries, making them vulnerable in their capacity to deliver services to their citizens, to control corruption, or to provide for sufficient voice and accountability. They face risks of conflict and political instability."[791] From a legal point of view, a failed or fragile state is one which, though still retaining legal capacity, has for all practical purposes lost the ability to exercise it. The key element is the lack of an effective body that can commit the state in a binding way to for example conclude an agreement.[792]

In the current setting, many countries are addressed as fragile states with a permissive environment for NSAs and third states to operate in a hybrid manner. For example, Syria and Iraq in the aftermath of internal stability and NIAC that shifted to an internationalized conflict after the involvement of state actors in support to one of the parties to a conflict, or even in the operations against certain military groups such as ISIS. Also, Lebanon's fragile situation with corruption, NSAs (Hezbollah's influence in the region), and the guidance of regional powers such as Syria, Iran, Saudi Arabia, and Israel in shaping the political situation in the country. Likewise, the conflict in Ukraine starting from the Euromaidan revolution in 2014 that escalated to internal conflict in eastern Ukraine, the annexation of the Crimean Peninsula, and confrontation with Russia in many instances including the maritime incident after the Russian attack and seizure of Ukrainian naval vessels off the Crimean Peninsula. These incidents in fragile countries have been a perfect pattern of the link between fragility and conflicts and have resulted in decreased attempts to use conventional warfare and a higher likelihood of using

[790] Dinstein Y., The Conduct of Hostilities under the Law of International Armed Conflict, Cambridge University Press 2004.
[791] Grono N., Fragile States and Conflict, Speech by the Deputy President of the International Crisis Group, Brussels, 27th March 2010, https://www.crisisgroup.org/global/fragile-states-and-conflict
[792] Thurer D., The "Failed State" and International Law, ICRC 31st December, 1999, No. 836.

HW tools. Some of the most relevant tools that are developed and employed in such fertile environments are:

- Disinformation is used to weaponize information to gain influence by leveraging social media through propagation or the ability to spread narratives and themes to an audience far and wide.[793]
- Political and Economic Coercion relies on the tools to influence the political and economic status of another state towards the adversary's benefit and interests. Such tools can vary from election interferences to debt traps such as the Belt and Road Initiative (BRI) launched by China spanning a multitude of projects designed to promote the flow of goods, investment, and people.[794] Some of these projects are underway, such as the China-Pakistan Economic Corridor (CPEC), a 3000 km corridor that runs from Chia's Kashgar to Pakistan Gwadar.[795]
- Cyber Operations are quite successful in fragile states or war-torn states due to weak cybersecurity systems, lack of cyber regulations, and the role of multiple actors in a failed governed system. Cybercriminal networks prefer operating in functional but corrupted countries that provide baseline political order where sovereignty provides some protection from external interdictions. One example is the Syrian Electronic Army (SEA), a group of hacktivists that was formed in 2011 from patriotic hackers supporting the Assad regime. Despite their denial of any connection to the Syrian government, yet their self-assigned mission to protect the homeland and support the reforms introduced by President Bashar Al-Assad is evidence of their connection and role in the ongoing conflict in Syria. [796] Currently, there is no binding legal framework under international law that governs cyber

[793] Twitter is one of the tools used to spread disinformation via social bots that create thousands of fake accounts that can simultaneously broadcast hashtags and topics thousands of times advancing adversary's narrative into the trending topics on the platform (Twitter). See Watts C., Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions, October 2017, https://securingdemocracy.gmfus.org/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions/

[794] BRI that was announced in 2013 (also known as One Belt, One Road) aimed to strengthen China's connectivity with the world. The initiative involves 138 countries with a combined Gross Domestic Product of $29 trillion and some 4.6 billion people. The initiative's main asset is that Beijing has injected massive amounts of capital into Chinese public financial institutions (such as the Chinese Development bank "CDB" and the Export-Import Bank of China "EXIM") to allow these institutions to finance Chinese State owed enterprises with low borrowing costs and offer them highly competitive bids for projects around the world. See, China Power Team. How Will the Belt and Road Initiative advance China's Interests? CSIS, May 8, 2017, Updated August 26, 2020. https://chinapower.csis.org/china-belt-and-road-initiative/

[795] Ibid.

[796] Al-Masry A., The new face of the Syrian Electronic Army "SEA", May 17, 2018. https://chinapower.csis.org/china-belt-and-road-initiative/ . The SEA was behind several operations such as hacking the Associated Press's Twitter account in 2013, tweeting that the White House had been under attack and that President Obama had been injured, a three-minute hack that reportedly caused a $136 billion drop in stock markets.

warfare. While the AP I highlighted the study, development, acquisition, or adoption of new weapons and methods of warfare, and set the obligation on states to determine whether its employment would be prohibited by this protocol or by any other rule of international law applicable[797]. But the legal gap is recognizable by which the international community has witnessed numerous cyber incidents that indicated the serious concerns behind these newly emerging threats.[798] For instance, the confusion that cyber civilian hackers create was also reflected in Rule 29 of the Tallinn Manual which states: "civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection from attacks for such time as they so participate."[799] The fact that civilian hackers can be lethally targeted in both IAC and NIACs is not novel, on the contrary, it is a reflection of IHL that considers civilians participating in an armed conflict voluntarily waives protection from attack[800]. However, the challenges that may arise in such cases are in implementing the principle of distinction to the complex and vague nature of cyber warfare, and the promotion of military necessity that considers a military solution justifies the relaxation of normal rules against violence.

- NSAs (include Cyber NSA) blend their identity to create confusion as to whether they are civilians or combatants. The role of NSAs flourishes in failed states or ongoing conflicts, due to their ability to infiltrate communities, create paramilitary networks, ability to finance their operations through illegal businesses and use the fragile security and lack of government accountability in failed states, to evolve. These groups can start as a criminal network using illegal resources to recruit and build their organization, and then evolve to blazing or starting conflicts, and even operations of transnational threat. Hybrid actors develop different mechanisms to maintain their capability, legitimacy, power and seek to build local structures that run parallel to those of the weakened state and to gain a footing within the state.[801] Nonetheless, while addressing hybrid actors under IHL, despite the status or type they formulate (terrorist groups, hackers, criminal gangs, a proxy or private

[797] AP I, Ibid. Article 36.
[798] The ICRC in a recent study about the "potential Human Cost of Cyber operations" has listed a selection of high-profile tools developed or used by States or State-supported actors and that have both technical elements and actual impact. The list provided examples of malicious cyber-attacks as follows: Stuxnet, Flame, BlackEnergy, WannaCry, Triton/Trisis. See more about these malwares and trojans; Olejnik L and Gisel L., The Potential Human Cost of Cyber-Operations, ICRC Expert Meeting 14-16 November 2018, Geneva, pp. 54-55.
[799] Tallinn Manual, at 104.
[800] AP I, article 51(3). See also, Protocol Additional to the GC of August 1949, and Relating to theP of victims of NIAC, Article 51 (3), AP II, Article 13, June 8, 1977.
[801] Cambanis Th., Esfandiary D., Ghaddar S., Hanna M., Lund A. and Mansour R., Hybrid Actors: Armed Groups and State Fragmentation in the Middle East, A Century Foundation Book, New York 2019., p. 14

military companies), such actors are examined whether they meet the level of organization and structure of an organized armed group or they do not. Therefore, it does not matter what kind of operations these groups are involved in, but if they match the legal requirements articulated in GCs, APs, and case law. Yet the challenges that will be highlighted in this chapter chiefly relate to the impact of new technologies in the hands of such groups, the geographical limitation of such weapons, and the problem of attribution veiled in contemporary conflicts.

Legally speaking, IHL established rules as to how operations may be conducted during an armed conflict, such rules are regulated by the GCs of 1949 and international customary norms, similarly, any state development of the IHL in the future will be through customary international law, but that will not be easily achieved due to inconsistencies in the states' practices and challenging nature of contemporary conflicts. As explained briefly in Chapter I of this thesis, conflicts are classified as IAC or NIAC defined under common articles 2 and 3 of the GCs 1949 and its APs. Moreover, international law continues to reflect a war- peace distinction, but the division is based on whether a particular situation of violence amounts as a factual matter to armed conflict.[802] However, when hybrid means are employed in an ongoing armed conflict, whether it is formally declared war or not, or whether it is an IAC or NIAC, the IHL applies.

Therefore, an armed conflict of hybrid nature is regulated by the IHL that represents fundamental principles of humanity and applies to all those involved in armed conflict, but the unarguable theoretical applicability comes with practical challenges because the effectiveness of IHL rules must remain definitive, understood, and accepted in current conflicts and any confusion or ineffectiveness of certain rules would allow actors to consider this area of international law as an anachronistic nuisance than a legal imperative.[803] For example, the intensity of violence that occurred in Ukraine since 2014, has certainly reached the threshold of armed conflict. However, Russia has employed a strategy by combining irregular warfare (little green men) that do not hesitate to use conventional armed warfare and traditional weaponry, indirect tactics of asymmetric warfare to blur lines between combatant and civilian,

[802] ILA, Final Report of the Use of Force Committee, The Meaning of Armed Conflict in International Law, June 2010, Ch. 21, p. 277.
[803] Reeves Sh. And Barnsby R., the New Griffin of War "Hybrid International Armed Conflicts", Harvard International Review 2013, p. 17

cyber-warfare to achieve its strategic objective[804] , and lawfare by either misusing the law as means of warfare or dismissing the law to emphasize certain elements such as the military necessity, that threatens equilibrium set between necessity and humanity at which the law has been established. HW raises questions about the legal framework of non-kinetic military operations, especially that the IHL is geared towards regulating kinetic effects, while the military practice is showing that armed forces are employing a broad spectrum of non-kinetic methods and means.[805] The potential dehumanization of warfare created by the hybrid tools and actors is of high significance to the international legal order, and the international community must address the questions that are brought by such phenomena and reassert the primacy of the law in the challenging and complex environment of HW.

Therefore, in this section, the legal challenges created by HW means and methods to IHL will be examined, particularly the impact of cyber-attacks and NSAs on the classification of armed conflicts. To reach this objective, an overview of armed conflicts and their parties under international law will be evaluated in the context of contemporary hybrid warfare. Additionally, certain challenges will be raised with regards to the classification of co-existing IAC and NIAC. Such examination will require involving case studies, such as the conflict in Ukraine (particularly after the annexation of Crimea and conflict in Eastern Ukraine), and Syria. It will also highlight the problems that arise from cyber NSAs and the geographical limitation of IHL in NIACs.

2.1. Armed Conflicts in Theory and Practice under International Humanitarian Law (Classification and Core Elements)

As explained in the first chapter of this dissertation, IHL applies to armed conflicts and distinguishes between two types, the IAC opposing two or more states and the NIAC that is between governmental forces and non-governmental armed groups, or between such groups only. IHL by classifying the armed conflicts into two types has highlighted the fact that no other type of armed conflict exists, but considered that a situation can evolve from one type of

[804] Bachmann S., Russia's Hybrid War and its Implications for Defense and Security in the United Kingdom, Scientia Militaria, South African Journal of Military Studies, 2016, Vol. 33, No.2, p. 34. (Russia had combined a substantial ground force of 14,400 Russian troops supported by tanks and armored fighting vehicles, backing up the 29,300 illegally armed formations of separatists in eastern Ukraine.)

[805] Sari A., Legal Aspects of Hybrid Warfare, Lawfare Blog October 2015, https://www.lawfareblog.com/legal-aspects-hybrid-warfare

conflict to another, depending on the facts prevailing at a certain moment.[806] The GCs of 1949 uses the term armed conflict to highlight that the determination of whether an armed conflict exists within the meaning of CA 2 and 3 of GCs depends on the prevailing circumstances, not the subjective views of the parties to the conflict.[807] The categorization of whether an armed conflict exists is vital for the determination of whether IHL applies or not, the same is to determine whether a conflict is international or non-international. For example, the rules of engagement, targeting criteria, the status of combatants, and processes are different in both types of conflicts.

However, IHL does not apply to any confrontation between states or any internal disturbance, but rather a certain threshold of violence must be crossed first. However, the non-applicability of IHL does not necessarily mean lesser protection for the persons concerned, as human rights rules and peacetime domestic law would apply with stricter protection in certain areas, such as the use of force and detention.[808] For instance, military occupations are a particular form of international armed conflict, however, if not met with armed resistance then will not be considered an IAC because they do not involve the resort to armed force between states, but GCs are still applicable to them. The term armed conflict has no treaty definition, yet it was shaped by the state practice to determine the legal meaning and parameters of this concept. Nevertheless, it can be defined as a sustained contest between two or more organized adversaries, making purpose use of armed force through the involvement of combat, rather than a one-sided application of lethal force.

Depending on the prevailing circumstances the task to classify the legal character of a particular conflict does not seem complex, though the intensity and parties of a conflict are indicators, no single institution can make an explicit and authoritative determination, and the challenges occur as a result of blurring borderlines between the respective types[809]. The ICTY in the Tadic case established that: "an armed conflict exists whenever there is a resort to armed force between states or protracted armed violence between governmental authorities and organized

[806] ICRC, How is the term "Armed Conflict" defined in International Humanitarian Law? Opinion paper, March 2008, p.1.
[807] Ferraro T. and Cameron L., Article 2: Application of the Convention, ICRC, Commentary on the First Geneva Convention, 2016, p.212. see also, ICTY, The Prosecutor v. Ljube Boskoski and Johan Tarculovski, Trial Chamber, Judgment, 10 July 2008, at 174.
[808] Fundamentals of IHL, ICRC casebook available online: https://casebook.icrc.org/law/fundamentals-ihl#_ftnref_029
[809] Vark R., Legal Complexities in the Service of Hybrid Warfare, Kyiv- Mokyla and Politics Journal 2020, vol. 6, p.37.

armed groups or between such groups within a State".[810] The ICTY in the previous case has managed to include the definition of IAC and NIAC in one definition, however, the GCs and its APs have succeeded to classify them separately under different thresholds and requirements, but emphasized that the IHL does not apply beyond the geographical boundaries of the territory of parties to a conflict, a step that is seen to prevent the evolving existence of what so-called Global war that would permit global targeting of any individual believed to be associated with non-state armed groups. This has a huge impact on the war on terrorism perceived by some states to counter armed groups such as al Qaeda and ISIS.

Generally speaking, the classification of an armed conflict plays a vital role in identifying the applicable rules, rights, and duties that do not exist outside an armed conflict. So, the significances of the classification of armed conflict have an impact on the following:

- Status of combatants, civilians, and other persons who are hors de combat, especially in the status of fighters in the conflict and the rules governing detention of fighters and civilians. For example, fighters in NIACs lack combatant immunity, while in IACs members of armed forces have the combatant privilege.
- The scope of protection under IAC is wider than that of NIAC. For example, the detention regime (GC IV) applies to civilians and combatants detained in IAC. While the rules of detention in NIACs are left to domestic law and IHRL.
- The geographic scope of the IHL application, in which IHL in IACs extends fully to the territory of the parties involved. While in NIAC it is limited to the territory where hostilities taking place, except for spill-over actions. Also, the law on targeting that was considered by the ICRC to be less clear in NIAC than it is in IAC[811]. Although it is believed that this law is equally applicable in NIAC as in IAC, states such as the United States have rejected the applicability of the rule altogether in both IACs and NIACs alike.[812]
- Post-conflict prosecution of violations of international law in particular the ICC jurisdiction by which the list of war crimes subject to the ICC overlap in its Statute, but also vary in some areas based on the type of conflict, whether IAC or NIAC.[813] The Statute of the ICC

[810] ICTY, Prosecutor v. Tadic, Ibid. para. 70.
[811] ICRC, Customary IHL Database, Rule 45 that states the following: "The use of methods or means of warfare that are intended, or may be expected to cause widespread, long-term and severe damage to the natural environment is prohibited. Destruction of the natural environment may be used as a weapon." https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_rul_rule45
[812] Bellinger III, John B., Haynes I and William J., "A US Government Response to the ICRC Study Customary International Humanitarian Law", International Review of the Red Cross, 2007, Vol. 89, no. 866, pp. 445-60.
[813] Akande D., When Does the Use of Force Against a NOSA trigger an IAC and why does this Matter? EJIL Talk, Blog of the European Journal of International Law, October 18, 2016. https://www.ejiltalk.org/when-does-

recognizes 34 war crimes in IAC but only 19 war crimes in NIAC. For example, it recognizes the violation of proportionality rule as a war crime in IAC but not in NIAC.[814]

Nevertheless, the classification of contemporary armed conflicts is not a new challenge to international lawyers and scholars, but an evolving legal subject that has been criticized and debated. For example, the U.S. courts in the Hamdan case evidenced the problem with the classification of armed conflict in the context of "war on terror".[815] The case and its distinctive categorizations before the US courts demonstrated the difficulty in situating international terrorist actions within traditional legal classification under IHL. The challenge in classification will be even more complex in HW that is reflected in contemporary conflicts, such as that in Ukraine and Syria, due to the co-existing elements of both types of conflicts, numerous armed groups involved in parallel to third state interventions, non-kinetic means of warfare that can mask the real identity of adversaries (cyber-attacks), and finally the State's and NSA's ability to employ their lawfare tactics to manipulate the applicable law, by either enforcing it or rejecting its applicability, based on what serves their interest.

2.1.1. Core Elements of International Armed Conflict

The IHL has set rules with different arrays of applicable norms that apply distinctive types of conflicts. While, violence might be seen the same with similar impact (property damage, human casualties, people forced to leave their homes "displaced people" or even their countries "refugees"), the legal character of the particular conflict is necessary to be determined to establish which legal framework is applicable.[816] In an IAC the threshold is low and is crossed whenever there is a resort to hostile armed force between two States. Even border clashes between armed forces or capture of an individual soldier may amount to an IAC unless the States' involved provided evidence of good intentions such as involuntary incursion into the

---

the-use-of-force-against-a-non-state-armed-group-trigger-an-international-armed-conflict-and-why-does-this-matter/

[814] Haque A., Whose Armed Conflict? Which Law of Armed Conflicts? Just Security, 4 October, 2016. https://www.justsecurity.org/33362/armed-conflict-law-armed-conflict/

[815] Duxbury, A., Ibid. p. 3. Duxberry in his article examined the Hamdan case before the US courts and offered three separate opinions on the way in which the conflict in Afghanistan with Al Qaeda should be classified: "1- Justice Robertson described the conflict between US and Al-Qaeda as IAC; 2- the Court of Appeals characterized it as IAC but outside the scope of the GCs; 3- the Supreme Court decided that the protections afforded in NIACs should be applied, therefore treating the conflict as NIAC."

[816] Vark R., Legal Complexities in the Service of Hybrid Warfare, Ibid. p. 37.

foreign territory or wrongly identifying the target.[817] Similarly, an IAC does not exist if the targeted state has given its consent for a third State to take action in its territory (to fight a Non-state armed group). CA 3 of the GCs 1949, which is accepted of customary nature, define the scope of the law applicable to IACs states that the 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[818]. Therefore, as soon as armed forces find themselves in hostile operations with armed groups of another state, or have controlled the territory of a State, an IAC exist and they must comply with the relevant convention, despite whether the conflict extends over time or create a certain number of victims, or even if the state of war has been recognized by the parties.

Additionally, The ICJ in the Wall Opinion case distinguished between two categories of an IAC: "a- Belligerent occupation that arises during an IAC and included in the notion of CA 2 and leaves no doubt about the most evident manifestations of an armed conflict. b- Activities devoted to partial or full occupations that were not met by any armed resistance."[819] This section in CA 2 2(2) of the fourth GC 1949 provides that even if the occupation was not met by any resistance or even shot being fired against the belligerent, an IAC exists with the applicability of IHL to it.[820] So, IAC ruled by Article 2 (2) exists also in the form of occupation that is fulfilled under two conditions: the occupier can exercise effective control over a territory that does not belong to it, and its intervention has not been approved by the legitimate sovereign.[821] The previous article complements Article 42 of the 1907 Hague Regulations that consider the following: "A territory is considered occupied when it is placed under the authority of the hostile army. The Occupation extends only to the territory where such authority has been established and can be exercised".[822] While, Article 6 of the fourth GC states that: "the present Convention shall apply from the outset of any conflict or occupation mentioned in Article 2."[823]

---

[817] ICRC 32nd Conference of the Red Cross and Red Crescent: Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, 2015, p. 8.
[818] CA 3 to the GCs of 1949, Ibid.
[819] ICJ Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 9 July, 2004, paras 92, 95.
[820] GC IV, Ibid. article 6 that states: the present convention shall apply from the outset of any conflict or occupation mentioned in Article 42.
[821] Bothe M., Beginning and End of Occupation, Current Challenges to the Law of Occupation, Proceedings of the Bruges Colloquium, 20-21 October 2005, no.34, pp. 28-32.
[822] Convention IV respecting the Laws and Customs of War on Land and its annex, The Hague, 18 October 1907 article 42.
[823] The ICRC commentary to Article 6 states the following: "the word 'occupation', as used in the Article, has a wider meaning than it has in Article 42 of the Regulations annexed to the Fourth Hague Convention of 1907. So the application of the Fourth Geneva Convention does not depend upon the existence of a state of occupation

So, international law provides that a situation of occupation is a form of IAC and is regulated as such by the four GCs and its APs. The law applicable to IACs covers occupation even if it did not meet armed resistance or armed clashes, or if these armed clashes are with NSAs on the territory of the occupied State. The breaking points identified in both previous articles are that the Convention applies from the beginning of the conflict as well as from the beginning of the occupation, also the hostile army specified in the previous article does not mean only the governmental troops, but also covers the case of NSAs when acting under the control of a State, as in many cases the occupation is exercised by proxy armed groups or puppet government.
In this regard, according to the ICTY in the Tadic case, the relationship of de facto organs or agents to the foreign power includes those circumstances in which the foreign power *occupies* or operates in certain territory solely through the acts of local de facto organs or agents.[824] That brings us back to the Effective and Overall Control tests discussed in chapter two of this thesis that will be difficult to evaluate on a case-by-case basis. However, the ICTY retains the overall control and considers that occupation exists when a State has such control over the local government or armed groups that have "effective control" over the disputed territory.[825] Nevertheless, It is important to differentiate here between the effective control of territory by the de facto organ, and the overall control required by the State in question over the de facto organ. The Overall Control Standard goes beyond the mere financing of armed groups, it also involves a State in its participation in planning and supervision of military operation.[826] That could be seen to some as a challenge since the IAC would not exist in such cases until an effective control over a territory takes place. Yet, to exercise effective control, the Occupying Power (OP) does not need to establish an administration of the territory, but even a presence of some boots on the ground or at least close to the ground in a way that allows the OP to intervene at any moment in any part of the occupied territory to impose authority is necessary for an occupation to exist.[827]

within the meaning of the Article 42 referred to above.. See Pictet, Commentary on Geneva Convention IV, article 6, and Quoted with approval by the ICTY Trial Chamber in Prosecutor v. Rajic, IT-95012, Review of the Indictment. 13 September 1996.

[824] ICTY, Prosecutor v. Dusko Tadic, Trial Chamber 1997, Ibid. para 584.

[825] ICTY, Prosecutor v. Baskic, Case No. IT-95-14-T, Trial Chamber Judgment, 3 March 2000, para 149. See also, ICTY, Prosecutor v. Naletilic, Case No. IT-98-34-T, Trial Chamber Judgment, 31 March 2003 para 197-202.

[826] ICTY, Prosecutor v. Dusko Tadic, Trial Chamber 1997, Ibid. 584.

[827] Pedrazzi M., The Beginning of IAC and NIAC for the purpose of the applicability of IHL, The Distinction between IAC and NIAC: Challenges for IHL, p. 76-77.

Furthermore, the parties to an IAC are commonly two equal sovereigns that are granted equal treatment with regards to their combatants that enjoy the privilege of belligerency. So, the protection of civilians or combatants of an IAC is treated equally by both sides of the conflict as guaranteed through the rules of international. Combatants are members of the armed forces of a State or of groups assimilated to a State as defined by the GC III.[828] While, AP I to the GCs 1949 expanded the scope to non-conventional warfare, such as armed struggles against colonial domination and alien occupation.[829] For example, Article 43(1) of the AP I to the GCs defined armed forces as "all organized armed forces, groups, and units which are under a command responsible to that Party for the conduct of its subordinates.[830] Similarly, civilians directly participating in hostilities lose their protection against direct attack for the period they are engaged in the conflict[831]. Such scenario exists by either member of an armed force which is a belligerent party to a conflict or participates via *levée en masse*[832] if they carry arms openly and respect the laws and customs of armed conflicts, and therefore regarded as combatants that can be lawfully targeted and killed by the adversary.

So according to the ICRC Interpretive Guidance[833], to qualify as direct participation in hostilities, a specific act must meet the following cumulative criteria. Firstly, the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or to inflict death, injury, or destruction on persons or objects protected against direct attack (threshold harm). Secondly, there must be a direct causal link between the act and the harm likely to result either from that act or from a coordinated military operation of which that

[828] GC III, Article 4(A)(1)-(3) and (6).
[829] The Doha Declaration: Promoting A Culture of Lawfulness, E4J University Module Series: Counter-Terrorism "Classification of Persons", July 2018; available at: https://www.unodc.org/e4j/en/terrorism/module-6/key-issues/classification-of-persons.html
[830] AP I to the GCs 1949 and relating to the Protection of Victims of International Armed Conflict (Protocol I), 8 June 1977, Article 43. Additionally, Article 44(3) in the AP I provides certain rules to allow combatants to distinguish themselves and stated that "While, traditionally, belligerents who did not distinguish themselves from the civilian population in a permanent manner lost their right to combatant status, AP I now allowed combatants in certain circumstances to distinguish themselves only by carrying arms openly during a military engagement and while they are visible to the enemy in a military deployment preceding an attack."
[831] AP I to the GCs 1949, Ibid., Article 51(3) "Civilians shall enjoy the protection afforded by this section, unless and for such time as they take a direct part in hostilities."
[832] "Levee en Masse" is a French term that is applied to the inhabitants of a territory which has not been occupied, who on the approach of the enemy spontaneously take up arms to resist the invading troops without having had time to organize themselves into regular armed forces. The term should not be confused with resistance movements. See, ICRC Casebook, How Does Law Protect in War?; available at: https://casebook.icrc.org/glossary/levee-en-masse
[833] ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Geneva, May 2009; available at: https://casebook.icrc.org/case-study/icrc-interpretive-guidance-notion-direct-participation-hostilities

act constitutes an integral part. Thirdly, the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and the detriment of another (belligerent nexus). Besides, combatants or civilians taking part in hostilities may be detained and prosecuted for the commission of war crimes if committed, at the same time civilians participating in hostilities may be criminally prosecuted under domestic law by the detaining State for constituting domestic criminal offenses.

Nonetheless, states have agreed that soldiers killing enemy soldiers on the battlefield may not be punished for their mere participation, but solely for violation of IHL. This has been confirmed by the Preamble to AP I to the GCs 1949, by pointing out that the provisions of the GCs of 12 August 1949 and this Protocol must be fully applied in all circumstances to all persons who are protected by those instruments, without any adverse distinction based on the nature or origin of the armed conflict or the causes espoused by or attributed to the Parties to the conflict.[834] So, AP I has codified pre-existing rules of customary international law and laid the foundation for the formation of new customary rules.

i- The Annexation of Crimea

The annexation of the Autonomous Republic of Crimea and the city of Sevastopol on 18 March 2014, that started with the storming of the parliament building in Simferopol and then after three weeks the referendum in Crimea, is a perfect example for the rise of an IAC and applicability of IHL in an unconventional manner. The annexation reflects an operation conducted by the NSA with an indefinite relation to a foreign power, that led to full control over part of the territory of another State "Ukraine". As Russian forces moved out of their Sevastopol base on 28 February 2014, no single bullet was shot, and no casualties. An actual objective of Russian HW that requires capturing territory without resorting to overt or conventional military forces and reference is Russian Chief of the General Staff Valery Gerasimov who argued that nonmilitary means are used four times more often in modern conflicts than conventional military measures.[835] Russia considered the non-violent annexation as a winning card to prove that the population in Crimea wanted to be part of Russia and that

[834] Protocol I, para. 5 of the Preamble. Under the terms of Art. 31(2) of the Vienna Convention on the Law of Treaties of 23 May 1969, the preamble is an integral part of the treaty.

[835] Gerasimov V., The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations, Voyenno-Promyshlenny Kurier (VPK News), February 26, 2013.

Ukraine accepted the Russian annexation in the sense that such acquiescence can create legally binding outcomes.[836]

Simultaneously, the "Little Green Men" that were considered by Moscow as local self-defense groups with no relation to Russia were not considered so after the annexation and territorial control had been achieved. In April 2014 Russian President Putin himself, while answering the question related to the identity of these armed groups, considered them as Russian servicemen and justified that their operation was to back the Crimean self-defense forces, he stressed that: "one cannot apply harsh epithets to the people who have made a substantial, if not the decisive, contribution to enabling the people of Crimea to express their will. They are our servicemen."[837] Nonetheless, as explained before, sending armed groups qualifies as aggression, which violates international law.

From a legal point of view, the annexation of the Crimean Peninsula by Russia constitutes illegal use of force that qualifies as ongoing aggression as long as the territory continues to be under the annexation. Also, as the prohibition on the use of force includes both direct and indirect use of armed force, the annexation is considered an indirect use of force that is based on different levels of assistance provided to the NSAs proscribed by Res. 2625 (XXV) which is recognized on this specific point as a declaratory of customary international law by the ICJ (DRC v Uganda).[838] But for the interest of this section, the analysis of whether an occupation has occurred leading to an IAC is vital. Following the Russian President's statement admitting Russian troops involvement by having their boots on the ground, and that the so-called "Little Green men" operating in Crimea were not Crimean but Russian servicemen, taking control over a territory and establishing a local authority, multiple legal arguments took place. Based on the facts provided, Russia has violated its obligation that is articulated in AP I, according to which an occupation power shall not affect the legal status of the territory in question.[839] Therefore, such operation is a violation of the rule confirming that occupation cannot imply any right whatsoever to dispose of territory.

Consequently, an IAC concept applies based on the fact that territory is governed in practice (effective territorial control) by the Crimean authorities that took over after the referendum and as a result of foreign military intervention, and the overall control and even effective control

---

[836] C. Macgibbon, The Scope of Acquiescence in International Law, 31 British Yearbook of International Law, 1954, p. 143.

[837] Direct Line with Vladimir Putin, was broadcasted live by Channel one, Rossiya-1 and Rissiya-24 TV on April 17, 2014. http://en.kremlin.ru/events/president/news/20796

[838] Tancredi A., The Russian Annexation of the Crimea: Questions relating to the use of force, QIL, Zoom out I, 2014, p. 9.

[839] AP I of 1977, Ibid. Article 4. Taking into account that Russian Federation is a State party to it.

by Russia over the operational armed groups. Such local government or authority cannot be independent and qualify as a puppet government or a subordinate local administration.[840] The ICJ in its 2010 Advisory opinion on Kosovo's declaration of independence, held that a unilateral declaration of independence is not a per se violation of international law.[841] That falls under the external aspect of the principle of the self-determination of peoples that is mainly associated with situations of non-self-governing territories, and occupations. Opinio Juris with regards to what is known as "remedial secession", or the right to secede from the existing state if the rights of a certain people in that state are blatantly violated, did not find any sufficient position among states on the applicable international law leading to the conclusion to such right.[842] However, according to Judge Abdulqawi Yusuf in his separate opinion on this case, a declaration of independence is not per se regulated by international law, there is no point assessing its legality, as such, under international law. Yet, if such claims meet the conditions prescribed by international law, such as situations of decolonization, or peoples subject to alien subjugations, then the law may encourage it. But, if it violates international law the latter can discourage it or even declare it illegal.[843] The court in the Kosovo case has invoked the UNSCRs that urged not to recognize Northern Cyprus and the Republic of Srpska and to respect the territorial integrity of the Republic of Cyprus and Bosnia and Herzegovina. That was later expressed in the UN General Assembly Resolution (68/262) on the territorial integrity of Ukraine that was adopted on March 27, 2014. The resolution has called all states to refrain from any attempts to modify the borders of Ukraine through the threat or use of force or other unlawful means. It also considered that the referendum of March 2014, has no legal validity and states should not recognize the status of the Autonomous Republic of Crimea and the city of Sevastopol[844]. Therefore, it is understood that such a declaration of independence, whether it took the form of self-determination or the formation of a new de jure organ under a military intervention, will be illegitimate. That has an impact on the direct responsibility of Russia for the acts of its de jure organ that ended up being an instrument of the occupant.[845]

---

[840] Crawford J., The Creation of States in International Law, OUP 2nd Ed., 2006, p. 80.
[841] ICJ Advisory Opinion on Declaration of Independence in Respect of Kosovo, 22 July 2010, para 56. The court has interpreted the question posed by the General Assembly as to take a position on whether international law conferred a positive entitlement of Kosovo unilaterally to declare its independence, or a *fortiori* on whether international law generally confers an entitlement on entities situated within a State unilaterally to break away from it.
[842] Ibid. para 79.
[843] Separate Opinion of Judge Yusuf, Advisory Opinion, Accordance with International Law of the Unilateral Declaration of Independence in respect to Kosovo, Advisory Opinion of 22 July 2020.
[844] United Nations General Assembly, Resolution No. 68/262 on the Territorial Integrity of Ukraine of 27 March 2014.
[845] ICJ Judgment in the Bosnian Genocide case no. 44, Ibid. para 394.

Moreover, the definition of occupation reflected in Article 42 of the fourth Hague convention of 1907 and the effective control criteria have certain grounds in the annexation of Crimea case. Article 42 considers that the territory of a state is under occupation when it is placed under the authority of a hostile army. Similarly, the ICTY's trail Chamber in the *Naletilic* case considered that the regime of occupation would be triggered when a foreign power exercises potential control in the sense that the occupier, having established its control on the territory in question, should at least find itself possibly, or be able, to exercise governmental functions over the local population without necessarily having to do so.[846] Therefore, it can be argued that Russia has exercised indirect effective control through the overall control it exercised over local authorities in the annexed Crimean peninsula (occupation by proxy). The ICJ in the Armed Activities case has acknowledged the possibility of such occupation by proxy.[847] Yet, the threshold of control that qualifies to be effective control is circumstantial. For instance, the US Army Field Manual, the law of Land Warfare, confirms that "the number of troops necessary to maintain effective occupation will depend on various consideration such as the disposition of the inhabitants, the number and density of the population, the nature of the terrain and other factors."[848] So, in the case of Crimea, the presence of thousands of Russian troops in the annexed territory suffice for Russia to directly exercise effective control. Also, the legal regime of occupation prevents the occupier from overstretching the State structure of the occupied territory under both Article 43 Hague Regulations and Article 47 GC IV, by which an occupying authority is merely to be considered as a temporary, de facto administrator. [849]

Therefore, it can be concluded that the role of Russia is not restricted to mere logistic support but implies that it has had in the organization, coordination, and planning of the power established in Crimea. So, the territory is de facto in a situation of occupation and the hybridity of the conflict has played a vital role in progressing strategically and legally in a gradual manner to reach the main objective of full control over a territory of another state. This is reflected in the escalation and de-escalation of the operations, explained in the first chapter, to create the confusion looked for with regards to the legal responsibility of the targeted state and the international community. The law of occupation and human rights laws are vital and remain applicable to the situation in Crimea despite whether Russia consider Crimea as an occupied

[846] ICTY Judgment, Prosecutor v Naletilic and Martinovic, no. IT-98-34-T, 31 March 2003, para 217.
[847] ICJ, Armed Activities on the Territory of Congo, Ibid. para. 168.
[848] Department of the Army, FM 27-10, The Law of Land Warfare 1956, p. 139.
[849] Geib R., Russia's Annexation of Crimea: The Mills of International Law Grind Slowly but they Do Grind, The U.S. Naval War College, 2015, pp. 446-447

territory or not, by which Article 3(b) of the AP I remain in place, to both parties of the conflict that are also parties to the AP until the occupation is terminated. In addition, the law of military occupation is outlined in Articles 42 and 56 in the 1907 Hague Regulations and the Fourth GCs 1949. Moreover, with regards to human rights law, under the jurisprudence of the European Court of Human Rights, an occupying power, including when acting through local administrative authorities, is obliged to secure the European Convention on Human Rights. For instance, the case Ukraine v. Russia (application no. 20958/14) before the ECHR that was lodged on 13 March 2014, dealt primarily with the events leading up to the assumption of control by the Russian Federation over Crimean Peninsula and developments in Eastern Ukraine in 2014. The court has decided to apply rule 39 of the rules of court (interim measures), and called upon both Russia and Ukraine to refrain from taking any military actions which might violate the convention rights of the civilian population, notably articles 2 and 3 of the convention.[850] In the time of occupation, as it is been identified in Crimea, the application of IHRL is likely to overtake IHL when the hostilities have decreased, as it will ensure more protection to civilians.

And by that, based on the previous analysis, and in particular the UN General Assembly resolution 68/262, any valid status alteration could only be legal if based on different ground and in total disconnection from the preceding of unlawful use of force, otherwise it would still be qualified as a serious breach of international law, therefore no legal justification to the annexation of Crimea, that will remain to be a violation of international law until the occupation is lifted. However, despite the uncertain nature of the conflict in Crimea and Eastern Ukraine, the conflict is not in a legal vacuum, on the contrary IHL and IHRL are applicable.

2.1.2. Core Elements of a Non-International Armed Conflict

On the other hand, the NIAC that have become much more common in recent years, have two relevant instruments that apply to it, mainly CA 3 to the GCs 1949 (which is often called "*a treaty in miniature*" due to the number of rules it contains) and Article 1 of the AP II. The extension of international regulation to NIACs changed decisively after WW II, a period in which international law began to recognize the possibility of extending rights and obligations

[850] European Court of Human Rights deals with cases concerning Crimea and Eastern Ukraine, ECHR 345 (2014), 26.11.2014.

to individuals and other NSAs.[851] The NIAC has a higher threshold than IAC, which was not specified precisely in CA 3 of the GCs but was established by the ICTY in its Tadic decision and established it on two main elements: First, protracted armed violence taking place (intensity) and secondly the parties to a conflict must exhibit a certain degree of organization.[852] Both criteria must be met to qualify as an armed conflict, and will be evaluated on a case-by-case basis by weighing up a host of indicative data[853], but it was argued that the meaning of "protracted" and the question of whether this term relates to the duration or intensity of the fighting is not clear.[854] Therefore, certain forms of violence that include one criterion, such as riots, banditry, or terrorist activities, are excluded from the applicability of GCs and considered forms of mere disturbance which is appropriately governed by domestic criminal law and human rights law.[855] Internal disturbances are situations in which there is no NIAC as such, but there exists a confrontation within the country, which is characterized by a certain seriousness or duration and which involves acts of violence.[856] While internal tensions are of less violent circumstances that involve mass arrests, or a large number of political detainees, torture, or other kinds of ill-treatment.[857] So, for the threshold to be breached, the intensity of violence must necessitate the deployment of the State's armed forces for the existence of protracted armed violence against an organized armed group or between such groups, as articulated in the ICTY[858], and the hostilities must surpass situations of internal disturbances

[851] Akande D., Classification of Armed Conflicts: Relevant Legal concepts, in Wlimshurst R. (ed), International Law and the Classification of Conflicts, Ocford University Press 2012, Ch. 3, p. 1.
[852] ICTY, Prosecutor v. Dusko Tadic, Appeal Chamber 1995, Ibid. para 70. See also, The Prosecutor v. Dusko Tadic, Trial Chamber 1997, Ibid. para. 562.
[853] ICTY, Prosecutor v. Haradinaj, case No. IT-04-84-T, Trial Chamber judgment, 3 April 2008, para. 49. See also Prosecutor v. Rutaganda, Case no. ICTR-96-3, Trial chamber I Judgment, 6 December 1999, para 93.
[854] Edlinger K., Ibid., pp. 41- 42.
[855] ICTY, Prosecutor v. Limaj, Case no. IT-03-66-T, Trial Chamber Judgment, 30 November 2005, para. 84.
[856] Vite S., Typology of Armed Conflicts in International Humanitarian Law: Legal concepts and actual situations, International Review of Red Cross, vol. 91, number 873, March 2009, p.77. For further illustration, the ICRC considered that internal disturbances are when there is no NIAC as such, but there exists a confrontation within the country, which is characterized by a certain seriousness or duration, and which involves acts of violence. These latter can assume various forms, all the way from the spontaneous generation of acts of revolt to the struggle between more or less organized groups and the authorities in power. In these situations, which do not necessarily degenerate into open struggle, the authorities in power call upon extensive police forces, or. Even armed forces, to restore internal order. See, ICRC, Protection of Victims of NIACs, Document presented at the Conference of Government Experts of the Reaffirmation and Development of International Humanitarian Law applicable in Armed Conflicts, Vol. V, Geneva, 24 May – 12 June 1971, p. 79.
[857] Sandoz Y., Commentary on the Additional Protocols of 8 June 1977 to the GCs of 1949, ICRC/Martinus Nijhoff, Geneva, 1987, para. 4476.
[858] ICTY, Prosecutor v. Dule, 1995, Ibid. para 70. According to the ICTY, the armed conflict threshold in NIAC is breached in situations that include: "the number, duration and intensity of individual confrontations, the type of weapons and other military equipment, the number of munitions fired, the number of persons and types of forces partaking in the fighting, the number of causalities, the extent of material destruction and the number of civilians fleeing combat zones. Also, the involvement of the UNSC may be a reflection of the intensity of a conflict. See, ICTY, Prosecutor v. Haradinaj, Ibid. para 49.

on order for an armed conflict to exist.[859] The reason behind this threshold is reasoned for governments have always leaned towards lesser intrusion into their sovereign affairs, by which any supremacy of international law over their national ones and granting any appearance of legitimacy to armed groups rebelling against their authority, will impact their ability to maintain law, order and national security.[860] This has offered states more flexibility to deny the existence of an armed conflict, and deal with the situation as a matter of ordinary internal disturbance regulated by national laws. For example, the U.S. government has denied the applicability of CA 3 to the Al Qaeda in the aftermath of the 9/11 attacks[861], and the Bush Administration had designated this conflict a "Global War on Terror" and determined that it was neither an IAC because Al Qaeda is not a state party, and nor a NIAC since it exceeded the territory of one state.[862] The previous example is a NIAC of transnational nature and denying the role of CA 3 was suppressed by the US Supreme Court in the 2006 Hamdan case that ruled: "The armed conflict between Al Qaeda and its affiliates on one side, and United States on the other, was at least governed by CA 3 as a matter of US treaty obligation"[863], thereby implying that it was a NIAC.[864] However, such cross border conflicts are recognized as threat to the international peace and security, and international law provides coherence to the treatment of cross-border consequences of conflicts.

Moreover, a NIAC that starts within the territory of a single state might spill over into the territory of neighboring states, which raises additional legal concerns with regards to the violation of sovereignty and response from the armed forces of the state in concern.[865] Yet, it

---

[859] Prosecutor v Rutaganda, Case no. ICTE-96-3-T, Judgment and Sentence of December 6, 1999, para. 93.

[860] This was reflected in CA 3 (4) of the GC 1949 in its last paragraph, that stated: "the application of the preceding provisions shall not affect the legal status of the Parties to the conflict." To illustrate, the application of IHL to a NIAC never internationalizes the conflict or confers any status to a party to that conflict, other than the international legal personality necessary to have rights and obligations under IHL. See, ICRC's Handbook for Parliamentarians, Ibid. p. 20.

[861] More examples about instances where states denied the applicability of CA 3 to certain military operations. See, Provost R., International Human Rights and Humanitarian Law, Cambridge University Press, 2002, p. 268.

[862] White House Memorandum of February 7, 2002 on the "Humane treatment of Talban and AL Qaeda detainees", available online: http://www.pegc.us/archive/White_House/bush_memo_20020207_ed.pdf

[863] Hamdan v. Rumsfeld, United States Reports, Cases Adjudged in the Supreme Court at October term 2005, Vol. 548, Washington 2006, p. 628-631.

[864] The Supreme Court of the United States stated that it did not need to decide the merits of this argument because there is at least one provision of the GCs that applies here even if the relevant conflict is not between signatories. (Hamdan v. Rumsfeld, Ibid., p. 629.) Important to note that the Court's interpretation of the applicability of the CA 3 to the US's conflict with Al Qaeda was based on the quality of the parties involved and not on its geographical reach. Pejic J., Ibid. p. 14.

[865] Few examples of the extra-state hostilities can be taken into consideration: 1- the Israeli incursion into Lebanon in 1982 that was aimed to destroy the Palestinian insurgencies' bases on the Lebanese territory and led to multiple armed attacks across the international frontier. 2- the Turkish operations in Northern Iraq against the Kurdish armed groups. 3- the conflict between Morocco and the Saharawi in the Western Sahara, by which the territorial

was submitted that the spilled-over conflict will still be governed by CA 3 and customary IHL because such a situation must not have the effect of absolving the parties of their IHL obligations simply because an international border has been crossed.[866] The previous statement about the applicability and the geographic scope of IHL beyond the territory of the parties to the conflict is of high importance regarding the extra-territorial targeting and capture of individual members of an NSA group. Even though some States' practices have made arguments about the extra-territorial applicability of IHL, such as the United States, however, no such clear opinio Juris has been recognized by other states. It would be against the interest of these states to accept that the IHL does not apply to extra-territorial activities that will jeopardize the safety of their citizens in fights that took place on their territory without reaching the level of intensity required for NIAC.[867]

In jurisprudence, the Statute of the Rwanda Tribunal (ICTR) has confirmed the applicability of IHL to hostilities that exceeded the territory of a single state, and provided that Rwanda and Rwandan citizens responsible for serious violations of IHL committed in the territory of neighboring states, must be prosecuted and acknowledged the jurisdiction of the tribunal over violations of CA 3 and AP II to the GCs.[868]

According to the opposing views of the above section, several opinions endorsed the importance of developing a new legal framework for the extraterritorial effect of NIACs and argued that hostilities that spill over to the territory of another state, should not be placed in the traditional categories of armed conflicts.[869] This position is based on certain arguments that NSAs have developed their technological and military capabilities allowing them to have more influence at the international level. Also, the accelerated process of state creation has weakened the State's ability to prevent armed groups from using its territory as a base for launching

---

claims parties to the conflict were analyzed in the ICJ Western Sahara case in 1975. Schondorf R., "Extra-state armed conflicts: is there a need for a new legal regime?", New York University Journal of International Law and Politics, Vol. 37, No. 1, 2004, p. 9. now available at SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=644821. For additional examples see, Gasser H.P., Internationalized non-international armed conflicts: Case studies of Afghanistan, Kampuchea and Lebanon, AMUL Review 1983, vol 145, p. 155- 156.

[866] Pejic J., The Protective scope of CA 3: More than meets the eye, ICRC Vol. 93, no. 881, March 2011, p. 6.

[867] Droege C., The Geographical reach of IHL: The Law and Current Challenges, The 2015 Round Table on Current issues of International Humanitarian Law, 2015, Ibid. p. 98.

[868] Statute of the International Tribunal for Rwanda (ICTR), 2007, Article 1 on the Competence of the International Tribunal for Rwanda: " The International Tribunal for Rwanda shall have the power to prosecute persons responsible for serious violations of international humanitarian law committed in the territory of Rwanda and Rwandan citizens responsible for such violations committed in the territory of neighboring States between 1 January 1994 and 31 December 1994, in accordance with the provisions of the present Statute."

[869] Schondorf R., Ibid. p. 4.

hostilities against other states.[870] And finally, extra-territorial hostilities did not constitute a significant part of international practice at the time that the Hague regulations of 1907 or the GCs of 1949, were drafted.[871] However, this view argues that this new category of armed conflict is governed by specific rules that are derived from an interpretation of the general principles of IHL in the specific context of extra-state armed conflicts."[872] So, practically this theory proposes that a new category of armed conflict should be recognized, but still be regulated by similar, if not the same, provisions already exist under the IHL treaty and customary law for NIAC.[873]

To sum up, this argument is not sufficient to consider the existence of a critical gap, but a remedy for such confusion that might lead to the creation of new forms or misuse of law is to consider that CA 3, as a matter of treaty law, apply to conflicts that are originally generated as NIAC but occur between the parties of the conflict yet on the territory of another state. So, it will be an expanded version of CA 3 based on the parties of a conflict and partially based on the territory of actual hostilities. The developments of customary law reflected above shows that such expansion is possible.[874] The United Kingdom manual of the law of armed conflict illustrates this point, and states that: "Whilst states may not be willing to admit to the application of CA 3 as a matter of law, its provisions are frequently applied in fact."[875] Furthermore, the *"*Principle of Legislative Jurisdiction" that has been discussed by the Greek delegate during the Geneva 1949 conference, considers that the agreement or treaty that the state ratifies is automatically binding everyone within its jurisdiction including NSAs.[876] Similarly, the De facto control theory highlights that armed groups of a chain command over insurgents and exercising effective territorial sovereignty are bound by IHL conventions because treaties can create obligations for third parties[877], and to all treaties, the state is bound

[870] Watkin K., Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict, American Journal for International Law, 2004, p .14.
[871] Schondorf R., Ibid. p. 10.
[872] Ibid. p. 8.
[873] Pejic J., Ibid. p. 18.
[874] Above footnotes 135, 136.
[875] United Kingdom Ministry of Defense, The manual of the law of armed conflict, Oxford University Press 2005.
[876] Cf. S. Sivakumaran, 'Binding Armed Opposition Groups', 55 International and Comparative Law Quarterly 369, 381 (2006); the principle has been assailed by A. Cassese, 'The Status of Rebels under the 1977 Geneva Protocol on Non-International Armed Conflicts', 30 International and Comparative Law Quarterly 416, 429 (1981).
[877] Article 35 of the 1969 Vienna Convention on Law of treaties (VCLT).

to it.[878] Some challenges may arise concerning the compliance of NSAs with the IHL rules. For example, armed groups that have a cell structure, are highly organized but operate secretly. So, respecting the IHL norms on detention, for instance, is hard because such cells would not disclose their location or they will find themselves unable to detain.[879] Also, in contemporary conflicts, in particular urban conflicts, numerous armed groups are formed by civilians to protect themselves or the geographical area they are located in, against another armed group or governmental forces. Such groups that blend the civilian status and fighter with no organized structure or leadership, are challenging and create confusion in wondering to what extent IHL and Human rights law can even regulate these types of situations.[880] The latter will be further explained while addressing the principles of IHL, in particular the principle of distinction.

As underlined before, the groups must be armed, not merely dispersed individuals must possess a certain degree of organization that allows them to perform military activities of a certain intensity, and a code of conduct which the NSA applies.[881] Also, it is required that the armed group must entail a certain chain of command able to impose discipline on the group, yet this does not mean that effective respect shall be required, as long as the group is capable of respecting the provisions.[882] This requires that the leadership of the group must, as a minimum, have the ability to exercise some control over its members. [883] In this manner, the ICTY noted the factors that help to reveal the minimal level of organization of the armed group for CA 3 and falls into five broad terms:

- "An organized group has a hierarchical structure, a chain of command, and a set of rules as well as the outward symbols of authority. (e.g., the existence of headquarters, internal regulations, spokespersons)·

[878] Pictet J., ICRC Commentary to Convention I, Geneva, 1952, p. 51. See also, Cassese A., La Guerre Civile et Droit International, RGDIP, p.55. Cassese commented that common Article 3 of the GC 1949 confers rights and obligations on both sides of the conflict.
[879] Bella A., Challenges for Compliance by Non-State armed Groups, The Distinction between IAC and NIAC: Challenges for IHL, Ibid. p. 231-232.
[880] Ibid. p. 232.
[881] Prosecutor v L. Boskoski, j. Tarculovski Judgment, ICTY Trial Chamber, Case No IT-04-82-T, 10 July 2008, para. 194-105, and 199-203
[882] Pedrazzi M., Ibid. p. 80
[883] One of the examples provided by the ICTY is that Belgian military court refused to characterize the situation prevailing in Somalia in 1993 as an armed conflict to which CA 3 would apply on the basis that the groups involved were irregular anarchic armed groups with no responsible command. ICTY Prosecutor v. Ljube Boskoski and Johan Tarculovski, Trial Chamber II Judgment 10 July 2008, para 196. See also the original document sourced by the court (in French), Ministre Public and Centre pour L'egalite des chances et la lute contre le Racisme, Belgium, Military Court, Judgment of 17 December 1997, Journal de Tribunaux, 4 April 1998, pp. 286-289.

- The group could carry out operations in an organized manner. (Ability to determine a unified military strategy and conduct large-scale military operations, capacity to control territory, the capacity of operational units to coordinate their actions, effective dissemination of written and oral orders and decisions.)
- Level of logistics that allows the group to recruit new members, provide military training, supply and use of uniform, and the existence of communications equipment for linking headquarters with units or between.
- Ability to possess a level of discipline and implement the basic obligations of CA 3, such as the establishment of disciplinary rules and mechanisms, proper training, the existence of internal regulations.
- The armed group can speak with one voice, such as its capacity to act on behalf of its members in political negotiations with representatives of international organizations and foreign countries, ability to negotiate and conclude agreements such as cease-fire or peace accords."[884]

Moreover, CA 3 to the GCs and AP II offer guidance regarding the conduct of hostilities in NIAC situations, not as detailed as in IAC notably regarding concepts such as "civilians", "armed forces", and attacks. Though the principle of distinction applies equally during NIAC, as in IAC, members of armed groups are referred to as fighters rather than combatants, and the purpose of categorizing such person relates to their conduct of hostilities and should not affect their treatment.[885] For example, Article 1(1) of the AP II to the GCs 1949 states that "this Protocol, which develops and supplements CA 3 to the GCs of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the GCs of 12 August 1949, and relating to the Protection of Victims of IAC (Protocol I) that 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 and to implement this Protocol."[886] Therefore, civilians lose their immune status once being part of

[884] ICTY, Prosecutor v Ljube Boskoski and Johan Tarculovski, Ibid., para. 199-203.
[885] AP II to the GCs 1949 and relating to the Protection of Victims of Non-International Armed Conflict, 8 June 1977, Article 13(1) "the civilian population and individual civilians shall enjoy general protection against the dangers arising from military operations. To give effect to this protection, the following rules shall be observed in all circumstances."
[886] AP II, Ibid. Article 1(1).

an armed group involved in a NIAC, and rather described as "fighters", "unlawful combatants" or "unprivileged belligerents".[887] In other words, an individual whose continuous function involves the preparation, execution, or command of operations amounting to direct participation in hostilities (continuous combat function) on behalf of an organized group is considered a member of that group and loses his protection against the dangers arising from military operations for the duration of that membership. The "continuous combat function" criterion distinguished members of the organized fighting forces of a NSA from civilians who directly participate in hostilities on a merely spontaneous, sporadic, or unorganized basis.[888] The term "unlawful combatant" is rather descriptive for individuals who unlawfully engage in combat without being entitled to do so.[889] Consequently, unlawful combatant means that a person does not have the legal right to participate directly in hostilities, so may be prosecuted for any act or omission provided for under relevant domestic law, even if such conduct is permissible under IHL. Though international law requires humane treatment and fair trials for individuals detained or are under the status of hors de combat, there remains a built-in distinction between the government forces and those who fight against it[890]. Yoram Dinstein demonstrates that "unlawful combatants in NIACs are viewed as traitors and, if captured, are liable to be prosecuted and punished for violations of domestic law. They cannot be expected to be accorded the privileges of "POW" status."[891]

After all, the distinctive thresholds between CA 3 to the GCs 1949 and that of AP II are of great importance. While both agree that non-governmental forces have to demonstrate a degree of organization, yet CA 3 does not stipulate that the armed group must control part of a territory for a NIAC to exist. This difference between the two understandings is challenging in practice, by which unlike CA 3 of the GCs, the AP II will not apply to conflicts between dissident groups and to conflicts that match the traditional conceptions of inter-state warfare (when an organized

[887] The Doha Declaration: Promoting a Culture of Lawfulness, E4J University Module Series, Ibid.
[888] ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Ibid. Important to note that "such individual must be distinguished from persons comparable to reservists who, after a period of basic training or active membership, leave the armed group and reintegrate into civilian life. By which such reservists are civilians until they are called back to active duty or direct participation in hostilities." Ibid.
[889] Dormann K., The Legal Situation of "Unlawful/Unprivileged Combatants", International Review of the Red Cross, 2003, p. 45.
[890] Wallace D. and Reeves Sh., The Combatant Status of the "Little Green Men" and Other Participants in the Ukraine Conflict, International Law Studies, U.S. Naval War College, 2015, Vol. 91, p. 391.
[891] Dinstein Y., The System of Status Groups in International Humanitarian Law, in International Humanitarian Law Facing New Challenges, Wolff Heintschel von Heinegg and Volker Epping eds, 2010, p. 148.

group exercise military control over a part of the territory of a State party)[892]. By which if Article 1(1) of AP II is interpreted strictly, cases that require territorial control will be similar to that of an IAC and the degree of control will be perceived differently from one case to another.[893] The restrictive definition applies only to AP II and does not apply to CA 3 of the GCs. Therefore, some situations trigger only the application of CA 3 if it did not meet the requirement of the organization level of the dissident groups.[894] However, the ICRC approach that adopted an intermediate position while commenting on the APs by stating that: "territorial control can sometimes be relative, for example, when urban centers remain in governments hands while rural areas escape their authority."[895] So according to the ICRC's commentary, even modest control or some degree of stability in it, is sufficient for the obligations presented in AP II. This also has been seen as an intermediary threshold of the application by the ICC statute and the jurisprudence of the ICTY in the Tadic case.[896]

Besides, CA 3 to the GCs has failed to elaborate profound distinction between military and civilian targets, and covered non-participants of an armed conflict and persons who have laid down their arms[897], but did not cover the combat or protect civilians against the effects of hostilities. So, unlike IAC, in NIAC no combatant status or privilege exists and AP II does not contain specific rules and definitions concerning the principles of distinction and proportionality.[898] Moreover, the humane treatment in CA 3 has been interpreted to "safeguard the entitlements which flow from being a human being"[899], but without listing these safeguards. Therefore, it was argued that the right of injured people in NIACs is only recognized once the deprivation has occurred. While human treatment is explicitly addressed in CA 2 and its AP I it is seen that CA 3 provided comparatively less protection than CA 2. For that reason, there should be no acceptable compromise concerning human treatment based on the status of a conflict.[900] However, states are reluctant to extend IHL entirely to NIACs since equating the

---

[892] Stewart J., Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict, International Review Red Cross 2003, p. 319.
[893] Moir L., The Law of Internal Armed Conflict, Cambridge University Press, 2002, p. 106.
[894] AP II, Article 1 states that: "This Protocol, which develops and supplements Article 3 Common to the GCs, without modifying its existing conditions of application."
[895] Sandoz Y., Ibid. para 4476.
[896] Statute of the International Criminal Court, adopted by the Diplomatic Conference of the plenipotentiaries to the United Nations on the creation of an International Criminal Court, 17 July 1998, Part A, Article 8 (2)(f). See also, ICTY, Prosecutor v. Tadic, Ibid., paras 49 and 60.
[897] Stewart J., Ibid. p. 320.
[898] For example, Article 13 of the AP II provides that "the civilian population as such, as well as individual citizens, shall not be the object of attack unless and for such time as they take a direct part in hostilities."
[899] Prosecutor v. Aleksovski, ICTY Trial Chamber 1999, Case No. IT-95-14/1T, para 49.
[900] Brier-Mills M., Questioning the Utility of the Distinction between Common Articles 2 and 3 of the Geneva Conventions of 1949 since Tadic: A State Sovereignty Approach, Macquarie Law Journal, Vol 17, 2017, p. 20-21.

two types of conflicts would undermine States' sovereignty and national security. For example, in IAC the principle of combatants' immunity prevents the prosecutions of combatants merely for taking part in an armed conflict, and if such principle applies to NIACs, states would be unable to criminalize acts that are traditionally regarded as treasonous.

Therefore, it can be established that a normative gulf exists between the law governing IAC and NIAC, by which the law of the latter is considerably more under-developed than the law of the former. The division of IHL between rules applicable to IAC and NIAC that was established by the CCs 1949 and that established a single provision (CA 3) to the four GCs which that apply to an armed conflict, not of an international character and occurring in the territory of one of the high contracting parties, was further confirmed when the ICRC convened a Diplomatic Conference between 1973 and 1977 adopting the APs I/II. The classification can also be seen in the relevant provisions of the 1954 Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict.[901] The rules that apply to specific conflicts depend on whether it is IAC or NIAC, and the classification is not left to the parties of the conflict but on what happens on the ground. However, despite the difficulty in classifying the armed conflicts and disparity in certain articles that provided different thresholds applied to IAC and NIAC and different treatment of parties to the conflict based on classification of it, yet with the role of IHRL and IHL, and the jurisprudence of international criminal courts, it has been noticed that the difference was rationalized by claiming that under customary international law the difference between the two categories of conflict has gradually disappeared.[902]

Nevertheless, as the main aim of the IHL, treaty and customary law, is to provide maximum protection to victims of an armed conflict, it is accepted that the current classification can meet this objective. Although certain variations were identified between GCs and their APs, especially in NIACs, however CA 3 is of customary nature with less strict requirements than AP II, so with expanding the former's rules through customary law to meet the intermediate threshold recognized by the ICC statute and the jurisprudence of the ICTY in the Tadic case, the gap would partially diminish. For example, the gaps that are noticed in the regulations of

[901] Article 18 of the mentioned Hague Convention states that the treaty entirely applies to IAC, while under Article 19 only limited aspects apply to NIACs. See, O'Keefe R., The Protection of Cultural Property in Armed Conflict, Cambridge University Press 2006, pp. 96-98.

[902] Fundamentals of IHL, ICRC casebook, Ibid.

the conduct of hostilities in AP II are largely filled through State practice but applicable as customary law to NIAC, and it covers basic principles on the conduct of hostilities, rules on protected persons, and objects and specific methods of warfare (includes but not limited to the following: Rules 7- 10 on the distinction between civilian and military objects; Rules 11-13 on indiscriminate attacks; Rule 14 on Proportionality in the attack).[903] Whilst in contemporary conflicts any failure to classify a state of affairs as an armed conflict has grave legal and humanitarian consequences, the role of customary law is significant, as most treaty regimes are not universal. For example, the United States is not a party to the APs of 1977, yet it complies with the norms expressed in the treaty on the basis that they reflect customary international law.

2.2. Hybrid Warfare and Modern Armed Conflicts

Hybrid adversaries, whether states or NSAs with state sponsorships or state-like capabilities have increased and developed their strategic, military, and technological capabilities in the last years, which seized the attention of legal and security experts. HW concept is neither new nor created a new type of conflict, however, it has progressed and become more influential in the international arena because of the emergence of NIACs after WW II and the development of International law on the use of force and IHL. So, for hybrid adversaries, a fusion of methods and means, employment of multiple actors in multi-model domains, and calibrating the level of intensity and organization of parties to a conflict, is seen to be the new norm.[904] In other words, armed conflict of hybrid nature is a situation in which parties refrain from the overt use of armed forces against each other unless necessary, rather, relying on a combination of military intimidation falling short of an attack, exploitation of economic and political vulnerabilities, and diplomatic or technological means to pursue their objectives.[905]

---

[903] Henckaerts J.M, Study on Customary International Humanitarian Law: A contribution to the understanding and respect for the rule of law in armed conflict, ICRC review, p. 188-189. See also, ICRC on Customary International Humanitarian Law, Ibid. Rules mentioned above.

[904] According to Laurence Freedman, "Russia has succeeded in Crimea and eastern Ukraine by adopting skillful techniques of hybrid war. This was reflected in the use of a range of force types. Initially, the main requirement was sufficient force to take over administrative buildings and intimidate local police forces. Over time the demands increased, to the point where local agitators had to be supplemented with Russian fighters with combat experience, apparently often Chechen. Eventually, regular forces had to become directly involved." See, Laurence F., Ukraine and the Art of Limited War, Survival 2014, vol. 56, no. 7, p. 21-22.

[905] At a Glance: understanding Hybrid Threats, EU Parliament Fact Sheet, June 2015. Available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/564355/EPRS_ATA(2015)564355_EN.pdf

In modern conflict, particularly of hybrid nature, a clear cut between NIAC and IAC is more challenging, and many incidents have risen where both types of conflicts broke out at the same time and geographical location. The traditional guidelines of IHL have developed in a conventional kinetic military context, opposite to the hybrid warfare that relies heavily on unconventional, non-kinetic, and non-military means and methods. The hybrid states are well aware of these guidelines and try to either avoid crossing the threshold of armed conflict or combine its thresholds in one or more types of conflicts.[906] States have increased their involvement and interventions in ongoing conflicts under various justifications. For instance, Russia's involvement in Ukraine can be described as a conventional state actor waging a hybrid war through local hybrid proxies. At the same time, hybrid NSAs progressed and urbanized to create fragmented armed groups that are heavily involved in the hostilities.[907] Different scenarios are recognized in contemporary conflicts, with a variety of means and methods employed to create a legal grey zone to the applicable law. For instance, states intervene directly by attacking armed groups on the territory of other states with or without the consent of the territorial state. Also, states intervene to support an armed group in an ongoing NIAC, where another third state is involved on the side of the territorial state in its fight against the NSA. This scenario results, on one hand, in a NIAC between the territorial state and NSA operating within its territory. On the other hand, an IAC starts between the intervening state and the territorial state. A further possible scenario is when the third state deploys proxy NSA to intervene on its behalf in an ongoing conflict to deny any direct confrontation with the territorial state, and by that avoid triggering the application of IHL.[908]

Nevertheless, this section will analyze the fusion of hybrid means and methods shaped at the operational level in respect to the traditional legal classification of armed conflicts. Also, will determine if the significantly different protections provided to the combatants in IAC and NIAC, such as the immunity of combatants and detainees, in a hybrid classified armed conflict is properly regulated by IHL, treaty, and customary laws. Moreover, two scenarios of actual armed conflicts will be taken into consideration while analyzing the above-mentioned issues, the conflict in Ukraine is highly considered as a complex conflict with hybrid characteristics (in particular the conflict in Eastern Ukraine excluding the latest unprovoked aggression against Ukraine in 24th of February 2022), and the conflict in Syria that involved multiple actors

[906] Vark R., Ibid, p. 37-38.
[907] ICRS's Handbook for Parliamentarians, Ibid. p. 20.
[908] Monaghan A., the "War" in Russia's "Hybrid Warfare", Parameters, Vol. 45, No. 4, Winter 2015.

(states and NSAs). In doing so, the focus will be purely on the classification of the armed conflict in situations seen to be reflecting HW examples, to apply the law to the facts. Moreover, it will not concentrate on cyber-attacks as a hybrid tool that has potential physical harm effect triggering the armed conflict threshold. The answer the author is aiming to achieve is how IHL applies to HW in IAC, NIAC, and mixed conflicts. Also, if it would be possible to divide a conflict taking place on a territory of one State into two different types of conflicts and apply the rules of IHL to each one of them with no impact on the core values and aims behind the applicable law due to the geographic limitation of armed conflicts and technological means that manipulate such limitation.

The fusion of conventional and unconventional methods, technological and non-kinetic means employed by hybrid adversaries, make it difficult to decide whether HW qualifies as an armed conflict. However, hybrid operations that fall below the threshold of an armed conflict are not in a legal vacuum, and that was explained in the second chapter of the thesis while addressing the law on the use of force and armed attack threshold, likewise when addressing the relationship between IHL and IHRL. While violent or potentially violent actors (terrorist organizations, criminal gangs, proxy fighters), and partially violent means (tools that are not necessarily developed for violent or military reasons, but are being employed violently with the ability to cause physical and property damage, such as cyber-attacks), are both in the essence of the range of tools and means used in HW, their role in armed conflict is highly relevant to the application of IHL that will come into force immediately. As explained before, the GCs of 1949 and its APs did not provide a well-defined delineation of armed conflicts, but the ICTY in the Tadic case has established that an 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.[909]

Theoretically, violence is a central element in the definition of armed conflicts, so whenever a hybrid operation reaches the level of intensity of armed conflict that includes violence, IHL applies. Afterward, it will be important to identify the parties of the conflict to determine the type of conflict. According to Schmitt in discussing the importance of conflict classification under IHL, he stated that classifying the conflict is a subject of seminal importance and is

[909] ICTY, Tadic case, Ibid. para. 70.

always the first step in any IHL analysis, for the nature of conflict determines the applicable legal regime.[910] Moreover, HW scenarios involve State and non-state adversaries, Russia is not the only state that has developed HW capabilities, but it can be observed through Iran, North Korea, and China too. Similarly, ISIS was not the first to develop non-state HW, but the nature of conflict it was involved in, the extraterritorial hostilities, and its ability to build a cocktail of hybrid capabilities, was significant.[911] So, in this chapter, the term cyber-operations and the NSAs will be referred to means, methods, and parties of warfare that amount to or are conducted in the context of an armed conflict within the meaning of IHL only.

A hybrid armed conflict is expressed by multiple means and methods that include cyber-attacks. Hence, applying IHL to cyber context is vital, as cyber-attacks in armed conflict are a novelty that brings advantages of strategic nature over an unprepared opponent. For example, Article 36 of the AP I to the GCs provides that in developing or adopting a new weapon, means, or method of warfare, states are under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.[912] Similarly, the ICJ in its advisory opinion about the legality of the threat or use of nuclear weapons invoked the Martens Clause in the preamble to the Hague Convention IV of 1907, which stated that even in cases not explicitly covered by specific agreements, civilians and combatants remain under the protection and authority of principles of international law derived from the established custom principles of humanity and the dictates of public conscience.[913] The latter was reflected in Article 1 to the AP I of 1977 and aims to limit the belligerents' ambition to use methods or means that are not covered by treaty regulation or customary law.

Consequently, IHL extends to the sphere of cyber operations in armed conflicts, mainly because cyber operations can have the same violent consequences as kinetic operations, for instance, if they were used to open the floodgates of dams or to cause aircraft or trains to collide.[914] Therefore, the applicability of IHL to cyber operations will be based on the nature,

---

[910] Schmitt M., Classification of Cyber Conflict Journal of Conflict and Security Law 2012, Vol 17, p. 245.
[911] For more examples, see, Hashim A., State and Non-State Hybrid Warfare, Oxford Research Group "Breaking the Cycle of Violence", 30 March 2017. https://www.oxfordresearchgroup.org.uk/blog/state-and-non-state-hybrid-warfare
[912] AP I of 1977 to. the Geneva Conventions 1949, Ibid. Article 36(1).
[913] ICJ, Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, paras. 74-87. See also, Preamble of the 1899 Hague Convention (II) with Respect to the Laws and Customs of War on Land 1900 and 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land 1910.
[914] IHL provides limits on the use of certain weapons and methods that are indiscriminate by nature, therefore, IHL imposes some limits on the militarization of cyberspace by prohibiting the development of cyber capabilities

effects, and circumstances of such operations. States have recognized that international law applies in cyberspace, and that IHL applies to cyber operations during armed conflict. Similarly, the Groups of Government Experts (GGE) cited that established international legal principles, including, where applicable the principles of humanity, necessity, proportionality, and distinction, apply to cyberspace.[915] According to the ICRC, cyber operations during armed conflict are operations against a computer system or network, or another connected device, through a data stream, when used as means or methods of warfare in the context of an armed conflict.[916] The latter is reflected in the IHL's aim to regulate future conflicts that occur after the adoption of the IHL treaty, in an attempt to cover emerging methods and tools that might be used in future conflicts.[917]

Correspondingly, not every cyber-attack constitutes violence in the strict sense of Article 49(1) of the AP I that defines armed attacks as an act of violence against the adversary in offense or defense. In an attempt to differentiate between cyber-attacks and cyber nuisances, Schmitt considered that the term "violence" is a prescriptive shorthand intended to address specific consequences and it must be considered in the sense of violent consequences rather than violent acts.[918] Applying Schmitt's observation to the cyber-attack that targeted Estonia in April 2007, it is argued that despite the scale of DDOS attacks that caused harm on the multiple sectors in the country due to their reliance on the internet, however, it did not reach the level of violence required in Article 49 of the AP I, as the consequences of such attacks were not sporadic and did not cause injuries, death, damage, and destruction.

---

that would qualify as weapons and would be indiscriminate by nature or would be of a nature to cause superfluous injury or unnecessary suffering. See, Henchaerts J.M. and Doswald-Beck L., Customary International Humanitarian Law, Ibid. rules 70 and 71.

[915] ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, Position Paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2019, p. 3. available at: https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts

See also, Un GGE reports between 2013 and 2015, that concluded the following: "International law, and in particular the UN Charter, is applicable in the information and communication environment." See, UN General Assembly, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General", UN Doc. A/68/98, 24 June 2013, para. 19, and UN Doc. A/70/174, 22 July 2015, para. 24.

Moreover, this conclusion was confirmed by the UN General Assembly Resolution 73/27 on the "Developments in the Field of Information and Telecommunications in the Context of International Security", UN Doc. A/RES/73/27, 11 December 2018, para. 5.

[916] ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, Ibid. p.3.

[917] AP I to the GCs of 12 August 1949, Ibid. Article 36 (1).

[918] Schmitt M., Wired Warfare: Computer Network Attacks and Jus in Bello, International Review of the Red Cross, Vol. 84m No. 846, p. 377.

On the other hand, the Operation Olympic Games, that targeted the Iranian nuclear enrichment facility at Natanz, Iran (also known as the Stuxnet attack) that consisted of a covertly cyber beacon into the Iranian computer network, and was designed to leave no trace of attackers, though it was not classified as an armed conflict in the discourse of states[919]. However, some have argued that if the attack was attributed to a state at that time, it would amount to an IAC.[920] Attribution in cyberspace in the context of IHL looms for whether state support creates an armed conflict, serves a transformative or initiating function concerning the conflict itself.[921] According to the Tallinn manual, the circumstances under which the internet in its entirety could be attacked, are so highly unlikely as to render the possibility purely theoretical at present. Instead, it was agreed that, as a legal and practical matter, virtually any attack against the Internet would have to be limited to certain discrete segments thereof.[922] The experts in Tallinn Manual has interestingly agreed that damage in the digital world also means loss of functionality of an object, and the ICRC has agreed with this view by considering that: "if an object is disabled, it is immaterial how this occurred, whether through kinetic means or a cyber operation. Otherwise, a cyber operation aimed at making a civilian network dysfunctional would not be covered by the IHL prohibition on targeting directly civilian persons and objects."[923] Accordingly, an attack that disrupts the functioning of objects without physical damage or destruction, even if the disruption is temporary, constitutes an attack as long as the aim of the attack is directed at the physical infrastructure relying on the computer system and not merely aiming to disrupt or block communication. It is therefore seed to be that cyber operations are considered armed attacks based on the object targeted and its effect on it. For example, shutting down the air defense system of a country or disrupting the functioning of an electrical grid, amount to an armed attack in cyberspace.[924]

To sum up, the destructive effect of cyber-attacks is achievable and can reach the level of an armed attack in the context of IHL. Also, Cyber operations might constitute an attack in the meaning of IHL not only by causing death, injury, or physical destruction or damage but also

---

[919] The Group of experts to the Tallinn Manual could not agree whether the damages to the centrifuges were sufficient to meet the armed requirement, and could not determine whether Stuxnet amounted to an IAC under IHL. See, Wallace D. and Jacobs CH., Ibid., p. 671.
[920] Schmitt M., Classification of Cyber Conflict, Ibid, p. 252.
[921] Schmitt M. and Vihul L., Ibid, p.70.
[922] Tallinn Manual, Ibid, Commentary on Rule 39, para. 5.
[923] ICRC , Cyber Warfare and International Humanitarian Law: The ICRC's position available online: https://www.icrc.org/en/doc/assets/files/2013/130621-cyber-warfare-q-and-a-eng.pdf
[924] Droege C., Get off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians, ICRC International Review 2012, Vol. 94, no. 886, p. 560.

any interference with the functioning of an object by disrupting the underlying computer system.[925] Although in practice, no armed conflict started based on cyber operations exclusively, it does not mean that such conflicts might not occur shortly. The US Secretary of Defense Leon Panetta noted: "The internet is a battlefield of the future where adversaries can seek to harm our country, to our economy, and our citizens. A cyber-attack perpetrated by nation-states and violent extremist groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation."[926] The challenge noted in the previous statement is based on the effects of cyber-attacks that are pervasive, insidious, and borderless. Though this is not seen as a challenge in an ongoing IAC if the victim state has identified the source of a cyber-attack, but will be more challenging when belligerent states employ private contractors or civilians to conduct operations that include cyber roles.[927]

Based on the previous analysis, there is no doubt that the role of armed groups[928] or NSAs in armed conflicts is regulated by the IHL (treaty and customary law) during an armed conflict. The recognition of the NSAs concerning international norms based on the GCs and AP II is vital, as such contribution will protect civilians in armed conflict zones from human rights abuses and violation of IHL rules.[929] According to Gabon Rona, there can be no IHL without identifiable parties to which such law applies by its obligations and rights. Although states may resist granting such groups any international legal personality, fearing to legitimate their actions. Yet, the development of the IHL and the binding character of CA 3 of the GCs and its AP II have shaped the rights and obligations of NSAs for being active in an armed conflict on the territory of a contracting party. Therefore, the parties are the fundamental elements of an

---

[925] The US Operational Law Handbook considered that cyber-attacks against electrical grid have the effect of shutting down electricity for civilian facilities with follow-on effects such as: unsanitary water and therefore death of civilians and the spread of disease because the water purification facilities and sewer systems do not work; death of civilians because the life support systems at emergency medical facilities fail; or death of civilians because traffic accident increase due to a failure of traffic signals. See, the Judge Advocate General's Legal Center and School, International and Operational Law Department, Operational Law Handbook, Charlottesville 2008, p.151.

[926] Panetta L., Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, 11 October 2012, United States Department of Defense.

[927] Melzer N, Cyber Warfare and International Law, Ibid. p. 34.

[928] An organized armed group is the armed wing of a non-state party to a NIAC, and may be comprised of either:

- Dissident armed forces (breakaway parts of state armed forces);
- Other organized armed groups which recruit their members primarily from the civilian population but have developed a sufficient degree of military organization to conduct hostilities on behalf of a party to the conflict.

The term organized armed group refers exclusively to the armed or military wing of an NSA to a NIAC. It does not include those segments of the civilian population that are supportive of the non-state party such as its political wing. See ICRC casebook, available online: https://casebook.icrc.org/glossary/armed-groups

[929] Article 3 common to all four of the Geneva Conventions of 12 August 1949.

armed conflict. In IAC only states and National Liberation Movements (AP I), as it was mentioned before, represent the parties to such conflicts; on the other hand, NIAC covers the involvement of governmental and non-governmental armed forces with certain requirements. The armed conflicts that include NSAs are well treated in treaties and doctrines and do not need more elaboration in this section. It is with no doubt that such conflict will be classified as NIAC unless the NSA is acting under the control of a State party and conducting operations or involved in hostilities against an opposing State party, then the NIAC is internationalized between the victim state and the state those armed groups fighting on behalf.[930] However, in a hybrid context, a fusion of non-state armed groups with non-kinetic means such as cyber operations that can be conducted from the territory of another state, more challenges to the classification of armed conflict are identified. This hybridization of warfare has strained the traditional classification of armed conflicts and more likely has the characteristics of both.

2.2.1. Hybrid International Armed Conflict

When considering an IAC based on the classification of IHL (treaty and customary), the scenario that would prevail is a conflict between two or more states, that are well regulated in GCs of 1949 and its APs. While, the hybridity of an IAC involves an operational and strategic level by combining conventional and unconventional, kinetic and non-kinetic means during the conflict, it will be mere IAC that involves different means and methods, that are neither novel nor challenging to the IHL framework.[931] CA 2 to the GCs is clear that a certain level of violence and parties to the conflict can identify the type of conflict, so there is nothing new about such hybridity and international law is well established to address such conflicts. Even when countries intervene in a conflict to either support the territorial State's armed forces or the NSA in its fight against another NSA or governmental forces, IHL still applies with no legal implications. For example, Russia and Georgia were engaged in an IAC in 2008. The conflict traces back its roots to the time when South Ossetia in 1990, supported by Russia, declared its independence from Georgia.[932] When Georgia in 2008 tried to take control over South Ossetia, it was faced with Russian military intervention in an attempt to support South Ossetia's secessionist efforts.[933] The military operation was supported by non-kinetic means.

[930] Tallinn Manual 2.0, Ibid. p. 380.
[931] Wittes B., What is Hybrid Conflict, Lawfare blog, 2015. https://www.lawfareblog.com/what-hybrid-conflict
[932] Joyce S., Along a Shifting Border, Georgia and Russia maintain an Uneasy Peace, NPR 2017, https://www.npr.org/sections/parallels/2017/03/13/519471110/along-a-shifting-border-georgia-and-russia-maintain-an-uneasy-peace?t=1611156869557
[933] Ibid.

Russia has launched cyber operations against Georgia before and during the armed conflict, which played a major role in the ongoing armed conflict, and in limiting Georgia's ability to disseminate information.[934] Although Russia did not acknowledge launching these cyber-attacks, computer security researchers managed to track the attacks and had evidence that a St. Petersburg-based criminal gang known as the Russian Business Network (R.B.N.) was behind these attacks.[935]

Nonetheless, whether adversaries used a combination of hybrid means in an IAC or not, does not change the nature of the conflict nor the classification. However, if the cyber-attacks launched during an armed conflict have led to civilian casualties or destruction of civilian property protected under IHL rules, and the State denied its responsibility or the attacks were not attributed or traced back to a party of the conflict, state responsibility for its violations to IHL rules will be compromised, but not the classification of an armed conflict. The Tallinn Manual takes a similar legal view that the mere fact that a cyber operation has been launched or otherwise originates from governmental cyberinfrastructure is not sufficient evidence for attributing the operation to that State but is an indication that the State in question is associated with the operation.[936]

Nevertheless, as mentioned above, the DDOS cyber-attacks against Georgia were before and during an armed conflict, so the question is whether the cyber-attacks that took place three weeks before the Russian physical military intervention in the South or the troops that moved into the conflicted zone, has commenced an IAC.[937] In this regard, the ICTY in the Tadic case considered that an IAC exists whenever there is a resort to armed force between States.[938] The court's statement reveals that neither the duration requirement nor an intensity requirement in terms of the number of victims or the destruction of property is needed for an IAC to exist.[939]

---

[934] Markoff J, Before the Gunfire, Cyberattacks, New York Times, 2008. https://www.nytimes.com/2008/08/13/technology/13cyber.html

[935] Ibid.

[936] Tallinn Manual 2.0, Ibid. Rule 7 p. 34-35.

[937] Taking the facts available about the conflict between Georgia and Russian in South Ossetia, DDOS attacks that targeted Georgia's servers were launched on 20 July 2008, while the Russian military intervention that included airstrikes and deployment of troops in South Ossetia took place in 8th of August 2008. See, Wallace D. and Jacobs Ch., Ibid. p. 668.

[938] ICTY, Prosecutor v. Tadic, Ibid., p. 70.

[939] The ICRC has commented on the GCs that: "any difference arising between two States and leading to the intervention of armed forces is an armed conflict within the meaning of Article2, even if one of the Parties denies the existence of a state of war.", the ICRC added:" it makes no difference how long the conflict lasts, or how much slaughter takes place." See, 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, 2nd ed., Cambridge University Press, 2016, para 236.

Additionally, the low threshold to IACs was explained in the 1960 commentary to the third GC and the intent of states behind, by which it highlighted that any difference arising between two states and leading to the intervention of members of the armed forces is an armed conflict within the meaning of Article 2, even if one of the Parties denies the existence of an armed conflict. It makes no difference how long the conflict lasts, how much slaughter takes place, or how numerous are the participating forces; it suffices for the armed forces of one Power to have captured adversaries falling within the scope of Article 4. Even if there has been no fighting, the fact that persons covered by the Convention are detained is sufficient for its application. The number of persons captured in such circumstances is, of course, immaterial.[940] Perhaps most importantly, the question is whether the DDOS attacks that targeted Georgia in 2008 commenced the beginning of IAC or not. To be able to answer this question, it is important to be able to first find concrete evidence that the attacks were launched by Russia being a part of the conflict, and whether the cyber-attacks were sufficient to trigger an IAC. Rule 82 to the Tallinn manual states that: "an IAC exists whenever there are hostilities, which may include or be limited to cyber operations, between two or more States."[941] Therefore, apart from the attribution requirement that was addressed in the second chapter of the thesis, and assuming that the cyber-attacks launched in the events of the armed conflict between Georgia and Russia in 2008 were attributed to Russia, it is seen that IAC exist from the time cyber-attacks were launched. However, the operations combining both kinetic and non-kinetic means must be treated based on the actual situation, by which non-kinetic means rely on the effects of the kinetic means. The previous statement is concluded from State practice rather than a legal framework.

To illustrate, based on previous analysis, taking into account rule 82 of the Tallinn Manual, the cyber-attacks between Russia and Georgia in 2008 were governed by IHL as they were part of an existing IAC. Therefore, though it may be seen that certain conflicts of conventional nature are easy to classify as IAC, however, its hybrid nature creates uncertainties and fault lines. From a legal perspective, while IHL applies the moment an armed conflict exists, cyber-attacks have to be taken into consideration to assess when the actual armed conflict started. While state practice did not reach a definite manner with regards to armed conflicts based solely on non-kinetic means, nevertheless it can be concluded that the current position is to treat non-kinetic attacks that have the same effect as kinetic ones in the same manner. In

[940] Commentary to the III Geneva Convention relative to the treatment of Prisoners of War, (Pictet J. ed.) 1960, p. 67.
[941] Tallinn Manual, 2.0, Ibid., at 379.

practice, states are still having the power in determining the interpretation of the international law in IAC, the reason why so many attacks are not reported or denied even though they amount to armed attack. The ICRC was clear in its commentary to CA 2 by suggesting that State can always pretend when it commits a hostile act against another State, that it is not making war, but merely engaging in police action, or acting in legitimate self-defense. The expression armed conflict makes such arguments less easy.[942]

Based on the previous analysis, cyber operations in contemporary conflicts cannot be ignored, especially since IHL is more geared towards regulating kinetic effects, while state practice is more shifting towards employing a broad spectrum of non-kinetic means and methods.[943] It is also noticed that current practices show that cyber operations which occur in isolation from kinetic attacks do not reach the level of armed violence, and even if who launched these attacks were identified, then either domestic law exercising jurisdiction over the person and the particular subject matter, or human rights law, apply. Although, it is generally accepted that cyber-attacks must meet the threshold of violence akin to those of more traditional means and methods of warfare and despite the restrictive impact of this traditional towards other cyber operations that meet the necessary violence of an armed attack without damage to persons or property. However, a less restrictive approach would lead to escalations in international relations with more armed conflicts and hostilities. Nonetheless, the author suggests that operations conducted in a hybrid manner involving other kinetic or non-kinetic means, even below the threshold of an armed attack, but accumulatively reach the level of violence required for an armed attack, then an armed conflict would commence. In such case, IHL can be expanded to cover cyber operations that traditionally do not meet the scale and effect threshold, such as severe data loss or financial loss, when in accumulative it is seen that these cyber operations are part of larger-scale attacks, such as military intervention or more violent cyber operations.

In applying the previous suggestion on the conflict between Russia and Georgia in 2008, it would have led to the applicability of IHL rules at the time cyber-attacks were launched, rather than such applying IHL due to the conventional intervention by Russia and direct confrontation. The accumulative theory of events and operations in an armed conflict is of high importance to tackle the possible legal uncertainty while choosing to apply the norms of

[942] ICRC Commentary on the First Geneva Convention, Ibid., p 32.
[943] Sari A., Legal Aspects of Hybrid Warfare, Ibid. https://www.lawfareblog.com/legal-aspects-hybrid-warfare

peacetime or LOAC. Nevertheless, attribution remains a vital indicator in identifying the link between actors and ongoing events, especially since an independent and impartial investigation can hardly be conducted in circumstances of growing tensions with a state labeled in advance as hostile.[944] While Rule 17 in the Tallinn Manual considers that certain State becomes an enemy of war if the perpetrators have operated according to instructions, guidelines or under the control of the state, and the State recognizes and accepts that operation as its own[945], it is unlikely to be reflected in State practice that has general tendency to deny any involvement in cyber-attacks. Nonetheless, cybercriminals might take advantage of the legal uncertainty and shift from being cybercriminals under peacetime regimes to being combatants with certain privileges under the IHL, a scenario that is highly possible due to the broader protection such attackers might receive under IHL if considered as combatants associated with another State.

Similarly, the Russian Federation has always been considering the conflict in Ukraine in 2014 as an internal conflict between the government in Kyiv and the self-proclaimed republics of DNR and LNR. That has been clearly expressed by the official representatives of the Russian defense sector considering the conflict in eastern Ukraine was a civil war between the nationalist power, which led the country as a result of a coup, and Donbas militias, that refuse to live in a country denying their right to speak their language.[946] Though, Kremlin is openly utilizing private military companies (PMCs) such as the Wagner group and proxy militias such as the Donetsk and Luhansk People's Republic in Ukraine to wage these hybrid operations exploiting the West's lack of understanding of these groups to maintain deniability and reduce the risk of military response, which would likely result if Russia has used its conventional forces in the battlefield.[947] Moreover, the Minsk agreement that was first signed in September 2014 and contained 12 measures to achieve a ceasefire, was breached numerous times, by which the OSCE Special Monitoring Mission to Ukraine documented that there were more than one million violations in Donbas since February 2015[948], did not include Russia as a party to the conflict and did not include any specific obligations on de-facto belligerent state implementation. Likewise, Ukraine issued legislation that classified the conflict in Donbas as

[944] Rasevic Z., "Cyber Warfare and International Cyber Law: Whither?", Journal of Criminology and Criminal Law, Belgrade 2020, p. 32.
[945] Tallinn Manual, Ibid. Rule 17.
[946] Russian defense commentator Viktor Likovkin, A statement in Nezavisimoe Voennoe Obozrenie, 10 July 2015.
[947] Clark M., Russian Hybrid Warfare, Military Learning and the Future of War Series, Institute for the Study of War ISW, September 2020, p. 27.
[948] Atland K., Destined for Deadlock? Russia, Ukraine, and the unfulfilled Minsk Agreements, Vol. 36, 2020, p. 122.

an anti-terrorist operation and that the proxy militias were called "terrorists" which does not correspond with the international legal framework and does not reflect the actual circumstances with the application of domestic law. The controversy surrounding the classification of armed conflict and the standards governing attribution is a key area of interest and the baseline for any effective response. And the Ukrainian conflict explained before, is a clear example of the inadequacy of attribution tests, especially effective control, in certain situations as to determine whether the conduct of an organized armed group should be attributed to a state and the level of involvement to transform a NIAC to an IAC and enable the rules of international law to apply more efficiently.

2.2.2. Hybrid Non-International Armed Conflict (Cyber and Non-State armed groups)

First, as discussed previously, two main bodies of treaty law regulate hostilities in NIACs, the CA 3 to the GCs and AP II that adheres only when the state in armed conflict is a party to the treaty and once additional factors are met.[949] CA 3 to the GCs defines NIACs as conflicts that are not international. While the ICTY in the Tadic case described such conflicts as "protracted armed violence between governmental authorities and organized armed groups or between such groups within a State." The AP II refers to NIAC as a conflict between a State's armed forces and dissident armed forces or other organized armed groups, so must be both organized and armed. Therefore, NIACs have common features that include the participation of an organized armed group in a conflict and a particular level of intensity. The hybridity of elements in a NIAC is more challenging than that of IAC because most internal conflicts lack detailed information and investigations about the facts and ongoing operations, most states deny the existence of a NIAC in their territory as it would legitimize the NSAs involved and trigger the rules of IHL to deal with the situation under its national laws, and the fact that non-state armed groups conduct operations among civilian population blending non-kinetic means of transnational effect by which the savage and brutality of civil wars are even greater than those of IAC. Hybrid actors operate either in concert with the state or compete with it, such actors depend on state sponsorship to flourish, but rather enjoy the flexibility that comes with not being a state.

[949] Deeks A., Is (or Was) Ukraine in a Non-International Armed Conflict, Lawfare Blog, 2014. https://www.lawfareblog.com/or-was-ukraine-non-international-armed-conflict

Furthermore, HW represents a type of irregular armed conflict that usually features state actors but in an unconventional manner by operating covertly. The early stages of HW are conducted unconventionally and states are increasingly engaging in proxy conflicts, afterwards, the regular armed forces reveal their true identity at the final stages of the conflict. States' reliance on NSAs in internal conflicts, is a form of Hybrid warfare. States deny their involvement in a conflict, though operationally are heavily involved through their proxies, to lower the likelihood of retaliation as the degree of responsibility for the groups that they control is disguised.[950] However, this section will focus on the hybrid means used during a conflict that does not involve an international character, as internationalizing a NIAC will be addressed later. Also, the author will highlight the use of cyber means by NSAs or governmental forces in an internal conflict and will address the hybridity of multiple armed groups to a single battlefield. Cyber operations play a central role in a hybrid environment and particularly in NIAC. Rule 23 to the Tallinn Manual on the characterization as NIAC notes that NIAC exists whenever there is protracted armed violence, which may include or be limited to cyber operations, occurring between governmental armed forces and the forces of or more armed groups. The confrontation must reach a minimum level of intensity and the parties involved in the conflict must show a minimum degree of organization.[951] The Group of Experts' definition has reproduced a combination of CA 3 of the GC 1949, which imitates customary international law, and the case law development of the issues of intensity and organization to cyber operations.

i- The Islamic State in Syria and Iraq (ISIS)

One of the most hybrid NSAs that is relevant to the type of armed groups investigated in this section, is what so-called ISIS (also known by the deliberately derogatory Arabic acronym as Da'esh).[952] The armed group has not been considered a proxy group nor an ordinary NSA, rather it is a fusion of typical armed group practices with ideas of statehood in a dedicated effort to govern captured areas in a state-like fashion.[953] ISIS's hybridity is represented in its

[950] Graja C., SOF and the Future of global Competition, CNA, Washington 2019. https://www.cna.org/CNA_files/PDF/DCP-2019-U-020033-Final.pdf
[951] Tallin Manual, Ibid. Rule 23, p 84.
[952] For more information about the ISIS: formation, legality to use force, and the interplay between IHL, IHRL and Islamic Law. See Al Aridi A., An Interdisciplinary Approach to Combat ISIS: Legal, Political, and Socio-Economic, Paper presented at the International Network of Doctoral Studies in Law, 4th International Conference for PhD Students and Young Researchers: Interdisciplinary approach to Law in Modern Social Context, Vilnius April 2016, pp. 26-36.
[953] Cambanis Th., Esfandiary D., Ghaddar S., Hanna M., Lund A. and Masour R., Ibid. p. 106.

combination of secular and religious forms of structure and agency, yet it is not a mystery but a mere NSA under law. First of all, the group has taken over a large swath of territory in Syria and Iraq and had its operational headquarters in the Syrian provincial city of "Al-Raqqa"[954], also consisted of a considerable number of fighters estimated by the CIA between 20,000 and 31,500 in Iraq and Syria, while others consider that number of fighters range between 80,000 and 200,000.[955] ISIS is a group that applies a strict interpretation of Sharia Law and has conducted countless war crimes and violations of the international law (Arbitrary detention, fair trial violations, torture and other forms of ill-treatment, collective punishments of citizens, brutal crimes that amount to war crimes and crimes against humanity or genocides).[956] By which ISIS was considered as the "most deadly terrorist organization operating at that time and the greatest threat to world peace, amassing more fighters, more funding, and more territory than any other terrorist movement."[957]

Applying the GCs and its APs to the conflict that involves ISIS as a NSA is essential to identify the classification of the armed conflict, especially since the conflict was not limited to one specific territory, but was taking place in both Iraq and Syria. Also, the hostilities were complex by which ISIS has conducted operations against the governmental forces of both states, against other armed groups involved in the conflict (Kurdish militias, Iranian backed militias "Popular Mobilization Forces", Al Nusra Front "associated to Al-Qaeda", the Free Syrian Army "the military wing of the Syrian people's opposition to the regime" …etc.).[958] Moreover, the conflict in Syria and Iraq was hybrid due to the involvement of conventional troops and irregulars, interventions by third states that targeted ISIS on the territory of Syria and Iraq (Anti-ISIS Coalition and Turkey), and border clashes between ISIS and neighboring state's armed forces (Turkey and Lebanon). After all, despite the involvement of numerous armed groups and state actors in the conflict, IHL is the applicable law to the conflict.

---

[954] Gill T., Classifying the Conflict in Syria, International Law Studies 2016, vol. 92, no 353, p. 359.
[955] Ibid.. see also Sciutto J, Crawfor J. and Carter CH., ISIS can Muster between 20,000 and 31,500 Fighters, CIA says, CNN September 12, 2014. http://edition.cnn.com/2014/09/11/world/meast/isis-syria-iraq/
[956] Iraq Events of 2018, Human Rights Watch Report. https://www.hrw.org/world-report/2019/country-chapters/iraq
[957] Lekas A., ISIS: The Largest Threat to World Peace Trending Now, Emory International Law Review, 2015-2016, vol. 30, p. 314.
[958] See more, Al-Ubaydi M., Combating Terrorism Ctr. At West Point, The Group calls itself a State: Understanding the Evolution and Challenges of the Islamic State, 2014, p. 18. See also, Wallace D., McCarthy A. and Reeves Sh., Trying to Make Sense of the Senseless: Classifying the Syrian War under the Law of Armed Conflict, Michigan State International Law Review 2017, Vol. 25.3, p. 567- 568.

While CA 3 to the GCs 1949 is applicable in the case of armed conflict not of an international character occurring in the territory of one of the high contracting parties, the armed hostilities taking place in two different states with a one-armed group does not change the nature of the conflict, rather it will be dealt with it as one in two different States. The fighting between the Syrian government forces and the anti-governmental groups has protracted armed violence based on the ICTY understanding of armed violence in the Tadic case. Nonetheless, with the myriad of actors involved in the Syrian conflict, the classification of the conflict might be vague, especially with the involvement of state actors. Nevertheless, an important perspective on the relationship between different actors that fight on the same side in a situation of armed conflict is the "support-based approach" that was developed by Tristan Ferraro and endorsed by the ICRC.[959] Based on this approach, a conflict that originates as a NIAC between the territorial state and NSA, as long as the supporting entities intervene against the latter (NSA), the conflict remains a NIAC because of the non-state nature of the opposing parties.[960] In any case, the conflict with ISIS will be classified as NIAC because the conflict is either between governmental forces and NSA, or between such groups within a State.[961] With regards to the level of intensity of the armed conflict, ISIS operations have crossed the threshold recognized by both the CA 3 and AP II, mainly by the territorial control and protracted armed violence.

On the other hand, the organizational criteria that are essential to implement IHL to armed groups under the protective scope of CA 3 and the AP II, also based on the ICTY factors and indicators provided by the ICTY in the Ljube and Tarculovski case, there is no doubt that ISIS fulfills the aforementioned requirements.[962] ISIS has created a well-organized command structure that included institutions, judicial authority, and Islamic courts. Also, fulfilled the factors related to logistics and communications, ability to recruit fighters globally through multiple traditional (mosques, communities) and non-traditional (social media, financial institutions). ISIS has evolved to the level of quasi-state, so there is no reason to assume that it

[959] Support-based Approach The approach was initially put forward in relation to cases of support provided by multinational troops deployed under the aegis of an international organization (IO) to States involved in a territorial NIAC against an armed group (AG), and later expanded to cover any hypothesis of a State or 'supranational organization' supporting the party to a pre-existing NIAC. Ferraro T., The Applicability and Application of International Humanitarian Law to Multinational Forces, International Review of the Red Cross 2013, p. 561. http://www.rulac.org/assets/downloads/Feraro_Multinational_forces_IRRC.pdf. See also, Ferraro T, The ICRC's Legal Position on the Notion of Armed Conflict involving Foreign Intervention and on Determining the IHL Applicable to this type of Conflict, International Review of the Red Cross 2015, p. 1227.

[960] Maganza B., Which role for Hybrid entities involved in multi-parties NIACs? Applying the ICRC's support-based approach to the armed conflict in Mali, Questions of International Law Journal, May 31, 2019, Vol. 59, p. 38-39.

[961] ICTY, Prosecutor v. Tadic, Ibid. para 70.

[962] ICTY, Prosecutor v. Ljube Boskoski and Johan Tarculovski, Ibid. para 196-203.

is not an organized armed group with the required level of intensity and organization to classify the conflict it is involved in as NIAC, although it extends to the territory of third countries which is justified earlier in what so-called "spill-over". One of the issues raised by the hybrid nature of ISIS is whether the group is bound by IHL.

To sum up this argument, it is vital to differentiate between the ability to comply with international norms and the unwillingness to do so. The relevant laws and opinio Juris, mentioned above, are clear that groups must have the ability to implement based on the existence of disciplinary rules or mechanisms within the group. ISIS has the ability but not the will (ability to comply, not actual compliance), and that was reflected by its actions and crimes committed in the conflict zone and overseas. After all, the actions of ISIS will be more challenging with regards to the charges for terrorism and war crimes before the courts. Though this is not covered by this study, important to mention that such cases demonstrate that ISIS fighters are not only terrorists but also be considered as participants in a NIAC in Syria and Iraq, taking into account that both states are not parties to the Rome Statute that requires the acceptance of states for the jurisdiction of the ICC to prevail.[963] Also, states may refuse the formation of an international tribunal to prosecute violators of war crimes, for example, Syria has rejected any international judicial mechanism that contradicts with its national judiciary powers.[964] The Rome status still stipulates that the assembly of states parties shall discuss and deal with, pursuant to article 87 that gives the ICC the authority to refer circumstances of non-co-operation by states to the assembly of states parties[965], or to the security council if the referral was by it to the ICC. However, the assembly of states parties hardly ensures any practical outcome as it does not have the same authority as the UNSC. According to Bashir Ali Abbas, "this confusion opens the prospects for a hybrid tribunal which reconciles municipal and international law and resembles an international court set up within the domestic judicial apparatus."[966] An argument that necessitates further research in the legal domain.

ii- Non-State Cyber Actors in NIAC

For NIAC to exist, it is important to differentiate between criminal activities and armed conflict. That is more important when non-kinetic means are used by NSA in hostilities taking

[963] Rome Statute of the International Criminal Court, Ibid., Article 12 (1) and Article 13.
[964] Abbas B., Prosecuting the Islamic State: The Case of a Hybrid Tribunal, Institute of Peace and Conflict Studies IPCS, 16 May 2019. http://www.ipcs.org/comm_select.php?articleNo=5586
[965] Artile 112.2(f) of the Rome Statute.
[966] Ibid.

place on the territory of a state that is considered of hybrid nature. For example, Hackers are protected under the IHL during an armed conflict, unless they took a direct part in hostilities that deprives them of legal protection.[967] Nonetheless, members of the virtual organization may never meet nor even know each other's actual identity. Such groups can act in a coordinated manner against the government or an organized group, take orders from a virtual leadership, and be highly organized. Schmitt has also added that in practice one element of the group might be tasked to identify vulnerabilities in target systems, a second might develop malware to exploit those vulnerabilities, a third might conduct the operations and a fourth might maintain cyber defenses against counter-attacks.[968] However, organized groups operating in cyberspace are hardly detected based on the traditional definition of organized armed groups under IHL (organized and armed). Cyber actors can create confusion to the applicable law during an armed conflict, such actors are unlikely to be visible with identifiable uniform or by openly carrying out a certain weapon. Conversely, combatants may be targeted solely based on their combatant status and must be recognizable combatants during or before an armed attack.[969] The aforementioned creates a legal challenge to the principle of distinction during an armed conflict. Nonetheless, Article 44 of the AP I considered that soldiers who do not identify themselves as combatants by wearing a uniform or by carrying arms openly during or in preparation for the engagement would likely be stripped of their combatant privilege by a tribunal.[970] Yet, it generates a challenge to the classification of a conflict too.

While assessing the required degree of organization of NSA conducting cyber operations, a few scenarios might be taken into account. First, cyber operations are conducted by armed groups that already meet the requisite degree of organization and intensity, such as Taliban, ISIS, or Hezbollah, then it is with no doubt that a NIAC would be triggered. Second, if private individuals conducted cyber operations in an ongoing armed conflict or not, such attacks will not trigger an armed conflict, as the group must have a certain level of organization that allows

[967] The term hackers encompass variety of people in so many different activities that exclude them from being considered as combatants, the reason why most cyber operations are not linked to armed conflict. At the same time, hackers are usually groups of civilians that are protected under international law from direct attacks, whether in peacetime by national laws and IHRL, or during an armed conflict by IHL. See, Cyber Warfare and International Humanitarian Law: The ICRC's position, Ibid. p.3. See also, Tallin Manual, Ibid. at 95 and 104.
[968] Schmitt M., Classification of Cyber Conflict, Ibid. p. 256.
[969] Courlam A., Unarmed Attacks: Cyber Combatants and the Right to Defend, The California International Law Journal, Winter 2018, Vol. 26, no. 1, p. 21.
[970] Sassoli Mand Bouview A., How Does Law Protect in War? International Review of the Red Cross, Geneva 1999, no. 836, p. 117.

it to act in a coordinated manner heightening its capability to engage in violence.[971] Therefore, it is unlikely that the organizational requirement to be met virtually, assuming that the group of hackers is conducting operations solely online without any connection to a State or an existing organized armed group involved in an armed conflict. Correspondingly, the ICRC has acknowledged that whether cyber network attack alone will ever be seen as amounting to an armed conflict will probably be determined in a definite manner only through future state practice[972].

Another problem that might arise, is that certain armed groups can influence or recruit individual hackers to launch attacks against another state armed group or government. After all the linkage of attribution will be even harder and the ability to target these hackers as combatants based on their relation to the armed group, will probably violate the IHL, especially if the individual members of an organized group carried out cyber-attacks not on behalf of the group, but on their own accord, then the group does not meet the armed criterion.[973] Such activities can be categorized as "patriotic hacking" where individuals voluntarily use their computer systems to conduct actions harmful to the belligerent, such as the cyber-attacks during the "Operation Cast Lead" in Gaza Strip by which there were instructions from sympathizers on both sides to the conflict to attack other party's website and networks.[974] As explained, such activities do not trigger an armed conflict, as attackers do not reach the required level of an organized armed group, but it is an indicator of a growing tendency in civilian engagement in cyber-attacks during armed conflicts that will have future legal and humane implication. However, with regards to the level of command, the ICRC Commentary to Article 1(1) of the AP II that required that a group must be under responsible command before a NIAC, has lowered the article's strict threshold and considered that some degree of organization of the insurgent armed group is required.

---

[971] Schmitt M., Classification of Cyber Conflict, Ibid. p. 255. Equally important, even if number of individuals are acting collectively in spreading malware tools, they do not qualify as organized armed group. See Geis R., Ibid. p. 635.

[972] DORMANN K., "The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint", ICRC 2001. See also, BOYSTOM K., International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Swedish National Defense College, Stockholm 2004, p. 142.

[973] Schmitt M., Ibid. p. 258.

[974] Shachtman N., Wage Cyberwar against Hamas, Surrender Your PC- Wired 8 January 2009. https://www.wired.com/2009/01/israel-dns-hack/

Given these points, the ICRC is taking the challenges of cyber operations in armed conflict seriously and urges all states to recognize IHL rules and protection it offers against the human costs of cyber operations, and requires full respect and protection to medical facilities and personnel at all times. Apart from the role of cyber NSAs in the classification of an armed conflict, the international community, and mainly ICRC as the guardian body of IHL, are more concerned about the nature of cyber-attacks and their technical characteristics to the IHL principles. The ICRC published a report in 2019 about the challenges of contemporary armed conflicts, and has considered that cyber-attacks in armed conflict carry the following risks:

- "Overreaction and escalation, due to difficulty in assessing whether the attacker aimed to gather information or cause physical damage (intent of the attacker);
- Can proliferate in an uncontrolled manner allowing the cyber groups or hackers to reengineer or repurpose a cyber tool to a more malicious end;
- Identifying the source or who created or launched the cyber-attack and holding them responsible for their actions under IHL, remains a challenge. A perception that will allow hackers or armed groups less scrupulous about violating international law;
- The development and increasing reliance on cyber operations by the most sophisticated actors will cause major human harm in the future that is observed so far." [975]

Therefore, a NIAC is triggered once cyber-attacks are launched by the NSA that meet the level of intensity and organization. On the other hand, if attacks are launched solely by a group of individuals or decentralized hackers that do not meet the traditional criteria of armed groups, it would not lead to an armed conflict even if the attacks collectively reached the level of armed violence. It is needed to distinguish between the general issue of cyber security from the specific issue of using cyber operations in an armed conflict. For instance, cyber-attacks or cyber terrorism may evoke methods of warfare but they may not necessarily be conducted in armed conflict. Hence, it does not mean that such operations are in a legal vacuum as international law and in particular the UN Charter is applicable, also the IHRL still applies, but without the existence of an armed conflict, IHL does not apply. Another equally important point is whether the cyber operations meet the criteria to be considered hostilities. It will be relevant once the attack was launched by a member of armed forces in an IAC or a member of an organized armed group involved in an ongoing NIAC. But more challenging once a civilian

[975] International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting the Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, Document prepared by the ICRC for the 33rd International Conference of the Red Cross, Geneva 9-12 December 2019, pp. 892-93.

conducts such operations, is that a civilian who directly participates in hostilities in an ongoing armed conflict, loses his entitlement to protection from attack as long as these acts are adversely affecting the enemy's military capabilities, having a direct link to the resulting harm, and having the requisite belligerent nexus.[976] The future will provide relevant state practices in this field that would either expand further the applicability of IHL to even less organized cyber groups or will require stricter rules of compliance that will cover the civilian sector. Conclusively, the hybrid element reflected in the employment of NSAs with non-kinetic means can create a challenge to the IHL based on their ability to launch operations below the threshold of armed violence, and in a decentralized manner but in a more aggressive manner than in their regular peacetime relations, or beyond the geographical limitation of armed conflict. Also, the challenges that may arise are more related to the status of combatants and international legal obligations of NSAs concerning the detention of members of state armed forces or civilians appears to be a central issue. Such operations are not unregulated by other bodies of legal regimes but will be a case-by-case examination.

iii- Geographic Limitation for IHL Applicability to Cyber-Attacks in NIAC

Organized armed groups or individual hackers in contemporary conflict can conduct cyber operations as means of striking at their asymmetric opponent[977]. As explained before, the nature of cyber-attacks allows them to be launched from any location far from the battlefield by either using the cyber infrastructure located in another neutral State or from multiple States. However, it is concluded that IHL applies to operations in cyberspace and is flexible enough to accommodate new technological developments[978]. Specifically, various rules and prohibitions arising such as the principle of distinction do not depend on the type of weapons or method used. Yet, various other humanitarian law prescriptions require careful assessment in view to specific features of cyber-attacks, mainly that IHL does not endorse nor prohibits computer network attacks but imposes certain constraints about the conduct of hostilities in cyberspace. Also, parties to an armed conflict are prohibited from employing means which cannot be directed at the specific military objectives to minimize incidental loss of civilian life or damage to civilian objects. But what is also highly important is the geographic limitation

[976] ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Ibid., p. 991.
[977] Schmitt M., Classification of Cyber Conflicts, Ibid. pp. 231-251.
[978] ICRC Commentary to AP I, Ibid., para. 1476.

and relevance to the applicability of IHL in the context of cyberspace. In Schmitt's territory-centric conception of international law, armed conflict is limited to locations such that it does not disturb the spatial order.[979] This may not be the case with cyber-attacks in an armed conflict. For example, botnets evolve on connected nodes on a global scale, and belligerents must take this into account when having to defend against it. Therefore, attacks like Stuxnet defy the spatial geography of States, instead of allowing them to project force through the alternate geography of cyberspace.

First of all, the extraterritorial parameters in NIAC are not clear as its law is designed for internal application. At the same time, NSAs have developed at an organizational level and created covert cells in different countries that contribute either financially or militarily to the group, a hybrid adversary or means are quite challenging. For instance, in a cyber context, the scenario that our analysis envision for the interest of this section is that State (A) is in a NIAC with an armed group (D) on its territory. State (A) gets targeted by a malicious cyber-attack that shut down its air force's command and control center, and three jets of its air force crashed due to communication loss. The attacks were traced and identified that group of hackers affiliated with Armed Group (D) are responsible for the attacks but located in the territory of State (B) that is not involved in the NIAC, nor has any control over the group of hackers on its territory. In this case, State (A) finds itself obliged to either target the group on the territory of State (B) based on its right to self-defense, which would highly lead to violation of territorial sovereignty. Or, it will consider expanding the NIAC to cover the territory the group of hackers is located in, which also will require the territorial State's consent, otherwise, an IAC between the two states will rise. To legally address such scenarios, an examination of the geographic scope of application of IHL to NIAC in a cyber context will be required. This discussion is relevant as it represents the hybridity of means that involve NSAs and cyber-attacks, as well the extraterritorial effect offered by technological means and its impact on applicable legal regimes.

Initially, despite the acknowledgment that CA 3 and relevant customary international law apply extraterritorially, there are inconsistencies in the rationale for the type of extraterritorial conflicts deemed to be covered by NIAC law. The ICTY when dealing with the geographic

[979] Blount P.J., How Cyberspace Changes International Conflict, E-International Relations, December 8 2019, p. 1. Available online: https://www.e-ir.info/2019/12/08/how-cyberspace-changes-international-conflict/#_ftn15

scope of CA 3 considered that "IHL continue to apply in the case of internal conflicts to the whole territory under the control of a party, whether or not actual combat takes place there."[980] Therefore, State (A) will be able only to target the armed group on its territory, as the group of hackers affiliated with the armed group does not control territory. That was reflected in AP II that only applies when organized armed groups control territory, and this instrument is thought to be inapplicable to cyber-only conflicts but involves an organized armed group that controls territory and conducts such operations, while in cyber-space such groups cannot control territory based on virtual operations. Some might argue that the law of neutrality applies in armed conflicts of international nature, by which the neutral State is required to prevent its territory from being used by belligerent as a place from which to launch attacks.[981] However, the law of neutrality might find a resort in an IAC, but in NIAC reasoning that law of neutrality is applicable to suppress the NSA's cyber operations without the territorial State's consent is arguable and have legal consequences. The U.S. appears to be in favor of this approach in the context of kinetic armed conflicts against NSAs that transcend a single State's borders.[982] But State practice does not support the expansion of the law of neutrality to NIACs.[983] On the other hand, CA 3 and Article 1 (1) of AP II contain a territorial link in defining a NIAC, also this is reflected in jurisprudence.[984] According to Schmitt, "While a State embroiled in a NIAC may sometimes cross borders into other states (arguably included those that are distant) to take the fight to its enemy under jus ad Bellum norms, it may not do so based solely on the fact that it is engaged in an armed conflict."[985] What Schmitt projected is that spill-over conflicts under certain circumstances might lead to the border crossing, but that is arguably in cases of distant territory and cannot be norm-based solely on the involvement of an armed conflict.

---

[980] Prosecutor v. Tadic, Appeal Trial Ibid. para 70.

[981] Tallinn Manual, Ibid., Rule 93. To illustrate, Law of neutrality is applied if a belligerent is initiating or conducting cyber-attacks against another belligerent using the cyber infrastructure of a neutral State, the neutral State must make efforts to terminate that use. And if the neutral State is unwilling or unable to stop that belligerent. Also, according to the Manual, it is well established in customary international law that a belligerent power may take action to end serious violations of neutral territory by an opposing belligerent when the neutral Power is unable to prevent belligerent use of its territory. See, Tallinn Manual Ibid., Rule 94. Furthermore, some have argued that in such cases the unable or unwilling test can be applied allowing targeted State to such cases. See, Deeks A., The Geography of Cyber Conflict: Through a Glass Darkly, International Law Studies, U.S. Naval War College, 2013, Vol. 89, pp. 7-8.

[982] Deeks A., Ibid. p. 8.

[983] Schmitt M., Charting the Legal Geography of NIAC, International Law Studies, U.S. Naval War College, 2014, Vol. 90, p. 6.

[984] The ICC Chamber in Bemba Gombo decision conclude that: "an armed conflict not of an international character, takes place within the confines of a State territory." ICC, Prosecutor v. Jean-Pierre Bemba Gombo, ICC-01/05-01/08, Decision on the Confirmation of Charges, Pre-Trial Chamber II, June 15, 2009, p. 231.

[985] Schmitt M., Charting the Legal Geography of NIAC, Ibid. p. 6.

Moreover, the geographic limitation of armed conflicts is reflected indirectly in Article 52(2) of the AP I, which is generally accepted as a reflection of customary international law in both IAC and NIAC. The article states that attacks shall be limited strictly to military objectives that make by their nature, location, purpose, or use an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offer a definite military advantage[986]. Applying this rule to justify the expansion of NIACs in cyber has legal effects by which although it renders the NSA's ability to conduct operations as the infrastructure used in the operations qualifies it as military objective and is relevant in an armed conflict, yet the interconnectivity of cyberspace and its civilian infrastructure nature will allow NSA to turn components of the worldwide cyberinfrastructure into legitimate military objectives.[987] Similarly, another important point that is highly relevant to cyber actors and their interconnectivity, is that the ICRC has rejected the notion that a person carries a NIAC with him to the territory of a non-belligerent State, on the basis that it would have the effect of potentially expanding the application of rules on the conduct of hostilities to multiple states according to a person's movement around the world as long as he is directly participating in hostilities concerning a specific NIAC.[988] ICRC has by this rejected the concept of "Global Battlefield" that can be relevant to "targeted killings" and the global war on terror and suggests that such operations should be assessed under the rules of law enforcement. Despite the growing tendency of some States, in particular the United States, towards applying the "unable or unwilling" test to expand the NIAC law based on an analogy from existing international law governing jus ad Bellum, however, the author agrees with ICRC's approach and considers that the drawbacks of potential attempts to expand the NIAC law to cyber-attacks that might be generated from neutral States, not bordering the territory of the State in conflict, outweigh the advantages. Concerns about a global battlefield also stem in part from fear that a non-geographically focused IHL paradigm would lead to more since targeting could be status-based and because IHL instead of IHRL proportionality norms would govern attacks.

Therefore, it is concluded that cyber-attacks generated from non-belligerent states impose certain challenges when the victim State is in a NIAC. Even if the relationship is confirmed

---

[986] Article 51(2) of the AP I relating to the Protection of Victims of International Armed Conflict.
[987] Geiss R., Cyber Warfare: Implications for Non-International Armed Conflict, International Law Studies, U.S. Naval War College, 2013, Vol. 89, p. 640.
[988] International Committee of the Red Cross, International Humanitarian Law and the Challenges of Contemporary Conflicts, Report Prepared for the 31st International Conference of the Red Cross and Red Crescent, October 2011, p. 22.

between the attackers and the armed group with which the State conflicts, yet expanding the NIAC to the territory of other State without its consent has legal consequences. It was also recognized that IHL's applicability in NIAC is viable with the spill-over incidents but makes sense if the applicability was border-based that is strictly limited to the territories of those states qualifying as parties to the conflict. Moreover, with the evolving role of NSAs in cyberspace and their ability to create worldwide cells and branches, such attacks might be launched from anywhere at any time, in an armed conflict or peacetime. So, targeting these groups would risk the evolvement of a global battlefield that has more disadvantages on the international peace and principles of IHL. As explained in the second chapter, cyber-attacks are not in a legal vacuum, and the rules of Jus Ad Bellum are capable of either binding states to control their infrastructure based on due diligence or controlling cyber groups according to its domestic laws. So coming back to the example suggested at the beginning of this section, in such case cyber-attacks originated from a third neutral State must be dealt with them through the law enforcement of the territorial State as long as it did not consent to any retaliation in its territory, and if the State is unable or unwilling to stop the threat and prosecute the members who conducted such attacks, then Jus Ad Bellum and other legal regimes are capable of addressing the State responsibility with regards to its wrongful acts in not securing its territory from being used to conduct operations against another States. However, even states with the most advanced technology might find it difficult to detect and immediately end malicious cyber activity that occurs on or originates from their territory.

2.2.3. Hybrid Warfare in a Co-existing Armed Conflict

In contemporary conflicts, both IAC and NIAC can exist on the same battlefield in which they do not reflect the traditional concept of IAC, nor internal conflict. But rather these conflicts are seen to involve multiple State and NSAs, operations below the threshold of armed conflict, even fragmented relationships between the actors that make it challenging to identify which groups can be considered a party to a particular armed conflict. HW and its means have a great impact on either creating this co-existence or thriving on it. Such co-existence, categorized sometimes as mixed or parallel armed conflicts, combine characteristics of both types of a conflict, challenges the classification of the conflict, and thus the identification of the relevant framework, the reason why it raised doctrinal debates.

The hybrid nature of contemporary armed conflicts lies in the core of the confusion created in multi-dimensional, multi-actors, and fusion of non-conventional and conventional elements. For instance, an attribution that is considered as one of the utmost complexities provided by new technologies, in particular cyber operations, creates technical issues and uncertainties to IHL.[989] And while conflict is classified on the assumption that the adversary's identity is recognized (State or NSA), attribution whether detected during an armed conflict or not can have the impact on either preserving the nature of the conflict or possibly changing it, such as internationalizing a NIAC, thereby placing it under CA 2 instead of CA 3.[990] Another problem that is similar to the cyber operations with regards to attribution, is the use of proxy actors that tend to mask their operations and true identity in an ongoing armed conflict. The ICRC often describes NSAs as being organized horizontally rather than vertically and some of them may not even constitute one single group at all.[991] While the jurisprudence of international criminal courts, international lawyers and NGOs such as the ICRC have sought to further develop this regime for unity between that apply to IAC and NIAC under IHL, by considering the extent to which elements of the two protocols constitute customary international law[992]. However, the classification is still very significant though the gap between the two types of armed conflict has narrowed, since considerable differences remain such as the position and status of armed groups and their members, and rules relating to the targeting of specific types of objects and the weapons which may be employed.[993] An ICRC committee-published guide in 2006 observed that:

> "Today, there is a general tendency to reduce the difference between IHL applicable in international and NIACs. The jurisprudent of international criminal tribunals, the influence of human rights, and even some treaty rules adopted by states have moved the law of NIAC close to the law of IACs, and it has even been suggested in some quarters that the difference be eliminated. In the many fields where the treaty rules still

[989] In this regard, the experts in Tallinn Manual 2.0 with regards to the uncertainty to the attribution of cyber operations, agreed that: "States must act as reasonable States would in the same or similar circumstances when considering responses to them. Reasonableness is always context dependent. It depends on such factors as reliability, quantum, directness, nature, and specificity of the relevant available information when considered in light of the attendant circumstance and the importance of the right involved. These factors must be considered together. Importantly in the cyber context, deficiencies in technical intelligence may be compensated by, for example, the existence of highly reliable human intelligence." See, Tallinn Manual 2.0, ibid, at 82.
[990] Wallace D. and Jacobs Ch., Ibid., p. 683.
[991] ICRC Report, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, October 2019, p. 50.
[992] Sassoli, Bouvier and Quintin, Ibid, p. 124. See also, Lovat H., Negotiating Civil War, The Politics of International Regime Design, Cambridge University Press 2020, p. 200.
[993] Gill T., Classifying the Conflict in Syria, Ibid. p. 377

different, this convergence has been rationalized by claiming that under customary international law the differences between the two categories of conflict have gradually disappeared."[994]

Nevertheless, contemporary conflicts are varying between being mere IAC, NIAC, or what was labeled by some scholars as internationalized armed conflict or internationalized NIAC. The latter is not described or defined in any treaty provision, but the concept has been raised numerous times by states and legal experts including the ICRC that referred to this concept in cases where NIACs are subject to outside intervention on either side of the conflict, whether or not the intervention transformed the conflict or altered the legal regime applicable.[995] The multifaceted nature of armed conflicts must be determined based on the prevailing facts and not on the subjective views of the parties to the armed conflict. The latter was reflected by the ICTY that stated:" the determination of the intensity of a conflict and the organization of the parties are factual matters which need to be decided in the light of the particular evidence and on a case-by-case basis."[996] It was also deliberated by the ICTR that considered the following: "the definition of an armed conflict per se is termed in the abstract, and whether or not a situation can be described as an "Armed conflict", meeting the criteria of CA 3, is to be decided upon a case-by-case basis."[997]

With this in mind, HW elements and methods are very useful strategies for states and NSAs to create a legal grey zone in which the international law and international tribunals will have a hard time identifying and examining the facts. Additionally, while states tend to deny their responsibility or direct involvement in armed conflicts, NSAs on the other hand have evolved to a certain level that makes them capable of using or misusing the laws based on the interest that serves their military and strategic operations. The grey zone in classifying armed conflict has legal impacts on the applicability of IHL, and is seen as an opportunity through State's Lawfare by deviating from and defying international consensus about what is lawful in the conduct of war and armed conflict, are evidence of violations of international law that thrive on certain ambiguities. For example, targeted killing has not gained international credibility

[994] Sassoli, Bouvier and Quintin, Ibid. Chapter 2, p. 23-24.
[995] Ferraro T., The ICRC's Legal Position on the notion of Armed Conflict involving Foreign Intervention and on determining the IHL applicable to this type of conflict, International Review of the Red Cross 2015, Vol. 97, no. 900, pp 1241-42.
[996] ICTY, the Prosecutor v. Limaj et al., Judgment by Trial Chamber II, Ibid., para 90.
[997] ICTR, The Prosecutor v. Rutaganda, Case No. ICTR-96-3-T, Judgment by Trial Chamber I, 6 December 1999, para. 92.

due to the challenges it imposes on the geographical requirement of an armed conflict, the persons and objects that may be targeted varies between the two types of conflict, yet is an available option for any government that would allow them to rewrite the laws of war to make international consensus-defying policies they wish to employ appear legal.[998] Additionally, the regime on prisoners of war and occupation is unsettled in the context of NIACs leading to uncertainties on the treatment of captives in a multifaceted armed conflict with fragmented actors. However, for the interest of this section, the study will analyze the internationalized NIAC concept (hereinafter INIAC) based on the examples of armed conflicts to further help the reader understand the nature of HW and its impact on the classification of armed conflicts, and briefly conclude whether co-existence of armed conflicts under the traditional classification of IHL is capable of addressing its complexity, or a new legal classification added to the two classic types of conflict will be more satisfactory.

i- The Applicability of IHL to a Co-existing Armed Conflict

In the first place, the co-existence of armed conflicts can ensue when a foreign State or coalition intervenes in an ongoing NIAC on the side of an NSA in its fight against the government forces of the territorial state. For example, the NATO intervention in the internal conflict in Libya escalated after the military airstrike in 2011 against the Gaddafi forces. Even though the intervention is cited as a model for implementing the so-called "Responsibility to Protect (R2P)" that was praised as a humanitarian success, it is not disputed that it is an IAC because State or coalition is using force against another state. So, the conflict turned to have two dimensions, a NIAC between Gaddafi forces and rebels, and an IAC between the coalition and Libya. In another scenario, when State (A) is in an armed conflict with State (B), and an armed group in State (A), meeting the requisite level of intensity and organization, conducted military operations against State (A). Then, State (A) is in an IAC with State (B), at the same time in NIAC with the armed group on its territory, unless the armed group is acting on behalf of a foreign State (de facto organ), then the whole situation will become an IAC.[999]

The aforementioned are classical examples of mixed armed conflicts and are not novel. For example, the ICTY's Appeals Chamber in the Tadic case stipulated that:

---

[998] Hajjar L., Lawfare and Armed Conflict: Comparing Israeli and US Targeted Killing Policies and Challenges against them, Issam Fares Institute for Public Policy and International Affairs, Research Report, Beirut 2013, p. 24.

[999] Vite S., Co-existing International and Non-International Armed Conflicts in one Country, Ibid. pp. 59-60.

- "It is indisputable that an armed conflict is international if it takes place between two or more States. Besides, in case of an internal armed conflict breaking out on the territory of a State, it may become international (or, depending upon the circumstances, be international alongside an internal armed conflict) if: (i) another State intervenes in that conflict through its troops, or if (ii) some of the participants in the internal armed conflict act on behalf of that other State."[1000]

Nonetheless, the Tadic Chamber declined to articulate any particular standard for what degree of intervention would be sufficient to internationalize a pre-existing NIAC.[1001] Similarly, with regards to military intervention, the ICTY Trial Chamber in the Blaskic Judgment considered that: " Croatia's direct intervention in Bosnia-Herzegovina has ample proof to characterize the conflict as international."[1002] The decision suggests that foreign military intervention that only indirectly affects an independent NIAC is sufficient to consider an armed conflict as an international one.[1003] Notwithstanding, more challenging mixed conflicts arise when multiple foreign states intervene in an armed conflict against or in support to NSAs or governmental forces (with or without the consent of territorial State) under different agendas and strategies, also in the unclear and fragmented relationship between the parties to the conflict. Besides, the transnational threat or operations spill over to neighboring countries (neutral or party to a conflict) in a hybrid manner. The latter can be described as "spill-over", "cross border", or "transnational armed conflict" that also occurs in NIAC not limited to the territory of one State and between a State and NSA that operates from the territory of a third State. These are not legal categories or terms, yet are useful for descriptive purposes.[1004] For example, the Israeli armed conflict in 2006 with Hezbollah as an armed group that meets the requisite level of intensity and organization on the territory of Lebanon. In such case, as Hezbollah does not act on behalf of the Lebanese Government (dismissing the facts of its direct relation with Iran and that Hezbollah's political wing is represented in the Lebanese government), the conflict

[1000] Prosecutor v. Tadic, Decision on the Defense Motion for Interlocutory Appeal on Jurisdiction (hereinafter Tadic Jurisdiction Appeal), 2 October 1995, para. 126.
[1001] Stewart J., Towards a Single Definition of Armed Conflict in International Humanitarian Law: A critique of Internationalized Armed Conflict, IRRC, June 2003, Vol. 85, no. 850, p. 328
[1002] Prosecutor v. Blaskic, IT-95-14, Judgment, 3 March 2000, Declaration of Judge Shahabuddin, paras. 75, 76 and 94. The chamber built its judgment on the fact that: "The Croatian Army's hostilities in the areas outside the conflict zone inevitably also had an impact on the conduct of the conflict in that zone. By engaging the Bosnia-Herzegovina Army in fighting outside the conflict zone, the Croatian army weakened the ability of the Bosnia-Herzegovina army to fight the Croatian Defense Council in central Bosnia." Prosecutor v. Blaskic, Ibid. para 94.
[1003] Stewart J., Ibid. p. 328.
[1004] ICRC, Commentary on the First Geneva Convention, 2016, CA 3, Para. 472. Published online on 22 March 2016, available: https://ihl-databases.icrc.org/ihl/full/GCi-commentary

between the Israeli armed forces and Hezbollah is a NIAC, but as long as Israel conducted operations on the territory of Lebanon without its consent (dismissing the facts that Israel had targeted critical infrastructure in Lebanon such as the Airport, Electric Grids, even the Lebanese armed forces base), it is, therefore, an IAC with Lebanon and NIAC with Hezbollah.[1005] With regards to spill-over of a NIAC, state practice seems to indicate that crossing an international border does not change the non-international character of the armed conflict[1006]. Nevertheless, certain questions may arise with regards to the geographical considerations as to what extent the "Spill-over" can be extended in the territory of another state, multinational forces or intervention of one or more State in NIAC, whether the multifaceted armed conflicts complicate any attempts to successfully attribute a link between actors. In a cyber context, such a scenario is extremely challenging in which a group engages in cyber operations attacks without doing so on behalf of one of the parties to an IAC. Though the ICRC's approach is to consider such attacks as a separate NIAC[1007], some experts in the Tallinn Manual rejected this conclusion as it would prove a difficulty in practice when applying the law of both armed conflicts to the same battlespace.[1008]

Another example of such mixed armed conflict is the ongoing conflict in Syria. In March 2011, anti-government protests broke out in Syria and were influenced by the widespread demonstration during the Arab Spring. The demonstration turned violent and steered to an ongoing armed conflict that lasted for nine years by now with countless fatalities, destruction and created the largest refugee crisis since WWII. The armed violence escalated to a fierce NIAC between Rebels, which split into a myriad of militarized opposition groups, and the

---

[1005] ICRC, Commentary on CA 2, paras 265-273. See also, ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Ibid., p. 10, noting that: "Such a scenario was hardly imaginable when CA 3 was drafted and yet it is submitted that this Article, as well as customary IHL, were the appropriate legal framework for that parallel track, in addition to the application of the law of IAC between the two states."

[1006] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Ibid., pp. 9-10. The ICRC notes that: "It is submitted that the relations between parties whose conflict have spilled over remain at a minimum governed by CA 3 and customary IHL. This position is based on the understanding that the spill over of a NIAC into adjacent territory cannot have the effect of absolving the parties of their IHL obligations simply because an international border has been crossed. The ensuing legal vacuum would deprive of protection both civilians possibly affected by the fighting, as well as persons who fall into enemy hands."

[1007] Melzer N., Interpretive Guidance on the Notion of Direct Participation under International Humanitarian Law, ICRC 2009, p. 24.

[1008] Schmitt M., Classification of Cyber Conflict, Ibid. p. 259. According to Schmitt, the experts who rejected ICRC's position, considered that: "it was more appropriate to ask whether an unambiguous nexus existed between the actions of the group in question and the IAC, rather than any party thereto. For instance, an organized armed group might conduct cyber-attacks against an occupying force because of religious or political opposition to the occupants, not to expel them on behalf of the government. The requisite nexus between the group and the conflict would be their opposition to the occupation. In such case the conflict would remain entirely international irrespective of the lack of relationship between the group and the occupied State." Ibid.

Syrian government forces.[1009] As the conflict turned to NIAC and more armed groups joined the conflict (over 1500 armed groups and militias), the level of hostilities reached an unprecedented level.[1010] Additionally, as the Syrian government started to lose control over its territory, the situation shifted to more violence as armed groups (Iran-backed Shia Militias such as Hezbollah and National Defense forces[1011]) joined the fight alongside the Syrian armed forces against the rebels. The fluidity of the conflict kept evolving and involved foreign interventions from Russia in support of the Syrian regime, and similarly, an Anti-ISIS coalition was initiated to target ISIS fighters in Syria and Iraq. On the other hand, Turkey was also involved in the conflict to block the Kurdish rebels' goal of establishing a viable autonomous Kurdish region across the borders and increased in intensity in 2016. The conflict involves multiple armed groups with different objectives that meet the requirements of intensity and organization, have clashed in numerous events among each other, and with the government forces and its allies. The many-sided clashes do not change the non-international character of the conflict, as parties of the conflict are State and NSAs which is examined as an overall conflict despite the numbers of actors.[1012] Similarly, the Russian intervention was based on the consent of the Syrian regime, therefore such intervention does not internationalize a conflict, because the operations of the intervening state are directed against NSAs with the consent of the territorial state "Syria". However, when it comes to the Turkish operations in Syria or the U.S. airstrikes against ISIS, the question of territorial state consent arises. Some scholars argue that such conflict is a NIAC, as there have been no clashes between the Turkish forces and the Syrian government, and the operations were solely directed against the NSA.[1013] The argument is based on the wording of CA 3 which does not prevent NIAC from straddling more than one State.

Those who oppose considering the conflict between an intervening third state and NSA as IAC, consider that such classification would not only be contrary to the party structure of IAC, but disputed that NSAs would be unable to comply with many of the IAC provisions, and the state would be unwilling to grant NSAs immunities from prosecution granted to prisoners of war in conflicts of this type. The rules of NIAC are precisely designed for conflicts in which one of

[1009] Wallace D., McCarthy A and Reeves SH., Ibid. pp. 561-62. The article provides important historical and contributing factors to the conflict in Syria.
[1010] Blanchard Ch., Armed Conflict in Syria: Overview and U.S. Response, 9 October 2015.
[1011] The BDF and associated pro-government militias reportedly number between 60,000 and 80,000 fighters. See more, Gill T., Classifying the Conflict in Syria, Ibid., pp. 355-56.
[1012] Ibid. p. 375.
[1013] Gill T., Ibid. p. 376.

the parties is NSA.[1014] Nevertheless, this study disagrees with the views that consider operations by the third state against NSA in the territory of another state without its consent are of NIAC nature, based on the fact that it does not involve inter-state conflict or it is directed solely against NSA. While it might be argued not considering these conflicts as IAC is not to encourage NSAs to drag a third state to an ongoing NIAC and by that apply the rules of IAC, however, such arguments are not enough and contradicting. By which the ICJ in the case concerning Armed Activities on the Territory of the Congo case held considering 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, and were directed to securing towns and airports for the reason of its perceived security needs and in support of the parallel activity of those engaged in the civil war.[1015] Also, the UN Commission with regards to the armed conflict in Lebanon 2006 affirmed the hostilities were in fact between the Israeli Defense Forces (IDF) and Hezbollah. However, the fact that the Lebanese armed forces did not take an active part in them, does not deny the character of the conflict as a legally cognizable IAC, nor does it negate that Israel, Lebanon, and Hezbollah were parties to it.[1016] Nonetheless, this study argues that states intervening and conducting operations on the territory of another State without its consent, would also encourage states to conduct more operations as such, and violate the territorial sovereignty and integrity that not only concern Jus ad Bellum, but also the IHL in an ongoing armed conflict.

All in all, the extraterritorial intervention in NIAC is still a matter of debate, the ICRC's proposal, as mentioned before, requiring the law of IAC to be applicable in every case in which a foreign power acts on behalf of one or other of parties, was rejected by experts. However, the author's view is not to include all types of intervention as IAC, but it should still be constructed on a case-by-case analysis. So, with regards to the conflict in Syria, a mixed armed conflict took place as an example of co-existing legal regimes to one battlefield. To draw such a conclusion, it will be required to identify parties to the conflict and their nature, how the foreign intervention is conducted (directed against a state or NSA, with or without consent of territorial

[1014] Lubell N., Extraterritorial Use of Force Against Non-State Actors, Oxford Scholarship Online 2010, Part II, Ch. 14, p. 245.
[1015] ICJ., Armed Activities Case, Ibid, para163.
[1016] Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council Resolution S-2/1, 2006 UN Doc. A/HRC/3/2. Paras 50-62. https://www.un.org/ruleoflaw/blog/document/report-of-the-commission-of-inquiry-on-lebanon-pursuant-to-human-rights-council-resolution-s-21/

state), and other possible factors (intensity, organizational), which is not an easy task in complex armed conflicts, but not impossible.

To sum up, the suggestion of applying IAC rules to cases where NIAC is characterized by foreign military intervention was not accepted, because it will be challenging with NSAs that will try to attract third states to benefit from the application of IACs legal framework, to broaden the rules of protection to the belligerents. However, in cases where the foreign intervention aimed to target NSAs on the territory of another State without its consent, the IAC rules should apply. At the same time, the fragmented application of mixed conflicts is favored by states and opinio Juris, but as explained before, such fragmentation would involve practical and legal difficulties.

Based on the previous analysis, it has been concluded that armed conflicts include violence as a central element, which is achievable through the hybridity of non-kinetic means and irregular forces that can either start a conflict or be influential in an ongoing one. The author agrees with the experts in Tallinn Manual that cyber-attacks alone may constitute an armed conflict depending on the circumstances, mainly physical and property damage. Furthermore, geographical limitations in NIAC do apply in spill-over conflicts under certain circumstances, however, it is not applied in some extraterritorial conflicts. For example, certain ambiguities arise with regards to cyber NSAs in particular when conducting cyber-attacks from the territory of a neutral State against a State that is involved in a NIAC. But it is concluded that the NIAC should not expand to the territory of a neutral state without its consent, due to the fluid nature of contemporary conflicts and the role of NSAs in cyberspace which might lead to a catastrophic global battlefield.

Consequently, the traditional classification of armed conflict is capable of addressing the different scenarios of contemporary conflicts, even those involving cyber-attacks and fragmented actors to a single battlefield. Hence, IHL is highly capable of meeting such challenges, but certain legal issues may arise in a mixed armed conflict regarding the rights and obligations of states and parties to the conflict that have considerable variations under IAC and NIAC. Although it is agreed that both types of conflicts can co-exist, hybrid actors can skillfully combine and split their hostilities accordingly based on the regime that offers them broader protection. At the same time, the co-existence of armed conflict means applying different legal regimes (CA 3 and CA 2 of the GCs) to distinct but connected armed conflicts occurring simultaneously in the same territory. Therefore, eradicating the distinction between

CA 2 and CA 3 of the GCs of 1949 in certain matters would be an important step towards avoiding any future challenges to the classification of an armed conflict and the principles of humanity that IHL is based on. This suggestion has moral and legal reasons, as unequal humane treatment should not be acceptable, regardless of whether the conflict is of international or non-international nature.[1017] While such eliminations were acknowledged by ICRC and ICTY to be potentially occurring based on the role of customary IHL and opinio Juris, this distinction has not been abolished in law. For example, the rights of injured people in NIACs are only recognized once the deprivation has occurred. Similarly, the detention in NIAC by which lawful participants in such conflicts are ordinary prisoners once detained subject to national and human rights laws. While lawful combatants in an IAC once detained are considered "POW" under a certain level of protection guaranteed by Article 4 of the GC III afforded to captured combatants which are regarded as a measure of security and not of punishment.[1018]

Such conduct in contemporary hybrid warfare can be very crucial to humane treatment. For example, Ukraine condemned Russia for its belligerent occupation of Crimea and violations of its sovereignty in the Donbas. But always referred to the conflict in Eastern Ukraine as "anti-terrorist operations", denying the existence of an armed conflict in that region. Therefore, if Ukraine detained a member of an armed group in Eastern Ukraine, the treatment and rights of this member will be different than if he was detained in Crimea.[1019] While IHL applicability depends on the identification of the parties to a conflict to classify it and apply the rules relating to it, this might be confusing in cyberspace, especially that a legitimate target under IHL according to Article 4(2) of the GC III, must be commanded by a person responsible for their subordinates, have fixed distinctive sign, carry arms openly and conduct operations per the laws and customs of war. Yet, such requirements are indeterminate in cyberspace, as most cyber hackers operate anonymously and their direct participation in NIAC can be hardly detected. Nonetheless, participants in hostilities who do not satisfy the criteria under the

[1017] State practice confirms that lawful participants in NIACs should be entitled to POW status. In 1984, the Congolese Prime Minister stated: "For humanitarian reasons, and with a view to reassuring the civilian population which might fear that it is in danger, the Congolese Government suggest that ICRC observers come to check on the extent to which the GCs are being respected, particularly in the matter of the treatment of prisoners." See, Henckaerts J., Study on Customary International Humanitarian Law, Ibid., pp. 175-181.

[1018] GC III, Article 4 (A)(1) that limits its applicability to "Members of the armed forces of a Party to the conflicts well as members of militias or volunteer corps forming part of such armed forces."

[1019] Kahn J., Hybrid Conflict and Prisoners of War: The Case of Ukraine (2018). Lieber Institute for Law and Land Warfare Book Series - Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare, ed. by Christopher M. Ford and Winston S. Williams, Oxford University Press, 2018, Forthcoming, SMU Dedman School of Law Legal Studies Research Paper No. 381, p. 17.

abovementioned Article are considered to be civilians directly participating in hostilities under GC IV. In mixed conflicts that also raises some questions about the equal level of humane treatment to the participants in the hostilities whether civilians or combatants. The reason why it is suggested is that the elimination of the gap between CA 2 and CA 3 would have a more humane impact on the conflict. It would be fairer if the humane treatment accorded to a person be based on the status of the persons themselves, rather than on the status of the conflict. A subject that requires further examination and prospects for future academic research.

3. Application of Principle of Distinction to Hybrid Warfare (Cyber Operations and Hybrid NSAs)

The IHL is characterized to serve humanity in its most perilous situations, by which its main objective in an armed conflict, whether IAC or NIAC, is to outline certain limitations, restrictions, and prohibitions on the parties involved to limit the suffering and destruction produced by a conflict. According to Article 22 of the Hague Convention, "the rights of belligerents to adopt means of injuring the enemy is not unlimited."[1020] Such limitations to the use of force in armed conflicts are focused on sparing those who do not or no longer directly participate in hostilities, restricting it to the amount necessary to achieve the aim of the conflict that can only be to weaken the military potential of the enemy. Nevertheless, IHL faces challenges in stationing such limitations to situations that are not easily defined in concrete terms. David Eric perfectly underlines that "depending on the situation, the same act can be lawful or unlawful, not merely unlawful but a criminal offense, or neither lawful not unlawful."[1021] Yet IHL does not address the legality of an armed conflict, and treats all parties to the conflict equally regardless of the reason or its lawfulness, but rather reflects a constant balance between the military necessity arising in a state of war and the need for humanitarian protection. Such balance necessitates certain principles that must be respected by parties of an armed conflict and considered before any hostilities, development of any weapon, and employment of methods that contradicts with them. These principles that IHL is founded upon and explained previously, help to interpret the law when the legal issues are unclear or

---

[1020] Convention IV respecting the Laws and Customs of War on Land and its annex: Regulating concerning the Laws and Customs of War on Land (The Hague Convention 1907), The Hague, 18 October 1907, Section II, Article 22. In addition, with regards to means of injuring the enemy, sieges and bombardments, Article 23 of the Hague Convention forbids the following:
"1-To employ poison or poisoned weapons;
2-To kill or wound treacherously individuals belonging to the hostile nation or army;
3-To kill or wound an enemy who, having laid down his arms, or having no longer means of defense, has surrendered at discretion;
4-To declare that no quarter will be given;
5-To employ arms, projectiles, or material calculated to cause unnecessary suffering;
6-To make improper use of a flag of truce, of the national flag or of the military insignia and uniform of the enemy, as well as the distinctive badges of the Geneva Convention;
7-To destroy or seize the enemy's property, unless such destruction or seizure be imperatively demanded by the necessities of war;
8-To declare abolished, suspended, or inadmissible in a court of law the rights and actions of the nationals of the hostile party. A belligerent is likewise forbidden to compel the nationals of the hostile party to take part in the operations of war directed against their own country, even if they were in the belligerent's service before the commencement of the war."

[1021] David E., Principes de Droit des Conflits Armes (The Principles of the Law of Armed Conflict), Brussels 2002, 3rd ed. pp 921-922.

controversial. So, the balance between the principles and interest shifts depending on the situation. For example, military necessity may limit the notion of humanity to allow destruction, while in other situations that involve the protection of the wounded and sick, the principle of humanity prevails.[1022] So, armed forces are under an obligation to apply the basic principles of IHL, to ensure that the conduct of hostilities involves the least possible injury and damage that are militarily necessary to subdue the enemy forces.[1023]

The basic principles of IHL play an important role in armed conflicts and are more vital, especially in the rise of NIACs that are more of urban nature that replaced conventional warfare by conflicts, in which there is no clear-cut distinction between soldiers and civilians, and between organized violence, terror, crime and armed conflict.[1024] The hybrid nature of contemporary conflicts demoralizes and undermines the principles of humanity by operations that deliberately place irregular troops within civilian areas, including civilians in cyber operations directly by encouraging and equipping them with necessary technology by conveying their status to cyber hackers with relative impunity or use the civilian cyberinfrastructure to launch such attacks remotely by which civilian objects will be lawful targets. For example, terrorist organizations have manipulated the humanitarian laws for their military advantage, such maneuvering was employed by the Taliban which developed tactics by boomeranging NATO's campaign in the form of malicious lawfare, and regularly placed civilians near their positions.[1025]

For this section, the study will examine and review the principle of distinction in IHL in the context of hybrid activities, mainly cyber-attacks and NSAs, in contemporary conflicts, and the role in addressing the theoretical and practical consequences of certain characteristics of HW. This section will summarize the legal problems arising from cyber NSAs, especially regarding the distinction between combatants/military objectives, on one side, and the protection of civilians and their objects, on the other. In armed conflicts, categorizing the actors taking a role in hostilities is confusing when there is a mixture of actors. This creates so-called "hybrid adversaries" that complicate the classical interpretation analysis and prediction of the

[1022] Basic Principles of IHL, Diakonia International Humanitarian Law Centre; available at: https://www.diakonia.se/en/IHL/The-Law/International-Humanitarian-Law-1/Introduction-to-IHL/Principles-of-International-Law/

[1023] Vincze V., Taming the Untamable: The Role of Military Necessity in Constraining Violence, ELTE Law Journal 2013, p. 94.

[1024] Hoffman F., Conflict in the 21st Century: The Rise of Hybrid Wars, Ibid. p. 11.

[1025] Bachmann S., and Mosquera A., Lawfare in Hybrid Wars: The 21st Century Warfare, Ibid., p.72-73.

conflictual situation. Limiting the examination to one principle does not mean that other principles are less important or do not face challenges, however, to back up all the principles would require a good deal of work that could overstretch our thesis.

Additionally, the principle of distinction is of great importance to the complexity of HW in particular identifying the increasingly disturbing occurrence of belligerent cyber incidents, such as the inclusion of cyber means and methods in armed conflicts that force us to pay greater attention to the application of the principle of distinction to modern conflicts. And as it was analyzed earlier in the thesis, HW as an emerging form of warfare that combines conventional and unconventional threats blurs the line of distinction between civilian and combatant by deliberately placing irregular troops within civilian areas, or using civilian infrastructure through cyber means to conduct attacks in cyberspace. So, discussions will narrow down to an example of how cyber-attacks in current conflicts can be challenging with regards to the principle of distinction when fused with civilian objects and participation. As explained before, new technologies used in a hybrid manner through irregular NSAs or states must comply with the principles and rules of IHL[1026], nonetheless, the study argues that certain aspects that are related to the nature of cyberspace and its dual-use, are quite significant and relevant to hybrid warfare.

3.1. Principle of Distinction

The distinction in IHL is a cardinal principle that draws a distinguishing line and limitations on who and what is a legitimate target in an armed conflict, and what protections are entitled to persons and objects that must be immune from attacks if not directly participating or involved in the hostilities. The normative justifications for the principle of distinction are based on just war doctrine and suggested that civilians and combatants should be treated differently on the battlefield.[1027] The principle is the cornerstone of IHL by which Article 48 of the AP I

[1026] The ICJ Advisory Opinion on the Legality of the Threat or use of Nuclear Weapons established that principles and rules of humanitarian law applicable in armed conflict apply "to all forms of warfare and to all kinds of weapons, including those of the future." ICJ, Nuclear Weapons Advisory Opinion, Ibid. para 86. In addition, Article 49(3) of AP I established that the applicability of the provision of this Protocol apply to "any land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects on land. They further apply to all attacks from the sea or from the air against objectives on land but do not otherwise affect the rules of international law applicable in armed conflict at sea or in the air."

[1027] Walzer M., Just and Unjust Wars, 4ht ed., 2006, pp. 144-46. According to Walzer "Combatants are a class of people who are set apart from the world of peaceful activity; they are trained to fight, provided with weapons, required to fight on command. It is the enterprise of their class, and this fact radically distinguishes the individual soldier from the civilians he leaves behind." Walzer M., Ibid. p. 144.

of the GCs 1949 states that "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."[1028] Similarly, Article 52 of the AP I states that "civilian objects shall not be the object of attack or reprisals. Civilian objects are all objects which are not military objectives."[1029] Therefore, avoiding or minimizing incidental civilian harm during an armed conflict is a legal obligation under IHL.

Also, The ICJ in the Nuclear Weapons advisory opinion indicated that "a large number of customary rules have been developed by the practice of states and are an integral part of international law. And one should provide that the 'Hague law' fixed the rights and duties of belligerents in their conduct of operations and limited the choice of methods and means of injuring the enemy in an IAC. Also, the 'Geneva Law' provided safeguards for disabled armed forces personnel and persons not taking part in the hostilities."[1030] State practice established this rule as a norm of customary international law applicable in both IAC and NIACs and is contained in many military manuals. For example, Sweden's IHL manual of 1991, referring to Article 52 of AP I, states: "The basic rule in Article 52 is that civilian objects and civilian property may not constitute objectives for attack or be subjected to reprisals. The article does not represent any new thinking, but is rather a clarification of humanitarian principles established in older conventions."[1031] Therefore, any direct attack against a civilian or civilian object is not only a violation of IHL but also a grave breach that can be categorized as a war crime.

Instead, technological development and the role of cyber operations raise the question about the indiscriminate nature of such new weapons. IHL prohibits indiscriminate attacks which are not directed at a specific military objective or employ methods and means of combat which cannot be directed at a specific military objective or cannot be limited, as they are in nature capable of striking military and civilian objects without distinction.[1032] This rule is being

[1028] AP I, Ibid., Article 48.
[1029] Ibid. Article 52 (1). See also, Article 52(2) about Military Objectives, Ibid.
[1030] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, Ibid., para 75.
[1031] Sweden, International Humanitarian Law in Armed Conflicts, with reference to the Swedish Total Defense System, Swedish Ministry of Defense, January 1991, section 3.2.1.5, p. 53.
[1032] AP I, Ibid. Article 51(4).

accepted as a norm of customary international law even from non-state parties to the protocol and also contained in amended AP II on certain conventional weapons.[1033]

In contemporary conflicts, the principle of distinction is highly relevant and raises tangible legal questions about the nature of conflicts that embraces new weapons originally of civilian nature, and non-state armed groups evolved to use kinetic and non-kinetic means in an armed conflict, and by blending their civilian and military identity. The principle of distinction does not only exclude deliberate attacks against civilians, but also indiscriminate attacks without a target.[1034] The ICRC has confirmed the applicability of IHL to cyber warfare in armed conflicts and asserted that applying IHL to cyberspace does not legitimize cyber warfare, just as it does not legitimize any other form of warfare. Cyber-attacks have the technological capability to be as precise as necessary and can offer alternatives that other means or methods of warfare do not.[1035] Moreover, the ICRC considered that cyber operations enable parties to an armed conflict to achieve military aims without harming civilians or causing physical damage to civilian infrastructure. Nevertheless, the frequency of cyber-attacks against industrial control systems used in critical civilian infrastructure has increased, carrying potential risks to disrupt the provision of essential services to the civilian population, therefore there is a higher possibility that many undetected actors will be qualified of attacking civilian control systems.[1036]

In theory, the distinction in armed conflict is based on protecting those who are not directly participating in hostilities from being targeted and prohibiting indiscriminate weapons. However, cyber adversaries tend to disguise their involvement in an armed conflict by hiding their responsibility through technical means and perpetrating the attacks through NSAs with ambiguous relationships to State agencies, and through hacktivists or private contractors, which make the internet the ideal platform for plausible deniability. These actors range from individual hackers, criminal gangs, organized armed groups, and states that hamper the

[1033] Protocol II on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996, Article 3(3) "it is prohibited in all circumstances to use any min, booby trap or other device which is designed or of a nature to cause superfluous injury or unnecessary suffering."
[1034] AP I, Ibid., Articles 48, 51,52.
[1035] ICRC on the discriminate nature of cyber-attacks noted that "Many of the recent cyber-attacks that have been reported in public sources appear to have been rather "discriminate" from a technical point of view. The have been designed to target and harm specific objects and have not spread or caused harm indiscriminately." See, ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, ICRC Position Paper, November 2019, p. 5.
[1036] Ibid.

possibility to identify actors who violate IHL in cyberspace and hold them responsible.[1037] And finally, the inter-dependent nature of the cyber domain may result in unintended consequences whereby civilians or non-military infrastructure are affected, as such attacks may proliferate beyond that which is anticipated or planned, causing cascading effects on non-legitimate targets.

The IHL through the work of ICRC, with regards to new means and methods of warfare, guides the international community towards either prohibiting the use of certain weapons of indiscriminate nature or restricting their usage in compliance with its basic principles. Nonetheless, IHL does not legitimize cyber warfare but requires states to take all necessary measures on how IHL applies in cyberspace, including on how it protects civilian infrastructure from being disabled through cyber means and how it protects civilian data.[1038]

This section will be examining the impact of manipulating civilian infrastructure in hybrid cyber-attacks, and the serious adverse consequences of possible retaliation to such attacks, by which hybrid operations are successful because of the confusion they create to opponents, offensively and defensively. In offense, using cyberspace to launch attacks during an armed conflict through irregular troops, either remotely or within the territory of the victim State, will require the latter to respond without violating the basic principle of distinction between civilians and military objectives, a response that does not come without risks due to the unique interconnectivity and ambiguity of virtual space. On the other hand, it allows the hybrid adversary to hide their real identity, in a defensive attempt, behind the civilian nature of the operation. In addition, blurring the distinction between civilians and combatants through cyber hacktivists and private contractors has a huge impact on the determination of an individual's status under protections and rights afforded by IHL rules, particularly with regards to the civilian's direct participation in cyber hostilities. That will require an assessment of the Interpretive Guidance of Direct participation in hostilities introduced by the ICRC in 2009.

[1037] Olejnik L and Gisel L., Ibid. p. 6.
[1038] Durham H, Cyber Operations During Armed Conflict: 7 Essential Law and Policy Questions, ICRC Humanitarian and Law Policy, March 2020. Available at: https://blogs.icrc.org/law-and-policy/2020/03/26/cyber-armed-conflict-7-law-policy-questions/

3.1.1. Civilian Objects and Military Objectives in Hybrid Context

Albeit the weapons or methods used during an armed conflict, the challenges of distinguishing between civil objects and military objectives always appear. While, the premise remains that all principles of IHL apply to any kind of operations during an armed conflict, including those of cyber nature, however, in contemporary hybrid warfare the distinction principle is more complex through the employment of cyber technologies in NIACs by NSAs with ambiguous identity. As explained before, IHL applicability requires states and conflict parties to take all necessary measures that the development and use of weapons to comply with the IHL principles. But, the increased reliance on civilian and commercial facilities blurs the distinction line between civilian and military objectives, also between civilians and combatants.

To illustrate, the military objective requires two criteria, provided by Article 52(1)(2) of the AP I, that need to be met cumulatively. First, is the "nature, location, purpose or use" of the object that should be situated in an area that is a legitimate target, the current function of the object, the adversaries intended future use, and located in an area that is a legitimate target.[1039] Second, the object's destruction, capture, or neutralization has to offer a definite military advantage for the attacking side.[1040] By way of example, during the armed conflict in Ukraine in 2014, the governmental forces and Russia-backed militants have deployed military forces in and near schools without fully occupying it as it would turn into a legitimate military targets. In such cases, collecting data and evidence about the school's location, how long was it used by the military, and for what purpose, is very difficult.[1041] Similarly, the dual-use targets (objects that serve both civilian and military purposes) such as power stations, telecommunications, and civilian infrastructure, used by military forces in times of war, complicate the application of the principle of distinction.[1042] In this regard, the experts on the Tallinn Manual 2.0 opined that "an attacker is required to consider expected harm to clearly

[1039] AP. I, Ibid. Article 52 (1). See also, Customary International Humanitarian Law, Rule 7 "State Practice establishes this rule as a norm of customary international law applicable in both IACs and NIACs.", Ibid., p. 26-27.
[1040] Ibid. Article 52(2). Moreover, it is important to highlight that although the definition of military objectives was not included in AP II, it has been incorporated into treaty law applicable in NIACs, namely amended Protocol II to the Convention on Certain Conventional Weapons ("Article 2(6)" Ibid. para 321), and the Second Protocol to the Hague Convention for the Protection of Cultural Property ("Article 1(f)", para. 322).
[1041] Human Rights Watch Report, Studying Under Fire: Attacks on Schools, Military Use of Schools during the Armed Conflict in Eastern Ukraine, February 11, 2016. Available at: https://www.hrw.org/report/2016/02/11/studying-under-fire/attacks-schools-military-use-schools-during-armed-conflict#
[1042] Sassoli M., Legitimate Targets of Attacks under International Humanitarian Law, Harvard Program on Humanitarian Policy and Conflict Research, June 2003, p. 7.

distinguish civilian components of the military objective, and if the civilian component is not distinguishable, then the entire object qualifies as a dual-use military objective."[1043] Furthermore, attacks against a civilian object constitute a war crime under the Statute of the ICC as such an attack is not imperatively demanded by the necessities of the conflict[1044]. So, launching cyber-attacks from a civilian infrastructure creates the confusion desired by hybrid adversaries to the targeted state, by which any response on the cyberinfrastructure can constitute a war crime if it was deemed to be civilian and led to the destruction or physical damages.

Consequently, the ambiguity of cyber-attacks is two-sided, while technically it is a discriminate weapon capable of targeting precisely, its ability to operate through civilian infrastructure, and undetectable in most of cases, blends the military and civilian objects raising legal and humanitarian concerns. Some might argue that when attacks are launched by civilians and considered directly participating in hostilities, it makes them legitimate targets, however, the infrastructure used to launch such attacks might be still civilian in nature. Nonetheless, several states have stressed that the rule contained in Article 52(2) of AP I, does not deal with incidental damage resulting from attacks directed against military objectives, assuming that such effects are not unlawful as long as it is not excessive.[1045] Such reservations are relevant for states when attacking dual-use objects, as it gives a certain level of amnesty towards incidental damages. Similarly, states are required to take all feasible precautionary measures even when an attack directed at a military objective is not expected to have excessive effects on the civilian population.[1046]

[1043] Tallinn Manual 2.0, Ibid. Rule 101, para 3.

[1044] Rule 7, Customary International Humanitarian Law, Ibid. p. 27. According to Rule 7, the Statute of ICC does not explicitly define attacks on civilian objects as a war crime in NIACs, but define the destruction of the property of an adversary as a war crime unless such destruction be imperatively demanded by the necessities of the conflict. See, ICC Statute, Ibid., Article 8(2)(e), p. xii.

[1045] Six States (Australia, Canada, France, Italy, New Zealand and the United Kingdom) specified that "the first sentence of paragraph 2 in Article 52 AP I is not intended to deal with the question of incidental or collateral damage resulting from an attack directed against a military objective." See, Gaudreau J., the Reservations to the Protocols Additional to the Geneva Conventions for the Protection of War Victims, International Review of the Red Cross, no. 849, March 2003, p.159.

[1046] Article 57(1) of AP I, Ibid. we would like to note that, upon the ratification of AP I, the United Kingdom confirmed that commanders have the obligation to cancel or suspend an attack if it becomes clear that the target is nota. Military objective or that its attack is likely to cause excessive civilian damage to the effect that this obligation only applied to "those who have the authority and practical possibility to cancel or suspend the attack." See, Gaudreau J., Ibid. p. 158. Also, Customary International Humanitarian Law, Ibid. Rule 15 on Principles of Precautions in Attack.

Cyber-attacks will dominate future conflicts that are more of hybrid nature and safeguarding essential civilian infrastructure will be under more risks in an interconnected cyberinfrastructure especially since the principle of distinction appears too ambiguous in cyberwarfare. AP I prohibits a defender from using the civilian population or individual civilians to render certain points or areas immune from military operations.[1047] For instance, in a cyber context, commanders are under vast responsibility to assess and determine the precise use of an object. Such assessment was more challenged by the fact that Article 52 (2) of AP I, states that "in case of doubt whether an object which is normally dedicated to civilian purposes such as a place of worship, a house or other dwelling or a school, is being used to make an effective contribution to military action, it shall be presumed not to be so used."[1048] The latter language shifts the responsibility, to precisely determine the use of an object, from the defender as the party controlling it to the attacker as a party lacking such control and facts.[1049] So, in practice, an attacker on cyber-infrastructure will be responsible for determining whether the cyber object is military or civilian without having the precise data or control over the object.

Another challenge is from the term "purpose" which denotes the intended future use of the object, rather than that cyberinfrastructure to be used to be a lawful military object.[1050] For example, if there is reliable intelligence that a civilian server farm will soon be to store military data, the server farm is a military objective that may be attacked even before data storage begins.[1051] Therefore, the "Purpose" criteria will be satisfied once a State has reason to believe that an adversary intends to use the cyberinfrastructure for military purposes. While this does not present particular problems in the cyber setting however when an object is used for both civilian and military purposes, the civilian aspect of the target will be at risk and relevant to the requirements of proportionality and precautions in attack, but according to Schmitt "civilian use does not diminish its qualification as a military objective."[1052] While there are no clear

[1047] AP I, Article 51 (7) of AP I, Ibid. "the presence or movements of the civilian population or individual civilians shall not be used to render certain points or areas immune from military operations, in particular in attempts to shield military objectives from attacks or to shield, favor or impeded military operations. The Parties to the conflict shall not direct the movement of the civilian population or individual civilians in order to attempt to shield military objectives from attacks or to shield military operations." See also, Article 58 (2)(3) of AP I "Parties to the conflict shall, avoid locating military objectives within or near densely populated areas; 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."
[1048] AP I, Ibid. Article 52(2).
[1049] United States/United Kingdom, Report on the Conduct of the Persian Gulf War, ICRC Casebook. Available at: https://casebook.icrc.org/case-study/united-statesunited-kingdom-report-conduct-persian-gulf-war
[1050] Tallinn Manual 2.0, Ibid. at 439
[1051] Schmitt M., The Law of Cyber Targeting, Ibid. p. 107.
[1052] Schmitt M., The Law of Cyber Targeting, Ibid. p. 107.

standards provided by IHL or states as to what would be a nature of objects that cyber-attacks can target without violating the principle of distinction, the ambiguity of cyber-attacks and its interconnected nature of networks, yields a clear line of distinction and will allow hybrid actors in contemporary conflicts to continue manipulating the law and leaves civilians at risk due to the lack of clarity as to which cyber operations qualify as an attack.[1053] This also highlights the complexity of considering the status of data as an object, that is unsettled so far. For example, the Tallinn Manual considered that data should not be considered an object[1054], and concluded that data neither falls within the "ordinary meaning"[1055] of the term "object" since it is intangible nor comports with the explanation of it offered in the ICRC APs 1987 commentary.[1056] Though the latter subject will require further research and examination, however, it reflects the disruptive nature of cyber operations to civilian protection.

The GCs define military targets as objects of an effective contribution to military action[1057], by contrast, define civilian targets as objects "that offer no military advantages"[1058] So. This study concludes that cyber operations are used by hybrid actors as means to afoul the principle of distinction, in particular through NSAs that can conduct operations among civilians and through civilian infrastructure. Also, cyber operations by NSAs create a grey legal zone when civilian objects are considered military objects. Such challenges flourish when commanders responsible for taking countermeasures against a cyber object, are required to assess whether the object is civilian or a lawful target, given that the nature and characteristics of cyber operations will render the demanding degree of certainty an attacker is required to fulfill. Therefore, a clear definition of dual-use objects under the principle of distinction must be settled. Moreover, IHL experts consider that any military use of a civilian object, including cyberinfrastructure renders the object a military objective. This study agrees with the ICRC's

[1053] Schmitt M., Wired Warfare 3.0.: Protecting the Civilian Population during Cyber Operations, International Review of the Red Cross, 2019, Vol. 1010, p. 353.
[1054] Tallinn Manual 2.0., Ibid. at 875.
[1055] United Nations Convention on the Law of Treaties, signed at Vienna 23 May 1969 (entered into force 27th of January 1980), Section 2 on Application of Treaties, Article 3(1) "A treaty shall be interpreted in good faith in accordance with the ordinary meaning to be given to the terms of the treaty in their context and in the light of its object and purpose".
[1056] Sandoz Y., Swinarski CH. And Zimmerman B. (eds), Commentary on the Additional Protocols, ICRC, Geneva 1987, paras 2007-2008. "The English text uses the word 'objects', which means 'something places before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing.' So, object must mean something tangible and visible." According to Schmitt "it must be acknowledged that the context in which this explanation was offered is not directly applicable, but the Tallinn Manual experts nevertheless found it helpful in their deliberations." See, Schmitt M., Wired Warfare 3.0. p. 341.
[1057] AP I. Ibid, Article 52(2)
[1058] Ibid., Article 52(3).

position on this matter considering that a strict application of this understanding could lead to the conclusion that many objects forming part of the cyberspace infrastructure would constitute military objectives and would not be protected against attack, whether cyber or kinetic. This would be a matter of serious concern because of the ensuing impact that such a loss of protection could have in terms of disruption of the ever-increasing concomitant civilian usage of cyberspace.[1059] Nonetheless, IHL experts and states must establish a high threshold that limits the extent to which the "purpose test" is currently established under the principle of distinction. Such threshold must offer maximum protection to civilians and their objects and can extend to essential civilian data, such as medical data, deleting or tampering with such data could cause more harm to civilians than the destruction of physical objects. However, protection of data is outside the scope of our thesis as the focus will be on the operations that qualify as attacks under IHL that are designed or expected to cause physical effects.

3.1.2. Civilians and Combatants

HW that involves multiple actors (state and NSAs), as well as multiple means (military and non-military), have a direct impact on the civilian population that are either targeted, recruited, manipulated, employed indirectly, or used as human shields. As mentioned before, the modalities of conflicts have changed, and hybrid adversaries tend to blur the line between civilian and combatant status to secure a military advantage over the opponent. For example, many of those engaged in hostilities are not traditional uniformed combatants, but instead members of organized armed groups or civilians participating in hostilities who do not hold combatant status. Nevertheless, civilians according to IHL, are persons who are not members of the armed forces, and the civilian population comprises all persons who are civilians.[1060] The GCs refrain from giving a definitive definition to exclude certain civilians who fall in-between categories. However, unlike combatants, civilian status exists in NIACs as well as in IACs.[1061] Yet, according to Michael Schmitt "civilian's activities alone cannot constitute a NIAC, for such a conflict cannot exist without an organized armed group, on at least one side of the conflict."[1062]

[1059] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Geneva, October 2015, p. 42. Available at: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts

[1060] Customary International Humanitarian Law, Ibid. Rule 5.

[1061] AP. II, Ibid., Article 13(3).

[1062] Schmitt M., The Status of Opposition Fighters in a Non-International Armed Conflict, In Non-International Armed Conflict in the Twenty-First Century, U.S. Naval War College International Law Studies, 2012, Vol. 88, p. 119.

On the other hand, "Combatants" are described as those persons with a right to directly participate in hostilities between states.[1063] The GC III is more explicit in defining combatants as members of the armed forces of a party to the conflict.[1064] It covers members of the militia, volunteer corps, and organized resistance movements that are under responsible command with distinctive signs recognizable at a distance, carry their arms openly, and conduct operations under the law of armed conflict.[1065] Also, combatants include members of a regular armed force attributed to a government not recognized by the detaining power and those who form a *levee en masse*.[1066] Therefore, it is concluded that the distinction between military and civilian must be recognized by both sides of a conflict. Furthermore, the distinction provisions are universally applicable obligations under customary international law, as well as in military manuals of numerous armed forces. For example, the U.S. Law of War Manual states that "Distinction requires parties to a conflict to discriminate in conducting attacks against the enemy. On one hand, consistent with military necessity, parties may make enemy combatants and other military objectives the object of attack. On the other hand, consistent with humanity, parties may not make the civilian population and other protected persons and objects the object of attack."[1067] In this regard, Article 4 of the AP III to the GCs states that "in case of doubt whether a person is a civilian, that person shall be considered to be a civilian."[1068]

The classification of an armed conflict also plays a role in defining the parties and their legal status, and in the same manner parties to a conflict can also classify a conflict. The two-sided relation has been manipulated by hybrid adversaries that cloud both the classification of a conflict and the distinction between its parties. However, that does not mean that such confusion is novel, as the principle of distinction has always been a challenging topic in conflicts, particularly after the introduction of terms such as "fighters", "terrorists" and "Private

[1063] Ibid. Rule 3" All members of the armed forces of a party to the conflict are combatants, except medical and religious personnel." See, also, AP I., Ibid. Article 43(2).
[1064] Geneva Convention III, Ibid. Article 4.
[1065] Ibid. Article 4(2).
[1066] GC III, Ibid. Article 4(A)(6).
[1067] Office of the General Counsel, U.S. Department of Defense, Law of War Manual 63, December 2016. Section 2.5.2, p. 63. See also, the U.K. Manual of the Law of Armed Conflict "Since military operations are to be conducted only against the enemy's armed forces and military objectives, there must be a clear distinction between the armed forces and civilians, or between combatants and non-combatants, and between objects that might legitimately be attacked and those that are protected from attack. United Kingdome Ministry of Defense, the Manual of the aw of Armed Conflict, 2004, section 2.5.
[1068] GC, AP III, Ibid. Article 4.

Security contractors"[1069]. Nonetheless, the line of distinction according to the GCs must be respected despite any practical difficulties, and the non-compliance does not mean that applicable laws are not sufficient, but rather not respected. However, contemporary conflicts that involve cyber-attacks, and the resurgence of urban warfare that occurs in civilian spaces and amongst the people, require a re-assessment of the principle of distinction, particularly in civilian participation in hostilities. Moreover, uncertainties in defining a combatant, civilian, or direct participant in hostilities under the applicable laws, particularly GCs, have encouraged states and NSAs to manipulate this legal regime.

The rules of the GCs and the APs dealing with the conduct of hostilities remain as relevant in conflicts today as they were before. Yet, the challenges IHL currently faced have more to do with respect, the application, and sometimes also the interpretation of certain rules in specific situations than with the existing law itself. This is why it is of utmost importance to clarify certain notions of IHL. That is to say, this section will focus on cyber operations that involve civilians, especially those who are directly participating in hostilities, and will highlight the challenges imposed by blurring the line of distinction between civilians and combatants that continues to be fluid and fragile in practice. Also, direct DPH in the physical world would be clear though with certain challenges. However, DPH in cyberspace imposes more challenges that are believed to be unsettled and require further attention due to the complex nature of cyberspace.

i- Blurring the Line of Distinction in Cyber Context

While kinetic warfare takes place in real space that is tangible and fixed, cyber warfare takes place in a virtual environment that is accessible regardless of geographic location[1070]. It is a domain that exists along with but apart from the physical world.[1071] Such virtual warfare world requires virtual combatants and actors that are different than kinetic combatants that are required to distinguish themselves from the civilian population while they are engaged in an attack or a military operation preparatory to an attack.[1072] This rule lies at the core of IHL's

[1069] According to Nils Melzer "organized armed violence failing to qualify as an IAC or NIAC remains an issue of law enforcement, whether the perpetrators are viewed as rioters, terrorists, pirates, gangsters, hostage-takers or other organized criminals." See, Melzer N., Interpretive Guidance on the Notion of Direct participation in Hostilities under International Humanitarian Law, ICRC, Geneva 2009, p. 24.
[1070] Brenner S. and Clarke L., Civilians in Cyberwarfare: Conscripts, Vanderbilt Journal of Transnational Law, 2010, Vol. 43, p. 1027.
[1071] Brenner S., Is there such a Thing as "Virtual Crime"? California Criminal Law Review, 2001, p. 11
[1072] Customary International Humanitarian Law, Ibid. Rule 106.

seminal goal of protecting innocent civilians and persons who are hors de combat.[1073] Even in traditional conflicts, distinguishing between combatants with distinct uniforms and civilians not venturing near the battlefield, was also a challenge. For example, during Operation Iraqi Freedom[1074], Iraqi insurgents commonly wore civilian clothing when approaching American and British forces to get closer without seeming to present a threat.[1075] However, in contemporary hybrid warfare of cyber dimensions, greater efforts are demanded to determine who is in the zone of combat operations.[1076] Especially since most contemporary conflicts are taking place in an urbanized environment of asymmetric nature. As such asymmetry grows, "the disadvantaged party has an incentive to blur the distinction between its forces and the civilian population in the hope that this will deter the other side from attack."[1077] While some scholars and governments consider that persons belonging to an armed group failing to distinguish themselves from the civilian population maybe be targeted as a legitimate target, when and for such times as they directly participate in hostilities. The difficulty of identifying persons in cyberspace puts other civilians at risk.[1078] Generally, members of an organized armed group are legitimate targets during an armed conflict based on their status, even if they dress as civilians. In this regard, GC requires for promoting the protection of the civilian population from the effects of hostilities, that combatants are obliged to distinguish themselves from the civilian population while engaged in an attack or a military operation preparatory to an attack. However, in situations where combatants cannot distinguish themselves from civilians, they shall retain their combatant status provided that in such situations they carry arms openly.[1079]

Moreover, as explained before, GC III required individuals to meet four conditions to be considered lawful combatant "command by the person responsible for his subordinates; having fixed, distinctive sign recognizable at distance; carrying arms openly; and conducting operations under IHL rules."[1080] Therefore, any combatant that does not match all four

[1073] Blank L., Taking Distinction to the Next Level: Accountability for Fighters' Failure to Distinguish themselves from Civilians, Valparaiso University Law Review, 2012, Vol 46, no. 3, p. 770.
[1074] The official U.S. military name for the war between the U.S. and its allies on one hand, and Saddam Hussein's regime and later various insurgent groups, on the other hand.
[1075] Ibid. p 776.
[1076] Ibid. p 774.
[1077] Schmitt M., The Impact of High Tech and Law Tech Warfare on Distinction, in International Humanitarian Law and the 21st Century's Conflicts: Changes and Challenges, 2005, pp. 169-178
[1078] ICRC casebook on the Definition of the Civilian population, Ibid. available at: https://casebook.icrc.org/law/conduct-hostilities#ii_6_c
[1079] AP I, Ibid. Article 44(3).
[1080] GC III, Ibid. Article 4.

conditions set before is considered an "unlawful" combatant, so is not entitled to claim the rights granted to prisoners of war. Members of armed forces who conduct cyber operations are combatants and always targetable (unless hors de combat)[1081]. Nonetheless, the rules regarding when civilians may be targeted are more complex. So states must ensure that military cyber operations are conducted with the same degree of assurance as conventional military operations, and avoid blurring the functions of the organizations involved in the conduct of state-run cyber operations so it would not jeopardize the protection of civilian entities during an armed conflict.

On the other hand, in armed conflicts especially of non-international nature, civilians choose to take up arms and engage in hostilities against a party to a conflict at any time. This participation turns them into legitimate targets with no immunity from direct attack, but will not result in a change of their civilian status. This means that they will not become combatants by their choice to participate in hostilities and thus will not be afforded combatant privileges such as prisoner-of-war status upon capture. This restriction seeks to discourage civilians from joining fights. Nonetheless, in current conflicts, the direct participation in hostilities through cyber means, is evolving rapidly due to easier access to technology than to guns for example, also because virtual space offers more protection through the indirect participation in hostilities in comparison to physical participation. The reason why hybrid adversaries have heavily relied on hacktivists and private contractors to operate in today's battlefields. These hacktivists or civilian hackers operate using computers only and lack basic requirements to be considered lawful combatants. For example, carrying a computer openly does not fit the requirement of carrying an arm openly, as a computer is not considered a weapon until deployed to perpetrate cyber-attacks. According to Susan Brenner, "the integration of civilians into military efforts can create uncertainty as to whether someone is acting as a civilian or as a combatant."[1082] Another example of how civilians are taking a direct part in hostilities can be seen through cyber warriors recruited by governments.[1083] In this context, Sean Watts noted that "Many private companies have employed the skills of experts in various weapons commonly used in

[1081] AP I, Ibid., Article 50(1) and 51(2). See also, Tallinn Manual 2.0., Ibid. rule 34.
[1082] Brenner S., Cyberthreats, The Emerging Fault Lines of the Nation State, Oxford University Press, 2009, p. 197.
[1083] The Estonian government, in the aftermath of the cyber-attacks on that targeted its infrastructure in 2007, recruited civilian volunteers to serve as cyber warriors in case another cyber-attack occurred. See, Blair D., Estonia Recruits Volunteer Army of "Cyber Warriors", The Telegraph, 26 April. 2015.
Available at: https://www.telegraph.co.uk/news/worldnews/europe/estonia/11564163/Estonia-recruits-volunteer-army-of-cyber-warriors.html

computer network attacks (CNAs). For example, governments hired cybercriminals as "cyberwarriors" for defensive purposes."[1084] That raises the questions about whether such actors meet the requirements of legitimate targets, especially in the Notion of Direct Participation in Hostilities (DPH) in conflicts where armed actors and civilians intermingle.[1085]

ii- Civilian Direct Participation in Cyber Hostilities

The DPH notion is reasoned in treaty law applicable to IAC and NIAC through AP I[1086], and AP II[1087]. The concept also appears in the Rome Statute of the ICC.[1088] On the other hand, CA 3 to the GCs related to NIACs uses the word "active" rather than "direct", and states that "persons taking no active part in the hostilities shall in all circumstances be treated humanely." Similarly, the ICC in its Judgment in the Lubanga case, considered that "Thomas Lubanga" is convicted for the war crime of conscripting and enlisting children under the age of 15 and using them to "participate actively in hostilities" in conflicts not of an international character, according to Article 8(2)(e)(vii) of the Rome Statute.[1089] However, the ICRC reflected that under IHL the terms active and direct are synonymously used. According to the ICRC's Interpretive Guidelines on the Notion of DPH, it was noted: "although the English texts of the APs and the GCs use the words 'active' and 'direct', respectively, the phrase '*participant directement*' is used consistently throughout French texts of each treaty, a fact that these two terms refer to the same quality and degree of individual participation in hostilities."[1090]

[1084] Watts, S., Combatant Status and Computer Network Attacks, Virginia Journal of International Law, 2012, Vol. 50, p. 160.

[1085] One of the cases that was considered as the first time a cyber hacker was lethally targeted, is the U.S. drone strike in Syria that targeted Junaid Hussain a British hacker that carried out cyber activities on behalf of ISIS. Hussain was only engaged in cyber activities and managed to hack the US Central Command's social media accounts and published US soldiers and officers identifying information. In response, the US through a Drone Strike targeted Hussain in August 2015. See, Ackerman S., MacAskill E. and Ross A., "Junaid Hussain: British hacker for ISIS believed killed in US air strike", The Guardian, 27 August 2015.
Available at: https://www.theguardian.com/world/2015/aug/27/junaid-hussain-british-hacker-for-isis-believed-killed-in-us-airstrike

[1086] Article 51(3) of the AP I to the 1949 GCs "civilians shall enjoy the protection afforded by this section, unless and for such time as they take a direct part in hostilities."

[1087] Article 13(3) of the AP II to the 1949 GCs. Same text in of article 51(3).

[1088] Article 8(2)(b)(i) of the Rome Statute, Ibid., considers that a war crime occurs if there were intentionally attacks against civilians "not taking direct part in hostilities."

[1089] ICC, Persecutor v Thomas Lubanga Dyilo, Trial Chamber I, No. ICC-01/04-01/06, 14 March 2012, paras 568-571, pp. 261-263. In this context, the Trial Chamber did not reach a conclusion on the legal meaning of term "active participation in hostilities", as used in Article 8(2)(e)(vii). But the majority found that active participation is a concept that is distinct from, and broader than, direct participation in hostilities. The court stated that "the use of the expression 'to participate actively in hostilities' as opposed to the expression 'direct participation' (as found in AP I to the GCs) was clearly intended to import a wide interpretation to the activities and roles that are covered by the offence." Ibid. para 627.

[1090] ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Adopted by the Assembly of the ICRC, Vol. 90, no. 872, December 2008, p. 1013-14. See

Therefore, the two terms are similar and it was agreed that the notion of DPH is customary international law, a clear definition of this notion was lacking. To understand how Article 51(3) of AP I is interpreted, the ICRC conducted a project from 2003 to 2008 to explain how existing IHL applies in light of the circumstances prevailing in contemporary armed conflicts and resulted in the publication of the ICRC's Interpretive Guidance in 2009 (hereinafter "Interpretative Guidance")[1091], and that was edited by Nils Melzer.[1092] For this subsection, the Interpretive Guidance is highly relevant, though it does not directly deal with cyber warfare, yet it provides a general paradigm that can be built upon with regards to civilians' direct participation in cyber operations. According to Melzer "despite the important consequences incurred by civilians directly participating in hostilities, neither treaty law nor state practice or international jurisprudence provides a precise definition of what conduct amounts to direct participation in hostilities."[1093] To demonstrate, the Interpretative Guidance on DPH requires three cumulative elements for DPH and an additional element that relates to those who perform continuous combat functions. These elements are as follow:

- **Threshold of harm**

It requires the act in question to reach a certain severity threshold to the harm caused, or likely to be caused, for the individual to forfeit his civilian status.[1094] So, for private hackers or civilians to be considered directly participating in hostilities, their activities must be likely to adversely affect the military operations or capacity of a party to the conflict or must be likely to inflict death, injury, or destruction on persons or objects protected against direct attack.[1095] So, the qualification of an act as direct participation does not require the materialization of

---

also, the Trial Chamber of the ICTR in the Akayesu Decision that was called upon to interpret the meaning of the term "active" in the concept of CA 3, and held that "direct" and "active" are so similar that, for the purpose of the chamber, they may be treated as synonymous. ICTR, Prosecutor v Jean-Paul Akayesu, ICTR-96-4-T, Trial Chamber, 1 September 1998, para. 629.

[1091] The Interpretive Guidance was heavily criticized by legal experts, including some of those who participated in the project. See, Watkin K, Opportunity Lost: Organized Armed Groups and the ICRC "Direct Participation in Hostilities Interpretive Guidance"; Schmitt M., "Deconstructing Direct participation In Hostilities: The Consecutive Elements". On the other Hand, Nils Melzer the editor of the Interpretive Guidance has responded to these critiques through "Keeping the Balance between Military Necessity and Humanity: A response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities."

[1092] Delerue F., Civilian Direct Participation in Cyber Hostilities, Journal of the Internet, Law and Politics (IDP), University of Catalunya, October 2014, Issue 19, pp. 6-7.

[1093] Melzer N., Civilian Participation in Armed Conflict, Max Planck Encyclopedia of International Law, February 2010, p. 17.

[1094] Interpretive Guidance, Ibid. p. 1016.

[1095] For example, electronic interference with military computer networks could also suffice DPH, whether through computer network attacks (CNA) or computer network exploitation (CNE), as well as wiretapping the adversary's high command or transmitting tactical targeting information for an attack. See, Melzer N., Interpretive Guidance on the Notion of DPH, Ibid. p. 48.

harm reaching the threshold, but merely the objective likelihood that the act will result in harm.[1096] This goes beyond the mere definition of DPH stated in the Commentary on AP I that considered "direct participation means acts of war which by their nature or purpose are likely to cause actual harm to the personnel and equipment of the enemy armed forces."[1097]

However, the interpretative guidance has linked the threshold of harm to the adverse military effect in cases such as interruption of electricity, water, food supplies, and manipulation of computer networks. So, in the absence of the adverse military effects in such operations, the degree of harm required to as DPH would not qualify[1098]. In the cyber context, hybrid adversaries tend to cause harm but more in an indirect manner. Therefore, cyber operations conducted by civilian hackers that tend to cause death, injuries, or destruction on persons or objects protected against direct attack, seem to be difficult. So, certain objects must be included such as destruction or damage of data that are likely to cause harm required, especially the destruction of medical data in hospital databases. For example, Michael Schmitt argued that the principle of military harm is "under-inclusive" because it excludes loss of protection for support activities that do not adversely affect the enemy.[1099] However, in response to this critique, Melzer considered that "the Interpretive Guidance does not discard the causation of harm as a central element of direct participation in hostilities but, again under treaty law, simply recognizes that such harm does not necessarily have to be of a military nature."[1100] Similarly, it is considered that acts which by nature and objective intended to cause damage to civilians, such as attacks on medical data, are already included in the second section of the threshold harm related to acts that are likely to cause death, injury, or destruction.[1101] Nevertheless, one of the problems that might arise with regards to operations that disrupt the military capacity, is whether these operations conducted by civilian hackers represent a form of expression, propaganda, or aims to affect the military capacity, as civilian cyber actors might not be aware of the consequences of their acts. However, this can be mitigated in the "continuous combat

[1096] Ibid. pp. 1016-17. The report added that "the likelihood standard is evaluated objectively in each case."
[1097] Sandoz et al. (eds), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Geneva ICRC 1987.
[1098] Melzer N., Interpretive Guidance on the Notion of DPH, p. 50.
[1099] Schmitt M., Deconstructing Direct Participation in Hostilities: The Constitutive Elements, New York Journal for International Law and Politics, 2010, Vol. 42, p. 697.
[1100] Melzer N., Keeping the Balance between Military Necessity and Humanity: A Response to Four Critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities, International Law and Politics, 2010, Vol. 42, p. 860. Melzer adds that "the fact that the harm caused in the course of hostilities does not necessarily have to be of a military nature is illustrated by numerous references in treaty law to "attacks" against protected persons causing harm of a military nature, are clearly discussed as part of the conduct of hostilities."
[1101] This was also the suggestion by the Israeli Supreme Court. See more, Kilovaty I., Conflict in Cyberspace and International Law, Ibid. p. 142.

function" that is an essential supplement to the three requirements associated with the DPH framework that will be explained later. To summarize, cyber-attacks or operations that neither cause harm of a military nature nor inflict death, injury, or destruction on protected persons or objects would not cause the kind and degree of harm required to qualify as direct participation in hostilities.[1102]

- **Direct causation**

This element requires 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.[1103] Therefore, the harm in question must be brought about in one causal step, so it will not be sufficient that the act and its consequences be connected through an uninterrupted causal chain of events.[1104] This is challenging in cyber operations, as such attacks could reach the level of harm set in the first requirement, but may not satisfy the requirement of a direct causal link. So, civilians involved in cyber operations but in an indirect way would not be directly participating in hostilities if there is no causal link to the harm caused.[1105] So, only persons who are specifically recruited and trained for the execution of a predetermined hostile act can qualify as activities of an integral part of that act and therefore as direct participation in hostilities.[1106] While most cyber operations that involve civilian or private contractors are

[1102] Melzer N., Ibid. p. 50.

[1103] The ICRC in its commentary to the Interpretive Guidance with regards to "Direct Causation" element stated that: "In the present context, direct causation should be understood as meaning that the harm in question must be brought about in one causal step. Therefore, individual conduct that merely builds up or maintains the capacity of a party to harm its adversary, or which otherwise only indirectly causes harm, is excluded from the concept of direct participation in hostilities. For example, imposing a regime of economic sanctions on a party to an armed conflict, depriving it of financial assets, or providing its adversary with supplies and services (such as electricity, fuel, construction material, finances and financial services) would have a potentially important, but still indirect, impact on the military capacity or operations of that party. Other examples of indirect participation include scientific research and design, as well as production and transport of weapons and equipment unless carried out as an integral part of a specific military operation designed to directly cause the required threshold of harm. Likewise, although the recruitment and training of personnel is crucial to the military capacity of a party to the conflict, the causal link with the harm inflicted on the adversary will generally remain indirect. Only where persons are specifically recruited and trained for the execution of a predetermined hostile act can such activities be regarded as an integral part of that act and, therefore, as direct participation in hostilities." Melzer N., Interpretive Guidance on the Notion of DPH, Ibid. pp.52-53. See also, Akande D., Clearing the Fog of War? The ICRC's Interpretive guidance on Direct Participation in Hostilities, Blog of the European Journal of International Law, June 2009. Available at: https://www.ejiltalk.org/clearing-the-fog-of-war-the-icrcs-interpretive-guidance-on-direct-participation-in-hostilities/

[1104] Turns D., Cyber Warfare and the Notion of Direct Participation in Hostilities, Journal of Conflict and Security Law, Oxford university Press 2012, pp. 287-88

[1105] Melzer N., Interpretive Guidance on the Notion of DPH, Ibid. p. 52.

[1106] Ibid. p. 53.

secondary or tertiary, the links in the causal chain may not all be similar.[1107] In such cases, the direct causation requirement will be hardly met, as the harm intended is likely to occur over several causal steps.[1108] For instance, the Stuxnet attack went through three stages: "penetration, exploitation, and modification" in which separately each stage would not count as one causal step to constitute DPH.[1109] On the other hand, in cases of collective cyber operations, if a civilian's contribution on its own does not satisfy causal link, the civilian will still be considered as taking part in hostilities.[1110] Nonetheless, with the lack of universal State practice and consensus, direct causation will remain to be decided on a case-by-case basis.[1111]

- **Belligerent nexus**

An element that is less controversial in cyber operations, and requires that the hostile act in question is specifically designed to cause the required threshold of harm and specifically designed to do so in support of one party to the armed conflict at the detriment of the opposing party.[1112] Therefore, if the attacks by civilians are not related to the armed conflict, the DPH requirement will not apply. The interpretive guidance does not specifically comment on cyber-attacks concerning the nexus element, however, if belligerent nexus needs to be assessed in an armed conflict, the previous two elements of harm threshold and direct causality will need to be considered. In this regard, the Interpretive Guidance on whether a belligerent nexus exists to a specific act, consider that:

> "It must be based on the information reasonably available to the person called on to make the determination, but they must always be deduced from objectively verifiable factors. In practice, the decisive question should be whether the conduct of a civilian, in conjunction with the circumstances prevailing at the relevant time and place, can reasonably be perceived as an act designed to support one party to the conflict by directly causing the required threshold of harm to another party."[1113]

[1107] See, Owens W., Dam K and Lin H. (eds), Technology, Policy, Law, and Ethics regarding U.S. Acquisition and Use of Cyber-Attack Capabilities, The National Academic Press 2009, p. 127
[1108] Turns D., Ibid. p. 288.
[1109] Falliere N., W32 Stuxnet Dossier, Symantec Security Response, February 2011, p.2
[1110] Delerue F., Ibid. p. 9
[1111] Crawford E., Virtual Battlegrounds: Direct Participation in Cyber Warfare, Sydney Law School Research Paper, 2012, p. 9.
[1112] Melzer N., Interpretive Guidance on the Notion of DPH, Ibid. p. 58
[1113] Ibid. pp. 63-64.

Nonetheless, the belligerent nexus element must be carefully distinguished from individual self-defense and other criminal activities. According to Melzer, armed violence which is not part of violence occurring between belligerent parties cannot constitute hostilities. But rather for DPH to apply it should be carried out both in support of one belligerent party and to the detriment of another.[1114] Therefore, not all uses of armed force in armed conflict will be considered as part of the ongoing hostilities. So, with the increase in cybercrime incidents, distinguishing between cyberspace actors who are directly participating in a conflict and those who are merely opportunistic criminals, could be challenging.[1115]

- **The notion of continuous combat function (CCF)**

In the first place, time and continuity are essential elements that play important role in considering whether a civilian is associated with the DPH framework.[1116] This notion reflects the intended aim of distinguishing combatants from civilians. Individuals whose role in NSAs is to "prepare, execute, or command of acts or operations amounting to direct participation in hostilities", can be targeted even if not actively participating in hostilities at the time they are engaged.[1117] So, being a member of an organized armed group means that an individual assumes a continuous combat function for the related group. The notion of CCF has been used to promote the principle of distinction in NIAC, but that does not rule out its use in IAC too.[1118] Nevertheless, the CCF's main concern was to extend to some individuals engaged by private military and security companies, and to irregular members of the armed forces[1119], and by that distinguish them from civilians who participate in hostilities on a merely spontaneous, sporadic, or unorganized basis, or temporary role assumed for the duration of a particular operation.[1120] According to this notion, for cyber hackers to be considered legitimate targets based on their DPH, they must carry out cyber-attacks continuously and assume membership in an organized armed group that is a party to the armed conflict, to be considered civilian with

[1114] Melzer N., Keeping the Balance between Military Necessity and Humanity, Ibid. pp. 873-74
[1115] Prescott J., Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States, 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn 2012, p. 254.
[1116] Melzer N., Interpretive Guidance on the Notion of DPH, Ibid., p. 33.
[1117] Ibid. p .34.
[1118] Ibid. p. 25. The Interpretive Guidance states that "membership in irregular armed forces, such as militias, volunteer corps, or resistance movements belonging to a party to the conflict, generally is not regulated by domestic law and can only be reliably determined on the basis of functional criteria, such as those applying to organized armed groups in NIAC
[1119] Henry S., Exploring the "Continuous Combat Function" Concept in Armed Conflicts: Time for an Extended Application, International Review of the Red Cross, 2018, Vol. 100, p. 270.
[1120] Melzer N., Interpretive Guidance on the Notion of DPH, Ibid., p. 34.

CCF.[1121] Nevertheless, cyber hackers, whether intentionally participating in a conflict or not, would in all cases mask their operations and their membership to an organized armed group. Therefore, civilians involved in cyber-attacks would qualify as "unprivileged belligerents" that are not entitled to the same treatment as combatants[1122], particularly because distinguishing cyber combatants who are engaged in a specific hostile act from members of an organized group, is difficult. Moreover, expanding the definition of DPH through the CCF notion increases the risk of mistaken targeting, especially where most of NSAs do not wear distinguishing uniforms. Nevertheless, if the CCF does not appear in IHL treaties and is unsettled as custom, for civilian hackers operating during an armed conflict but in situations regulated by the law enforcement, human rights law must apply especially that it prohibits the targeting of individuals if based purely on their membership in an armed group. This was also the view of the independent international commission with regards to protests in the Occupied Palestinian Territory.[1123]

Based on the elements provided by the Interpretive Guidance, certain characters of cyber operations with regards to DPH will be challenging. For instance, the temporal scope of the loss of protection requires that civilians are targetable for such time as they take a direct part in hostilities. Civilians conducting cyber operations with no CCF status, lose their protection for each specific act amounting to direct participation in hostilities and then regain it after the end of the act. Such a situation is what so-called "revolving door", according to the Interpretive Guidance "is an integral part, not a malfunction of IHL, and it prevents attacks on civilians who do not, at the time, represent a military threat"[1124]. Yet, there were major disagreements among Tallinn Manual experts with regards to this notion, considering that ICRC's approach, which requires immunity from attacks between those periods, poses practical problems on the battlefield. In practice, while such an approach can be possible in traditional means such as laying down arms on a battlefield as evidence of act cessation, but in cyberspace spreading malware for instance that fits with the "harm threshold" does not cease when the attackers cease their operations. This puts civilian hackers at risk of being targeted as long as the malware is still active. Moreover, most cyber-attacks are detected after their perpetration, the time the

[1121] Kilovaty I., ICRC, NATO and the U.S.: Direct Participation in Hacktivities, targeting Private Contractors in Cyberspace under the Law of Armed Conflict, Duke Law and Technology Review,2016, Vol. 15, p. 146.
[1122] Schmitt M., Tallinn Manual on the International Law Applicable to Cyber Warfare, Ibid. p. 98.
[1123] Report of the detailed findings of the Independent International Commission of inquiry on the protests in the Occupied Palestinian Territory, Hyman Rights Council, 40th session, 25 February -22 March 2019, paras 103-107.
[1124] Ibid. p. 70.

attackers have already regained their civilian protection, these forfeits and regain allows hybrid actors, through civilians, to conduct operations repeatedly while gaining certain immunity from being targeted. Nonetheless, their immunity is not infinite, as they remain subject to criminal prosecution for violations of international or domestic law committed during such participation.

Similarly, the interpretive guidance considers that temporal scope includes measures preparatory to the execution of a specific act of direct participation in hostilities, as well as the deployment to and the return from the location of its execution. In the cyber context, this may be interpreted to cover the creation of cyberweapons that may constitute an act of direct participation, if this weapon is created for a specific act of hostilities or target, such as Stuxnet that was programmed to target specific programmable logic controllers (PLCs) for centrifuges in the Natanz facility. Besides, the Interpretive Guidance with regards to cyber operations, confirmed that the execution of hostilities does not require geographic displacement, but it will be restricted to the execution of the act and does not include deploying and coming back from the location where the computer system was used to launch attacks. In contrast, the Tallinn manual took a broader position by considering any act of direct participation in hostilities by a civilian render that persons targetable for such time they are engaged in the qualifying act of direct participation. For instance, traveling to and from the location where a computer used to mount an operation is based would be encompassed in the notion.

Though both approaches are not binding to States, it shows clearly that civilians engaged in cyber-attacks during an armed conflict, whether intentionally or not, blurs the line of distinction due to the nature of cyber operations through the initiation, effects, materialization, and termination of the cyber operations. That adds to the legal complexities towards extinguishing the right to strike at direct participants for cyberattacks those last mere minutes or perhaps seconds, adding an extra challenge to the principle of distinction. Therefore, though DPH is essential to the principle of distinction, neither the interpretive guidance nor Tallinn Manual managed to address the complexity raised by the nature of cyber-attacks. While the AP I for instance consider that in case of doubt whether a person is a civilian, that person shall be treated as a civilian. That should be also the case with regards to civilian taking part in cyber hostilities in an unclear manner, however, the international experts were not able to settle on what is a precise threshold to assess when such doubt appear, a challenge due to the interconnectivity of civilian and military network that renders them indistinguishable. After all, the latter is vital

especially since civilians involved in cyber operations might be neutralized not only by cyber-attack but also using kinetic force, which brings the principle of proportionality to light. For this reason, it is recommended that cyber activity should be met with a cyber response, as a kinetic response might bring more harm and violate the principle of distinction, particularly with regard to dual-use objects.

And finally, the geographic limitation of IHL that is limited to the territoriality of armed conflict can also be challenged by civilians taking part in hostilities through cyber means from remote areas. However, if these civilians cannot be qualified as taking direct part under IHL, they are prosecuted for their acts under the territorial State's domestic laws. This was discussed in the previous section and concluded that it shall be solely addressed under law enforcement procedures to avoid the consequences of the global battlefield. Eventually, risks on the civilian population from being illegally targeted will increase due to the ambiguous nature of contemporary conflicts. At the same time, hybrid adversaries will rely more on civilians who will become more involved in cyber operations during armed conflicts. Therefore, with the shortcomings of IHL treaties and state practices, more normative developments especially for international rules of conduct in cyberspace, are necessary. Other principles such as proportionality and military necessity are also essential in the asymmetric nature of nowadays conflicts, whereby the disproportionate means used between cyber combatants and conventional combatants would be clear.

Conclusions

Summarizing the analysis of hybrid warfare, particularly cyber-attacks and NSAs, under the international law on the use of force and international humanitarian law, the following conclusions are to be drawn:

1- In analyzing the evolution of warfare from conventional to modern, the author concluded that hybrid warfare is not a new phenomenon, on the contrary the theories of Sun Tzu and Von Clausewitz explained the dynamics of all types of contemporary conflicts, including their hybrid nature. Modern hybrid warfare crystalizes several legal areas of uncertainty in international law and provides a relevant and potentially useful analytical framework for assessing the relation between International legal regimes governing the use of force and the law of armed conflict in contemporary warfare scenarios. Hybrid warfare's main feature is legal asymmetry, as adversaries tend to deny their responsibility for hybrid operations to escape legal consequences of their actions. Modern technology employed by states and non-state actors establish an asymmetric legal environment, as states that continue to abide by the law are placed at a competitive disadvantage against adversaries that exploit legal ambiguities and violate the rules of international law. Also, Lawfare is one of the means that create confusion to the applicable law and the legal responsibility of actions, based on the legal uncertainties arising from it, the adversaries (whether state or non-state armed groups) exploit the disadvantages of legal restrictions placed upon the complaint actor leading to the emergence of asymmetric warfare by abusing laws.

2- The prohibition on the use of force between states is the keystone of modern international law that applies to old and new threats, including hybrid warfare through cyber operations and the employment of non-state armed groups. The author concluded that the threshold of an armed attack to threats generated from hybrid warfare, particularly low-intensity attacks, erodes the effectiveness of the armed attack notion as these operations maintain a certain level that does not reach the armed attack threshold but brings the same effects as a large-scale armed attack. Nevertheless, attacks that lead to "disruption, degradation or destruction of core security assets" are considered eligible for qualification as an armed attack. The author promoted the accumulation of events theory in dealing with a series of separate low-intensity attacks, as to consider that even low-intensity operations if accumulated together can reach the threshold of an armed attack. Nonetheless, such assessment must ensure to be in line with the core legal meaning and purpose of the UN Charter and meet the essential legal requirements of proportionality and necessity.

3- The right to self-defense against non-state armed groups is granted under international law on the use of force and does not limit the potential originator of armed attacks to States. The author argued that the right to use force in self-defense without the consent of the territorial state against attacks by non-state armed groups generated from the territory of another state, whether through kinetic or virtual means, is still unsettled and can constitute an unlawful violation of the host state's territorial sovereignty. Hybrid warfare relies heavily on masking attribution that is highly relevant for the proper applicability of the Law on the use of force, particularly in responding to threats or violations of state sovereignty. This necessitates the establishment of legal basis that outweighs the principle of territorial sovereignty and prohibition on the use of force, e.g., through the United Nations Security Council resolution.

4- In analyzing the unable and unwilling standard, the author argued that considering the standard as a rule rather than an ad hoc decision by states requires to be embraced by consistent and widespread practice accompanied by opinio Juris as a matter of promulgation, that is not reached yet though relatively promoted by many states. The author concluded that cyber operations generated from the territory of another state would threaten the host state's sovereignty under this standard, as a state might be willing to cease the threat but unable due to the complex nature of cyberspace. Countermeasures under the abovementioned standard must consider the host state's technical abilities to identify and prevent such operations, otherwise, it will be considered a breach of basic principles of international law.

5- In the presence of two conflicting standards of effective and overall control generated from different legal regimes, it appeared that there is no unified regulatory mechanism that applies to current threats, particularly when international actors disregard certain rules for their interests. The nature of cyber operations does not fit with the classical control tests introduced by the ICTY and ICJ. The author concluded that hybrid warfare through operations of transnational effect is shifting the applicable law on the use of force to be stretched by ad hoc decisions by states to deter such operations, creating a pattern that could evolve into a conventional rule. The author argued that extending the right to use force in self-defense against cyber operations by eliminating the attribution of acts to a state requirement, violates the state sovereignty under current rules.

6- Examining the principle of sovereignty in the context of hybrid warfare, the author concluded that if a state exercises its authority whether through state agents, non-state actors, or proxies in another state's territory without the former's consent, constitutes a

violation of another state's sovereignty. The threshold of a state's involvement and its organs to trigger a violation of state sovereignty is dependent on case-by-case assessment if no other rules of international law apply to the incident. The principle of sovereignty applies in relation to states' cyber activities, as it applies in the non-cyber context. The degree of infringement upon the target State's territorial integrity and interference with or usurpation of inherently governmental functions, are two measures that reflect treating violations of sovereignty as a primary rule of international law. The author concluded that the irregular features of cyberspace led to no agreement as to what are the effects required under a de minimis threshold in the cyber context.

7- To eliminate the complexity of attribution in cyberspace, a state has a duty to prevent malicious cyber-attacks. Injured states in concordance with IHL and customary international law could take action to bring the harboring state into compliance with its international obligation if it refused to take actions. The author has suggested that the Due Diligence standard provides a preventive remedy. Due diligence is considered a legal standard of conduct whose content and extent vary according to the applicable primary rule in international law, it was also developed under law of armed conflict, particularly with regards to the obligation of conduct concerning preventive and repressive measures taken by States. The standard provides good practice in developing a preventive approach and eases the complexity associated with the attribution of cyber activities and strengthens the implementation and compliance with the law of armed conflict. The author suggested that certain improvements for due diligence's full functionality are vital, such as the level of control of cyberspace activity, technical feasibility, and capacity of states to monitor their cyber borders and settling the de minimis threshold otherwise due diligence could become a tool of provocation and the potential mean of lawfare that is used to destabilize an order.

8- International humanitarian law applies to armed conflicts despite the type of weapons or methods used. The interplay between IHL and IHRL, once interpreted in harmony, is necessary to eliminate the confusion created by hybrid adversaries that blur the line between peace and wartime. These two separate branches of international law are working in parallel to fill the normative gaps in the protection of individuals. However, certain situations might raise misconceptions in the co-application of both legal bodies, such as terrorist or cyber operations in NIACs. That has an impact on the "lex specialis" rule that is invoked once two principles coincide. So, it was proposed that the nature of

contemporary conflicts requires more developed co-application rules that provides a hybrid approach based on the elements of the conflict.

9- In analyzing cyber-attacks by non-state armed groups in non-international armed conflicts and the geographic limitation of IHL, the author argued that attacks generated from non-belligerent states impose challenges when the victim State is in a NIAC. The study concluded that the NIAC should not expand to the territory of a neutral state without its consent, due to the fluid nature of contemporary conflicts and the role of NSAs in cyberspace in which might lead to the catastrophic global battlefield. Such attacks do not fall in a legal vacuum in which jus ad Bellum and other legal regimes can address the State's responsibility for not securing its territory from being used to conduct operations against another state.

10- Cyber operations in international armed conflicts must meet the threshold of violence akin to those of traditional means and weapons for the application of international humanitarian law. Cyber operations that occur in isolation from kinetic attacks do not reach the level of armed violence, are regulated by either domestic or human rights law. The author proposed that when such operations are conducted in a hybrid manner involving kinetic or non-kinetic means, and accumulatively reach the level of an armed attack, international humanitarian law applies. It is required to expand the international humanitarian rules to cover cyber operations that cause severe data loss or financial loss (that traditionally do not meet the scale and effect threshold) when such attacks are seen as part of a larger scale operation.

11- In analyzing the co-existence of international and non-international armed conflict in single battlefield, the author argued that hybrid actors can skillfully combine and split their operations based on the legal regime that offers them broader protection under the Geneva conventions. The author proposed that the gap between the two articles requires certain eradication by expanding the coverage of Common article 2 of the Geneva convention in mixed conflicts, as unequal humane treatment should not be acceptable in cases of detention, similarly with regards the rights of injured people, and prisoners of war status that varies between international and non-international armed conflicts. Also, it would be fairer if the humane treatment accorded to a person be based on the status of the persons themselves, rather than on the status of the conflict.

12- In analyzing the impact of hybrid warfare means to the principle of distinction. The author concluded that cyber operations create a grey legal zone with regards to the legality of targeting civilian objects and distinguishing them from military objectives. With no

comprehensive definition of cyber operations under international humanitarian law, it is required to clearly define the dual-use objects under the principle of distinction, and while international humanitarian law considers that any military use of a civilian object including cyberinfrastructure renders the object a military one, the author argued that this will have a direct impact on the civilians in an interconnected nature of cyberspace. Also, the "purpose test" denotes the intended future use of the object, rather than the actual use of the cyberinfrastructure. So, when such infrastructure is of dual-use, the principle of distinction is at risk especially since there are no clear standards provided by IHL or states as to what would be the nature of objects that cyber-attacks can target without violating the principle of distinction. The author proposed that the "purpose test" must be established under a higher threshold to offer maximum protection to civilians and their objects and cover also the essential civilian data, such as medical ones.

13- Hybrid warfare has an impact on blurring the line of distinction between combatants and civilians, particularly those taking direct part in hostilities through cyber means. IHL applies and is sufficient in most cases of civilian direct participation in cyber hostilities. The interpretive Guidance provided three elements that prove civilians' Direct participation in hostilities (harm threshold, direct causation, and belligerent nexus) and an additional notion of continuous combat function. In analyzing these elements of civilian cyber operations, the author concluded that the nature of cyberspace does not fit the abovementioned elements. Cyber-attacks do not cease when the attackers cease their operations, therefore the direct cessation does not apply in most of the cases where perpetrators are spreading malware for instance. Likewise, cyber-attacks are identified after their perpetration, the time the attackers have regained their civilian status. This disqualifies belligerent nexus from the equation through which such forfeit and regain interplay allows hybrid actors to conduct recurrent operations while gaining certain immunity. In addressing the "temporal scope" on the Notion of Direct participation in cyber hostilities, the author concluded that the notion is underregulated in international humanitarian law and does not treat a civilian cyber combatant as lawful combatant causing tremendous disparity of treatment in the case of capture and detention when compared to regular lawful civilian combatant using conventional weapons.

Bibliography

PRIMARY SOURCES

TREATIES and CONVENTIONS

- Charter of the United Nations (adopted in San Francisco 26 June 1945, entered into force 24 October 1945) 59 Stat 1031, TS 993, 3 Bevans 1153.
- Convention for the Protection of Cultural Property in the event of Armed Conflict with Regulations for the Execution of the Convention 1954, The Hague, 14 May 1954.
- Convention IV respecting the Laws and Customs of War on Land and its Annex: Regulating concerning the Laws and Customs of War on Land (The Hague Convention 1907), The Hague, 18 October 1907.
- Convention on Cybercrime 2001 (signed at Budapest 23 November 2001, entered in force 7 January 2004, ETS 185).
- Convention on International Civil Aviation, December 1944, 15 UNTS 295
- Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May be Deemed to be Excessively Injurious or to Have Indiscriminate Effects (10 October 1980, as amended in 2001).
- Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to Have Indiscriminate Effects, Geneva, 10 October 1980.
- Convention on the Prevention and Punishment of the Crime of Genocide 1948, 78 UNTS 277
- Convention on the Prohibition of the Development, Production, Stockpiling and use of Chemical Weapons and on Their Destruction, Paris 13 January 1993 (entry in force April 1997).
- Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, 18 September 1997 (entry in force March 1999).
- Convention on the Rights of the Child of 1989, 28 I.L.M. 1448 (entered into force September 2,1990) Nov. 20, 1989.
- Covenant of the League of Nations (adopted 28 June 1919, entered into force 10 January 1920) 225 Parry 195; 1 Hudson 1; 112 BFSP 13; 13 AJIL Supp. 128 (1919).
- Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight, Saint Petersburg, 11 December 1868.
- Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 31.
- Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85.
- Geneva Convention relative to the Protection of Civilian Persons in Time of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 287.
- Geneva Convention relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135.
- International Covenant on Civil and Political Rights, UNGA Res 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967).
- Montevideo Convention on the Rights and Duties of States, signed at the International Conference of American States in Montevideo Uruguay, 26 December 1933, came into force 26 December 1934.
- Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, 25 May 2000 (entry in force February 2002).
- Preamble of the 1899 Hague Convention (II) with Respect to the Laws and Customs of War on Land 1900 and 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land 1910
- Protocol Additional (I) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (adopted 8 June 1977, entered into force 07 December 1978).
- Protocol Additional (II) to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (adopted 8 June 1977, entered into force 07 December 1978).
- Protocol II on Prohibitions or Restrictions on the Use of Mines, Booby-Traps and Other Devices as amended on 3 May 1996.

- Rome Statute of the International Criminal Court (adopted 17 July 1998, entered into force 1st July 2002) UN Doc. A/CONF. 183/9; 2187 UNTS 90.
- Second Protocol to the Hague Convention of 1954 for the Protection of Cultural Property in the Event of Armed Conflict (26 March 1999).
- Statute of the International Court of Justice (ICJ Statute) (annexed to the Charter of the United Nations, adopted 26 June 1945, entered into force 24 October 1945, 3 Bevans 1179, 59 Stat 1031, TS 993, 39 AJIL Supp 215 (1945)).
- Statute of the International Criminal Court, adopted by the Diplomatic Conference of the Plenipotentiaries to the United Nations on the creation of an International Criminal Court, 17 July 1998
- Statute of the International Tribunal for the Prosecution of Persons Responsible for Serious Violations of International Humanitarian Law Committed in the Territory of the Former Yugoslavia since 1991 (Adopted by UNSC Res 827 (1993) of 25 May 1993 amended by UNSC Res 1166 (1998) of 13 May 1998, Res 1329 (2000) of 30 November 2000, Res 1411 (2002) of 17 May 2002 and Res 1431 (2002) of 14 August 2002).
- Statute of the Permanent Court of International Justice (PCIJ Statute) (adopted 16 December 1920, entered into force 20 August 1921, 6 LNTS 379, 390, 114 BFSP 860, 17 AJIL Supp 115 (1923)).
- The Convention on Cluster Munitions was concluded by the Dublin Diplomatic Conference at Dublin on 30 May 2008.
- Treaty on the Non-proliferation of Nuclear Weapons of 1 July 1968, 729 U.N.T.S., p. 161. (entered into force on 5 March 1970)
- United Nations Convention on the Law of the Sea 1982 (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS 3, 21 ILM 1261 (1982)
- Vienna Convention on Diplomatic Relations (adopted in Vienna 18 April 1961, entered into force 24 April 1964) 500 UNTS 95, 23 UST 3227, 55 AJIL 1064 (1961
- Vienna Convention on the Law of Treaties (adopted 23 May 1969, entered into force 27 January 1980) UN Doc. A/Conf.39/27, 1155 UNTS 331, 8 ILM 679 (1969), 63 AJIL 875 (1969) 1980

JURISPRUDENCE

ICJ

- Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), Judgment of 26 Feb 2007, ICJ Rep 2007
- Application of the Convention on the Prevention and Punishment of the Crime of genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Judgment) [2007] ICJ Reports 43
- Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Separate Opinion of Judge Simma) [2005] ICJ Reports 334
- Armed Activities on the Territory of the Congo (Democratic Republic of the Congo v Uganda) (Separate Opinion of Judge Kooijmans) [2005] ICJ Reports 306
- Armed Activities on the Territory of the Congo (the Democratic Republic of the Congo v. Uganda), Judgment, 2005 I.C.J. Rep.168 (Dec. 19)
- Certain Activities Carried Out by Nicaragua in the Border Area (Costa Rica v. Nicaragua), Judgement, ICJ Reports 2015
- Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania) (Assessment of the amount of compensation) [1949] ICJ Reports 244
- Corfu Channel (United Kingdom of Great Britain and Northern Ireland v Albania) (Judgment on the Merits) [1949] ICJ Reports 4
- ICJ Advisory Opinion on Declaration of Independence in Respect of Kosovo, 22 July 2010
- ICJ Advisory Opinion on the Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, 9 July 2004
- Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (Advisory Opinion) [2004] ICJ Reports 136
- Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Reports 14
- Nuclear Tests, New Zealand v France, Admissibility, Judgment, [1974] ICJ Rep 457, ICGJ 137 (ICJ 1974), 20th December 1974, United Nations [UN]; International Court of Justice [ICJ]
- Oil Platforms (Islamic Republic of Iran v United States of America), (Judgment) [2003] ICJ Reports 161
- Oil Platforms (Islamic Republic of Iran v United States of America), (Separate Opinion of Judge Simma) [2003] ICJ Reports 324

- Oil Platforms, Iran v United States, Judgment, Merits, ICJ GL No 90, [2003] ICJ Rep 161, ICGJ 74 (ICJ 2003), 6th November 2003, International Court of Justice [ICJ]
- Separate Opinion of Judge Yusuf, Advisory Opinion, Accordance with International Law of the Unilateral Declaration of Independence in respect to Kosovo, Advisory Opinion of 22 July 2020.
- The Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Merits, 26 February 2007, ICJ Reports 43
- The Case of the SS 'Lotus' (1927) Serie A, N°10 Collection of judgments (PCIJ)
- The Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, Dissenting Opinion of Judge Higgins, ICJ Reports 226 (1996),
- The Oral Pleadings of Uganda, Cr 2005/7, 18 April 2005.
- United States Diplomatic and Consular Staff in Tehran (United States of America v Iran) (Judgment) [1980] ICJ Reports 3

ICTY

- Prosecutor v Dusco Tadić (sentencing Judgment), IT-94-1-Tbis-R117, International Criminal Tribunal for the former Yugoslavia (ICTY), 11 November 1999.
- Prosecutor v Dusko Tadić (Trial Judgement) [1997] IT-94-1-T (ICTY, Trial Chamber)
- Prosecutor v Fatmir Limaj, Haradin Bala, & Isak Musliu (Trial Judgement) [2005] IT-03-66-T (ICTY, Trial Chamber)
- Prosecutor v Ljube Boškoski & Johan Tarčulovski (Trial Judgment) [2008] Case No IT-04-82-T (ICTY, Trial Chamber II)
- Prosecutor v Naletilic and Martinovic, ICTY Judgment no. IT-98-34-T, 31 March 2003
- Prosecutor v Rutaganda, Case no. ICTE-96-3-T, Judgment and Sentence of December 6, 1999
- Prosecutor v Tadic, Decision on the Defense Motion for Interlocutory Appeal on Jurisdictions, 2 October 1995
- Prosecutor v. Aleksovski, ICTY Trial Chamber 1999, Case No. IT-95-14/1T
- Prosecutor v. Baskic, Case No. IT-95-14-T, ICTY Trial Chamber Judgment, 3 March 2000
- Prosecutor v. Blaskic, IT-95-14, Judgment, 3 March 2000, Declaration of Judge Shahabuddin.
- Prosecutor v. Dusko Tadic, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, ICTY IT-94-1-A, 2 October 1995
- Prosecutor v. Fatmir Limaj, Judgment, ICTY, IT-03- 66-T, 30 November 2005
- Prosecutor v. Haradinaj, case No. IT-04-84-T, ICTY Trial Chamber judgment, 3 April 2008
- Prosecutor v. Limaj, Case no. IT-03-66-T, ICTY Trial Chamber Judgment, 30 November 2005
- Prosecutor v. Ljube Boskoski and Johan Tarculovski, ICTY Trial Chamber II Judgment 10 July 2008,
- Prosecutor v. Naletilic, Case No. IT-98-34-T, ICTY Trial Chamber Judgment, 31 March 2003
- Prosecutor v. Rutaganda, Case no. ICTR-96-3, Trial chamber I Judgment, 6 December 1999
- Prosecutor vs Dusko Tadić (Interlocutory Appeal on Jurisdiction) [1995] IT-94-1 -AR72 (ICTY, Appeals Chamber)
- Prosecutor vs Dusko Tadić (Judgment) [1999] IT-94-1-A (ICTY, Appeals Chamber)

OTHER INTERNATIONAL COURTS AND TRIBUNALS

- Island of Palmas Arbitration (The Netherlands v. U.S.), Decision of 4 April 1928, reprinted in UNRIAA, Vol. 2
- Portugal v. Germany (The Naulilaa Case), Special Arbitral Tribunal, 31 July 1928 (1927-28) Annual Digest of Public International Law Cases
- Reports of International Arbitral Awards, Eritrea-Ethiopia Claims Commission - Partial Award: Jus ad Bellum- Ethiopia's Claims 1-8, December 2005, vol. XXVI
- The Claims of Rosa Gelbtrunk and the "Salvador Commercial Company", *et al.* (El Salvador, USA0, UNRIAA, vol. XV, no. 66, 1902
- The Prosecutor v Jean-Paul Akayesu (Trial Judgement) [1998] Case No ICTR-96-4-T (International Criminal Tribunal for Rwanda, Chamber I)
- The Prosecutor v Thomas Lubanga Dyilo (Decision on the confirmation of charges) [2007] Pre-Trial Chamber I ICC-01/04-01/06
- The Prosecutor v Thomas Lubanga Dyilo (Judgment pursuant to Article 74 of the Statute) [2012] Pre-Trial Chamber I ICC-01/04-01/06-2842

- The Prosecutor v. Rutaganda, Case No. ICTR-96-3-T, ICTR, Judgment by Trial Chamber I, 6 December 1999

NATIONAL COURTS

- Public Committee against torture in Israel v. Government of Israel (targeting killing case), HCJ 769/02, IsrSC 2006.
- Hamdan v. Rumsfeld, 548 U.S. 557 (2006), the Supreme Court of the United States .
- Decision No. 6-P of 19 March 2014, Rossiyskaya Gazeta, Federal Issue No. 6335, 19 March 2014.

UNITED NATIONS

- Documents of the United Nations Conference on International Organization, Vol. VI, 1945
- Draft Articles on Diplomatic Protection 2006, Part 1, Article 1, Adopted by the International Law Commission at its 58th session, 2006
- International Law Commission (ILC), Draft Articles on Responsibility of States for Internationally Wrongful Acts, in Report of the International Law Commission on the Work of Its Fifty-third Session, UN GAOR, 56th Sess., Supp. No. 10, at 43, UN Doc. A/56/10
- Draft Declaration on the Rights and Duties of States with commentaries, Text adopted by ILC in 1949
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 2015 report, Note from the Secretary-General, A/70/174, July 22, 2015
- ILA, Final Report of the Use of Force Committee, The Meaning of Armed Conflict in International Law, June 2010
- ILA's Report on Aggression and the Use of Force, International Law Association, Sydney Conference 2018
- ILC, Summary Record of the 242th Meeting of 21s July 1995, Yearbook of the International Law Commission, 1995
- International Law Commission, Commentary on the Draft Articles on Prevention of Transboundary Harm from Hazardous Activities, 2001, Report of the ILC on its 53rd Session
- International law Commission, Report of the International Law Commission on the work of its Thirty-second session, 5 May–25 July 1980, Official Records of the General Assembly, Thirty-fifth Session, Supplement No. 10, UN document A/35/10, 1980
- Letter dated 8 January 2020 from the Permanent Representative of the United States of America to the United Nations addressed to the President of the Security Council, 9 January 2020, S/2020/20.
- Letter dated 9 October 2019 from the permanent Representative of Turkey to the United Nations addressed to the President of the Security Council, United Nations Security Council, S/2019/804
- Letter from the Charge d'affaires a.i. of the Permanent Mission of Canada to the United Nations addressed to the President of the Security Council, UN Doc. S/2015/221, March 31, 2015
- Report of the Commission of Inquiry on Lebanon pursuant to Human Rights Council Resolution S-2/1, 2006 UN Doc. A/HRC/3/2.
- Report of the Commission of Inquiry, League of Nations Doc. C.663.M.320, Oct. 1, 1932
- Report of the detailed findings of the Independent International Commission of inquiry on the protests in the Occupied Palestinian Territory, Human Rights Council, 40th session, A/HRC/40/CRP.2, 25 February -22 March 2019
- Report of the High-level Panel on Threats, Challenges, and Change. A More Secure World: Our Shared Responsibility, UN General Assembly, A/59/565, 2 December 2004,
- Report of the International Commission on Intervention and State Sovereignty, The Responsibility to Protect, ICISS, December 2011
- Report of the International Community on Intervention and State Sovereignty, transmitted by Letter Dated 26 July 2002 from the Permanent Representative of Canada to the UN addressed to the Secretary-General, The Responsibility to Protect, UN Doc. A/57/303 (2001).
- Report of the Secretary-General on In Larger Freedom: Towards Development, Security, and Human Rights for All (A/59/2005)
- Report of the Secretary-General's High-Level Panel on Threats, Challenges and Change on A More Secure World: Our Shared Responsibility, 2004, (A/59/565).
- Report of the Special Rapporteur "Fionnuala Ni Aolain" on the promotion and protection of human rights and fundamental freedoms while countering terrorism General Assembly, 3 September 2020, 75th session

- Statute of the ICTY for the Prosecution of Persons Responsible for Serious Violations of IHL Committed in the Territory of the Former Yugoslavia since 1991, U.N. doc S/25704 , annex 1993 and S/25704/Add.1 1993, adopted by Security Council on 25 May 1993
- The Doha Declaration: Promoting A Culture of Lawfulness, E4J University Module Series: Counter-Terrorism "Classification of Persons", July 2018; available at: https://www.unodc.org/e4j/en/terrorism/module-6/key-issues/classification-of-persons.html
- UN Charter, Chapter VII on the Actions with respect to Threats to the Peace, Breaches of the peace and Acts of Aggression
- United Nations Convention on the Law of Treaties, signed at Vienna 23 May 1969 (entered into force 27th of January 1980), Section 2 on Application of Treaties.
- World Summit Outcome Document 2005, Resolution adopted by the General Assembly on 16 September 2005, https://undocs.org/A/RES/60/1 .

UNGA RESOLUTIONS

- Letters of the United States and the United Kingdom to the Security Council regarding their operations in Afghanistan, UNSCOR, 56th Year, UN Doc S/2001/946, and UNSCOR, 56th Year, UN Doc S/2001/947
- UN General Assembly resolution 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, 24 October 1970
- UN General Assembly Resolution, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, Resolution A/RES/25/2625, at the 25th session, 24 October 1970
- UN General Assembly resolution 2625 (XXV) on Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations 24 October 1970
- UN General Assembly Resolution 3314 (XXIX), A/RES/3314, (UNGAR 3314), 14 December 1974
- UN General Assembly Resolution 41/38 of November 20, 1986.
- UN General Assembly resolution A/RES/56/83 of 12 December 2001 and its annex
- UN General Assembly, International Convention for the Protection of All Persons from Enforced Disappearance, 20 December 2006, available at: https://www.refworld.org/docid/47fdfaeb0.html
- UN General Assembly, Resolution No. 68/262 on the Territorial Integrity of Ukraine of 27 March 2014.

UNGA DOCUMENTS

- A More Secure World: Our Shared Responsibility, Report of the High-level Panel on Threats, Challenges and Change, 2004, UN Doc A/59/565.
- Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, United Nations General Assembly, 68th session, 24, June 2013
- Secretary-General, Developments In The Field Of Information And Telecommunications In The Context Of International Security, U.N. Doc. A/66/152
- Letter from charge d'affaires a.i. of the Permanent Mission of Turkey to the UN addressed to the President of the Security Council, UN Doc. S/2015/563 of 24th of July 2015.
- Letter from the Permanent Representative of the United States of America to the UN addressed to the Secretary-General, UN Doc. S/2014/695, 23 September 2014.

UNSC RESOLUTIONS

- Security Council Resolution 2190 (2016) on "Prosecuting and Punishing the Crimes Against Humanity or even Possible Genocide committed by Daesh".
- Security Council Resolution 2133 (2016) on "Legal remedies to human rights violations on the Ukrainian territories outside the control of the Ukrainian authorities"
- Security Council Resolution 2132 (2016) on "Political consequences of the conflict in Ukraine"
- Security Council resolution 849 (1993) [on implementation of the cease-fire and dispatch of military observers to Abkhazia, Georgia]
- Security Council Resolution 858 (1993) [on the establishment of the UN Observer Mission in Georgia]
- Security Council Resolution 1150 (1998) [Extension of the mandate of the UN Observer Mission in Georgia (UNOMIG)]
- Security Council Resolution 1584 (2005) [on monitoring the implementation of the arms embargo imposed by resolution 1572 on Côte d'Ivoire]
- Security Council Resolution (S.C. Res.) 1368, September 12, 2001

- Security Council Resolution 270 of 26 August 1969
- Security Council Resolution 2625 (XXV) of 24 October 1970 containing the Declaration of Principles of International Law, Friendly Relations and Cooperation Among States in Accordance with The Charter of the UN, UN Doc. A/Res/2625
- Security Council Resolution 487 of 19 June 1981.
- Security Council Resolution 678, Iraq-Kuwait of 29 November 1990
- Security Council resolution 1368 of September 12, 2001 UN Doc S/RES/1368
- Security Council Resolution 1373 of September 28 2001, UN Doc S/RES/1373

EUROPEAN UNION

- Council of Europe, Draft Resolution on the Legal Challenges related to the Hybrid War and Human Rights Obligations, Committee on Legal Affairs and Human Rights, As/jur (2018) (Draft resolution and recommendation adopted unanimously by the committee on 14 March 2018.)
- European Commission (2016b), Joint Framework on countering hybrid threats: A European Union response, Communication, JOIN (2016
- European Council meeting (22 March 2018), Conclusions. https://www.consilium.europa.eu/en/meetings/european-council/2018/03/22
- European External Action Service, Food-for-Thought Paper "Countering Hybrid Threats", 8887/15, May 13, 2015
- European Parliament Resolution of 28 November 2019 on recent actions by the Russian Federation against Lithuanian Judges, Prosecutors and Investigators involved in investigating the Tragic events of 13 January 1991 in Vilnius, Doc. 2019/2938 (RSP)
- Interim Report of the Council of Europe Ad Hoc Advisory Group on Cross-Border Internet to the Steering Committee on the Media and New Communications Services, Incorporating Analysis of Proposals for International and Multi-Stakeholder Cooperation on Cross Border Internet, Strasbourg 2010
- Joint Research Centre and European Centre of Excellence for Countering Hybrid Threats, The Landscape of Hybrid Threats: A Conceptual Model, European Commission, Brussels 2020.
- Legal Challenges related to the Hybrid War and Human Rights Obligations, Committee on Legal Affairs and Human Rights, Council of Europe, AS/Jur 2018
- Opinion of CAHDI on Recommendation 2130 (2018) of the Parliamentary Assembly of the Council of Europe “Legal Challenges Related to Hybrid War and Human Rights Obligations”
- Parliamentary Assembly of the Council of Europe Resolution 2198 (2018) of 23 January 2018

ECHR

- European Court of Human Rights (ECHR), New Inter-State application brought by the Netherlands against Russia concerning the downing of Malaysia Airlines flight MH17, registered under no. 28525/20, July 2020.
- European Court of Human Rights (ECHR), case of Hassan v. The United Kingdom, Judgment 16 September 2014

International Committee of the Red Cross

- 31st International Conference of the Red Cross and Red Crescent, ICRC Report 2011: International Humanitarian Law and the Challenges of Contemporary Armed Conflicts.
- 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, ICRC 2016, Cambridge Core.
- Commentary to the Third Geneva Convention, J. Pictet ed., ICRC, 1960
- 32nd Conference of the Red Cross and Red Crescent: Report on International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, ICRC 2015
- 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, 2nd ed., Cambridge University Press, 2016
- ICRC Report on Avoiding Civilian Harm from Military Cyber Operations During Armed Conflict, ICRC Expert Meeting 21-22 January, 2021
- ICRC Report, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Recommitting to Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, October 2019

- ICRC, Commentary on the First Geneva Convention, 2016, Published online on 22 March 2016, available: https://ihl-databases.icrc.org/ihl/full/GCi-commentary
- ICRC, Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva,12 August 1949
- ICRC, Customary IHL, Israel "Practice relating to Rule 106.", Conditions for Prisoner of War Status, Section A, Chapter III.
- ICRC, Draft Revised or New Conventions for the Protection of War Victims, Geneva, May 1948
- ICRC, How is the term "Armed Conflict" Defined in International Humanitarian Law? Opinion paper, March 2008
- ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, Position Paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 2019.
- ICRC, International Humanitarian Law and Cyber Operations during Armed Conflicts, ICRC Position Paper, November 2019
- ICRC, International Humanitarian Law and the challenges of contemporary armed conflicts: Report, October 2011
- ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Geneva, October 2015. Available at: https://www.icrc.org/en/document/international-humanitarian-law-and-challenges-contemporary-armed-conflicts
- ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, Geneva, May 2009; available at: https://casebook.icrc.org/case-study/icrc-interpretive-guidance-notion-direct-participation-hostilities
- ICRC, Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, adopted by the Assembly of the ICRC, Vol. 90, no. 872, December 2008
- ICRC, Protection of Victims of NIACs, Document presented at the Conference of Government Experts of the Reaffirmation and Development of International Humanitarian Law applicable in Armed Conflicts, Vol. V, Geneva, 24 May – 12 June 1971
- IHL Database, Customary IHL , Chapter 33-34. https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter33
- International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Recommitting the Protection in Armed Conflict on the 70th Anniversary of the Geneva Conventions, Document prepared by the ICRC for the 33rd International Conference of the Red Cross, Geneva 9-12 December 2019
- Law and International Human Rights Law "Similarities and Differences", Advisory services 2003.
- Olejnik L and Gisel L., The Potential Human Cost of Cyber-Operations, ICRC Expert Meeting 14-16 November, Geneva 2018
- United States/United Kingdom, Report on the Conduct of the Persian Gulf War, ICRC Casebook. Available at: https://casebook.icrc.org/case-study/united-statesunited-kingdom-report-conduct-persian-gulf-war

SECONDARY SOURCES

MONOGRAPHS AND EDITED VOLUMES

- Cassese A., "Article 51", in J.P. Cot and A. Pellet eds., La Charte des Nations Unies (The United Nation Charter), 3rd edn., 2005
- Cassese A., International Law, 2nd ed., Oxford University Press 2005
- De Vattel E., The Law of Nations, Or, Principles of the Law of Nature, Applied to the Conduct and Affairs of Nations and Sovereigns 1797, Liberty Fund, Indianapolis 2008, Book I, Ch III
- De Vattel E., Le Droit De Gens, Ou, Principes De La Loi Naturelle, Appliqués À La Conduit Et Aux Affaires Des Nations Et Des Souverains, Buffalo, New York, W. S. Hein, 1995
- International Humanitarian Law: A Handbook for Commonwealth Parliamentarians.
- O'Connel M.E., What is War? An Investigation in the Wake of 9/11, Martinus Nijhoff/Brill. edited vol. 2012
- Peter R. Mansoor, Introduction, Hybrid Warfare in History, Hybrid Warfare, Fighting Complex Opponents from the Ancient World to the Present. (W. Murray and P. Mansoor eds., 2012).

- Roberto Barsotti, 'Armed Reprisals' in Antonio Cassese edn., The Current Legal Regulation of the Use of Force, Martinus Nijhoff, Leiden 1986
- Sun Tzu, The Art of War, The Book of Lord Shang, Wordsworth Editions Limited (1998)
- Thomas Hobbes, Leviathan, I00, 1651, Michael Oakeshott eds., Collier 1962

JOURNAL ARTICLES AND CHAPTERS IN EDITED VOLUMES

- A. Cullen, The Concept of Non-International Armed Conflict in International Humanitarian Law, Cambridge University Press 2010.
- Abbas B., Prosecuting the Islamic State: The Case of a Hybrid Tribunal, Institute of Peace and Conflict Studies IPCS, 16 May 2019.
- Ahram, A., Proxy Warriors: The Rise and Fall of State-Sponsored Militias, Stanford, Stanford University Press 2011.
- Akande D., Classification of Armed Conflicts: Relevant Legal concepts, in Wilmshurst R. (ed), International Law and the Classification of Conflicts, Oxford University Press 2012.
- Akande D., Clearing the Fog of War? The ICRC's Interpretive Guidance on Direct Participation in Hostilities, Blog of the European Journal of International Law, June 2009. Available at: https://www.ejiltalk.org/clearing-the-fog-of-war-the-icrcs-interpretive-guidance-on-direct-participation-in-hostilities/
- Akande D., When Does the Use of Force Against a NOSA trigger an IAC and why does this Matter? EJIL Talk, Blog of the European Journal of International Law, October 18, 2016.
- Akande, D., Classification of Armed Conflicts: Relevant Legal Concepts, Oxford University Press, 2012 .
- Al Aridi A., An Interdisciplinary Approach to Combat ISIS: Legal, Political, and Socio-Economic, Paper presented at the International Network of Doctoral Studies in Law, 4th International Conference for PhD Students and Young Researchers: Interdisciplinary approach to Law in Modern Social Context, Vilnius April 2016.
- Al Aridi, A. The Virtual Trojan Horse in Modern Conflicts, Law, 107, doi:10.15388/Teise.2018.107.11824.
- Al Aridi, A., How Hybrid Is Modern Warfare? Conference Paper at the 5th International Conference of PhD Students and Young Researchers, International Network of Doctoral Studies in Law, Vilnius 27-28 April 2017.
- Al-Aridi A., Legal Complexities of Hybrid Threats in the Arctic Region, Teise 2019, Vol. 112
- Al-Masry A., The new face of the Syrian Electronic Army, May 17, 2018.
- Al-Ubaydi M., Combating Terrorism Ctr. At West Point, The Group calls itself a State: Understanding the Evolution and Challenges of the Islamic State, 2014.
- Albrecht Randelzhofer, "Article 51 UN Charter", in Bruno Simma (ed.), The Charter of the United Nations: A Commentary, vol. I, 2002.
- Almang J., War, Vagueness and Hybrid war, Journal of Defence Studies, 2019.
- Alvarez Ortega E., The Attribution of International Responsibility to a State for the conduct of Private Individuals within the Territory of Another State, INDRET Barcelona 2015.
- Ambos K., The Crime of Aggression after Kampala, German Yearbook of International Law, vol. 53.
- Amos C. Fox, Hybrid Warfare: The 21st Century Russian Way of Warfare, School of Advanced Military Studies, United States Army Command and General Staff College Fort Leavenworth, Kansas, 2017.
- Anand R.P., Maritime Practice in South-East Asia until 1600 A.D. and the Modern Law of the Sea, 30 International and Comp. L.Q., 1981.
- Anderson K., Explaining Hybrid Warfare in the Annual National Security Conference on February 26-27, 2016 at Duke Law School.
- Arimatsu L. and Choudhury M., The Legal Classification of the armed Conflicts in Syria, Yemen and Libya, Chatham House, March 2014.
- Aronsson-Storrier M., Article 25(3) bis. Commentary on the Law of the International Criminal Court, Case Matrix Network June 30, 2016.
- Arrocha P., An Insider's View of the Life-Cycle of Self-Defense Reports by the U.N. Member States "Challenges posed to the International Order", April 2, 2019 www.JustSecurity.org.
- At a Glance. Understanding Hybrid Threats, European Parliament Research Service (EPRS), June 2015.
- Atland K., Destined for Deadlock? Russia, Ukraine, and the unfulfilled Minsk Agreements, Vol. 36, 2020.

- Babbitt E., Responsibility to Protect: Time to Reassess, Journal of Human Rights Practice, Vol. 9, 2017.
- Bachman, S. and Mosquera A., Lawfare and Hybrid warfare- How Russia is Using the Law as a Weapon, University of Exeter Strategy and Security Institute Workshop 2015.
- Bachmann S. and Gunneriusson H., Hybrid Wars: The 21st Century's New Threats to Global Peace and Security, Scientia Militaria, South African Journal of Military Studies, Vol. 43.
- Bachmann S. and Kemp G., "Aggression as Organized Hypocrisy?" – How the War on Terrorism and Hybrid Threats challenge the Nuremberg Legacy, Windsor Yearbook of Access to Justice, Feb. 2012.
- Bachmann S., Russia's Hybrid War and its Implications for Defense and Security in the United Kingdom, Scientia Militaria, South African Journal of Military Studies, 2016, Vol. 33.
- Bachmann Sascha-Dominik and Kemp G., Aggression as Organized Hypocrisy? – How the War on Terrorism and Hybrid Threats Challenge the Nuremberg Legacy, Windsor Y B Access Just , 2012.
- Bachmann, S. and Mosquera A., Hybrid Warfare as Lawfare: Towards a Comprehensive Legal Approach, In: Cusumano E., Corbe M. (ed.) A Civil-Military Response to Hybrid Threats, Palgrave Macmillan, Cham 2018.
- Ball J., Russia's Justification for the Annexation of Crimea, Global Security Review, June 10, 2019. Available at: https://globalsecurityreview.com/russias-legal-plausible-justification-for-the-annexation-of-crimea/ .
- Barkham J., Information Warfare and International Law on the Use of Force, New York University Journal of International Law and Politics, 2001.
- Barno, D. and Banshael, N., The Irrelevance of Traditional Warfare? *War on the Rocks*, May 2016.
- Bartels, R., Timelines, Borderlines and Conflicts, International review of the Red Cross, 2009.
- Bellinger III, John B., Haynes I and William J., "A US Government Response to the ICRC Study Customary International Humanitarian Law", International Review of the Red Cross, 2007, Vol. 89.
- Benvenisti, E., The Law on Asymmetric Warfare, Martinus Nijhoff Publishers, 2010.
- Berman, N., Privileging Combat? Contemporary Conflict and The Legal Construction of War, Col. J. Trans L. I, 2004.
- Bernstein M.S., Monroy-Hernandex, Harry D., Ande P., Panovich K. and Vargas G., An Analysis of Anonymity and Ephemerality in a Large Online Community, Fifth AAAI Conference on Weblogs and Social Media, July 2011.
- Berzins J., The New Generation of Russian Warfare, Aspen Review Central Europe, 2014, Vol. 3.
- Bethlehem D., Principles of Self-Defense - A Brief Response, American Journal of International Law, 2013.
- Blackburn, A., Brannum, R.K., Turmelle, D.R., Boyette, G.T. and Napolitano, W.M. A National Policy for Deterring the Use of Weapons of Mass Destruction, Air Command and Staff College, Air University, Montgomery 1996.
- Blanchard Ch., Armed Conflict in Syria: Overview and U.S. Response, 9 October 2015.
- Blank L., A New Twist on an Old Story: Lawfare and the Mixing of Proportionalities, Case Western Reserve Journal of International Law, 2011, vol. 43.
- Blank L., Taking Distinction to the Next Level: Accountability for Fighters' Failure to Distinguish themselves from Civilians, Valparaiso University Law Review, 2012, Vol 46.
- Blount P.J., How Cyberspace Changes International Conflict, E-International Relations, December 8, 2019.
- Boelaert-Siominen S., "Grave Breaches, Universal Jurisdiction and Internal Armed Conflict: Is Customary law moving towards a uniform enforcement mechanism for all armed conflicts?" Journal of Conflict and Security Law 2000, Vol. 5.
- Bothe M., Beginning and End of Occupation, Current Challenges to the Law of Occupation, Proceedings of the Bruges Colloquium, 20-21 October 2005.
- Boulos S., The Tallinn Manual and Jus ad Bellum: Some Critical Notes, ResearchGate Publications, May 2017.
- Boystom K., International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Swedish National Defense College, Stockholm 2004.
- Brahimi A., Jihad and Just War in the War on Terror, Oxford University Press, New York 2010.
- Brands H., Paradoxes of The Gray Zone, Foreign Policy Research Institute, February 2016.
- Brenner S. and Clarke L., Civilians in Cyberwarfare: Conscripts, Vanderbilt Journal of Transnational Law, 2010, Vol. 43.
- Brenner S., Cyberthreats, The Emerging Fault Lines of the Nation State, Oxford University Press, 2009.
- Brenner S., Is there such a Thing as "Virtual Crime"? California Criminal Law Review, 2001.

- Brier-Mills M., Questioning the Utility of the Distinction between Common Articles 2 and 3 of the Geneva Conventions of 1949 since Tadic: A State Sovereignty Approach, Macquarie Law Journal, Vol 17, 2017.
- Browne A., How China Upstaged U.S. with a " Great Wall of Sand", Wall Street Journal, April 12, 2016, https://www.wsj.com/articles/how-china-upstaged-u-s-with-a-great-wall-of-sand-1460439025
- Brownlie, Principles of Public International Law, Oxford University Press 2008.
- Brunne, J., The Meaning of Armed Conflict and the Jus ad Bellum, Martinus Nijhoff Publishers, 2012.
- Buckley E. and Pascu I., "NATO's Article 5 and Russian Hybrid Warfare", *Atlantic Council* 17 March 2015, http://www.atlanticcouncil.org/blogs/natosource/nato-s-article-5-and-russian-hybrid-warfare
- Burke E., Gunness K., Cooper C., and Cozad M., People's Liberation Army Operational Concepts, RAND Corporation, Research Report 2020.
- Butrimas, V. National Security and International Policy Challenges in a Post Stuxnet World, Lithuanian Annual Strategic Review 2013-2014, Vol. 12, De Gruyter Open 2014.
- C. Macgibbon, The Scope of Acquiescence in International Law, 31 British Yearbook of International Law, 1954.
- Cambanis Th., Esfandiary D., Ghaddar S., Hanna M., Lund A. and Masour R., Hybrid Actors: Armed Groups and State Fragmentation in the Middle East, A Century Foundation Book, New York 2019.
- Cantwell, D. Hybrid Warfare: Aggression and Coercion in the Gray Zone, American Society of International Law, Nov. 29, 2017, https://www.asil.org/insights/volume/21/issue/14/hybrid-warfare-aggression-and-coercion-gray-zone
- Cantwell, D., Hybrid Warfare: Aggression and Coercion in the Gray Zone, The American Society of International Law, Vol. 21, Issue 14, November 29, 2017.
- Carey, S., Colaresi,M., and Mitchel, N., Government, Informal Links to Militias, and Accountability, Journal of Conflict Resolution 2015..
- Carl Von Clausewitz, On War, Originally Published in German As Vom Kriege, 1832, Indexed Edition Translated and Edited by Michael Howard and Peter Paret, Princeton University Press, Princeton, NJ, 1976.
- Carr J., Inside Cyber Warfare, Responding to International Cyber Attacks as Acts of War, 2nd Edition, O'Reilly Media, December 2011.
- Cassese A., The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, The European Journal of International Law, Vol. 18, 2007.
- Cf. Habermas, 'Kant's Idea of Perpetual Peace, with the Benefit of Two Hundred Years' Hindsight', Edited by J. Bohman and M. Lutz-Bachmann, Perpetual Peace: Essays on Kant's Cosmopolitan Ideal, 1997.
- Ch. Greenwood, The Law of War (IHL), MD Evans Ed., International Law, First Edition, Oxford 2003.
- Chen Lung-Chu, An Introduction to Contemporary International Law, Oxford University Press 2000.
- China Power Team. How Will the Belt and Road Initiative Advance China's Interests? CSIS, May 8, 2017, Updated August 26, 2020. https://chinapower.csis.org/china-belt-and-road-initiative/
- Chorn A. and Michiko M., Maritime Gray Zone Tactics: The Argument for Reviewing the 1951 U.S.-Philippines Mutual Defense Treaty, CSIS, October 2019.
- Chris Tuck, Hybrid War: The Perfect Enemy, Defense in Depth, Research from the Defense Studies Department, King's College London, April 25, 2017.
- Christakis T., Challenging the "Unwilling or Unable" Test, Heidelberg Journal of International Law, 2017.
- Clapham A., Brierly's Law of Nations, 7th ed., Oxford University Press, Oxford, 2008.
- Clark M., Russian Hybrid Warfare, Military Learning and the Future of War Series, Institute for the Study of War ISW, September 2020.
- Cline A., Jus Ad Bellum "Just War theory and the Pursuit of War", Learn Religions, July 2019.
- Cordesman A., U.S. Competition with China and Russia: The Crisis-Driven Need to Change U.S. Strategy, Center for Strategic International Studies CSIS, August 2020.
- Corn G. and Taylor R., Sovereignty in the Age of Cyber, American Journal of International Law, 2017.
- Corn, G., Self-defense Targeting: Blurring the Line between the Jus ad Bellum and the Jus in Bello, Non-International Armed Conflict in the Twenty-first Century, Eds. Watkin K. and Norris A., International Law Studies 2012, Vol. 88, Chapter IV.
- Courlam A., Unarmed Attacks: Cyber Combatants and the Right to Defend, The California International Law Journal, Winter 2018, Vol. 26.
- Crandall M., Soft Security Threat and Small States: The case of Estonia, Defense Studies Vol. 14, No. 1, 2014.

- Crawford E., Virtual Battlegrounds: Direct Participation in Cyber Warfare, Sydney Law School Research Paper, 2012.
- Crawford J., The Creation of States in International Law, OUP 2nd Ed., 2006.
- Crawford J., The International Law Commission's Articles on State Responsibility: Introduction, text and commentaries, Cambridge University Press, 2002.
- Crowdstrike, Observations from the Front Lines of Threat Hunting, October 2018.
- Crowe J., and Westond-Scheuber K., Principles of International Humanitarian Law, 2013.
- Cullen, P., Hybrid Threats as a New "Wicked Problem" for Early Warning, Strategic Analysis, European Centre of Excellence for Countering Hybrid Threats May 2018.
- Dalton M. and Shah H., Partners, Not Proxies, CSIS Briefs, May 2020.
- David E., Principes de Droit des Conflits Armes (The Principles of the Law of Armed Conflict), Brussels 2002, 3rd ed.
- Davis J., The Hybrid Mindset and Operationalizing Innovation: Toward A Theory of Hybrid, School of Advanced Military Studies, United States Army Command and General Staff College Fort Leavenworth, Kansas 2014.
- Davis, D., Non-State Armed Actors, New Imagined Communities and Shifting Patterns of Sovereignty and Insecurity in the Modern World, Contemporary Security Policy.
- Dayspring S., Toward A Theory of Hybrid Warfare: The Russian Conduct of War During Peace, Naval Postgraduate School, California December 2015.
- Deeks A., Is (or Was) Ukraine in a Non-International Armed Conflict, Lawfare Blog, 2014.
- Deeks A., The Geography of Cyber Conflict: Through a Glass Darkly, International Law Studies, U.S. Naval War College, 2013.
- Deeks A., Unwilling or Unable: Toward a Normative Framework for Extraterritorial Self-Defense, Virginia Journal for International Law, 2012.
- Delerue F., Civilian Direct Participation in Cyber Hostilities, Journal of the Internet, Law and Politics (IDP), University of Catalunya, October 2014.
- Delmas-Marty M., Ambiguities and Lacunae, The International Criminal Court Ten Years on, Journal of International Criminal Justice, 2013, vol.11.
- Desk W., Explainer: What is Hybrid warfare and how has China used it?, 14 September 2020.
- Deterrence by Punishment as a way of Countering Hybrid-threats: "Why we need to go beyond Resilience in the Gray Zone", MCDC Countering Hybrid Warfare Project, Information note, March 2019.
- Dinniss H., Cyber Warfare and the Laws of War, Cambridge University Press, 2012.
- Dinstein Y, War, Aggression and Self-Defense, Cambridge University Press 2005, 4th ed.
- Dinstein Y., Computer Network Attacks and Self-Defense, 2002.
- Dinstein Y., The Conduct of Hostilities under the Law of International Armed Conflict, Cambridge University Press 2004.
- Dinstein Y., The System of Status Groups in International Humanitarian Law, in International Humanitarian Law Facing New Challenges, Wolff Heintschel von Heinegg and Volker Epping eds, 2010.
- Dormann K., "The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint", ICRC 2001.
- Dormann K., The Legal Situation of "Unlawful/Unprivileged Combatants", International Review of the Red Cross, 2003.
- Dörr O., "Use of Force, Prohibition of", Max Planck Encyclopedia of Public International Law, September 2015.
- Draper, G., Humanitarianism in The Modern Law of Armed Conflicts, Cambridge, CUP 2004.
- Droege C., Get off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians, ICRC International Review 2012, Vol. 94.
- Droege C., The Geographical reach of IHL: The Law and Current Challenges, The 2015 Round Table on Current issues of International Humanitarian Law, 2015.
- Droege C., The Interplay between International Humanitarian Law and International Human Rights Law in situations of Armed Conflict, International Law Forum, University of Jerusalem, ICRC, December 2007.
- Dunlap, Charles J. Jr., Colonel, USAF, Law and Military Interventions: Preserving Humanitarian Values In 21st Conflicts, Paper Prepared for The Humanitarian Challenges in Military Intervention Conference, Carr. Ctr. for Human Rights Policy Harvard University, Washington D.C., Nov. 29, 2001.
- Durham H, Cyber Operations During Armed Conflict: 7 Essential Law and Policy Questions, ICRC Humanitarian and Law Policy, March 2020.

- Elbahu R., Deterring Violent Non-State Actors: Dilemmas and implications, Journal of Humanities and Applied Social Science 2017.
- Eve La Haye, War Crimes in Internal Armed Conflicts, Cambridge Studies in International and Comparative Law, Cambridge 2008.
- F. Hoffman, The Rise of Hybrid Wars and F. Hoffman, Hybrid Warfare and Challenges (2009) 52 Joint Force Quarterly 34-48. See Also N. Freier, The Defense Identity Crisis: It's Hybrid World (2009) 39 (3).
- Falliere N., W32 Stuxnet Dossier, Symantec Security Response, February 2011.
- Farer T., Political and Economic Coercion in Contemporary International Law, American Journal of International Law, 1985.
- Ferraro T, The ICRC's Legal Position on the Notion of Armed Conflict involving Foreign Intervention and on Determining the IHL Applicable to this type of Conflict, International Review of the Red Cross 2015.
- Ferraro T. and Cameron L., Article 2: Application of the Convention, ICRC, Commentary on the First Geneva Convention, 2016.
- Ferraro T., The Applicability and Application of International Humanitarian Law to Multinational Forces, International Review of the Red Cross 2013.
- Ferraro T., The ICRC's Legal Position on the notion of Armed Conflict involving Foreign Intervention and on determining the IHL applicable to this type of conflict, International Review of the Red Cross 2015, Vol. 97.
- Fitton O., Cyber Operations and Gray Zones: Challenges for NATO, Connections Vol. 15, no. 2, Spring 2016.
- Forney, J., Who Can We Trust with a Gun? Information Networks and Adverse Selection in Militia Recruitment, Journal of Conflict Resolution 2015.
- Fraise Th., Shades of Jihad: Variation of Military Ethics between ISIS and Al Qaeda, SciencesPo Kuwait Program, Fall 2017.
- Frank G. Hoffman A Senior Research Fellow with The Institute for National Strategic Studies, and the author of Rise of Hybrid War, Conflict of 21st century in 2007.
- Freier N., Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context, Strategic Studies Institute, May 2007.
- Frowein, J, Article 51 and the Realities of the Present-Day World, Heidelberg Journal of International Law, 2017, vol. 77.
- Gasser H.P., Internationalized non-international armed conflicts: Case studies of Afghanistan, Kampuchea and Lebanon, AMUL Review 1983, Vol 145.
- Gaudreau J., the Reservations to the Protocols Additional to the Geneva Conventions for the Protection of War Victims, International Review of the Red Cross, no. 849, March 2003.
- Geiss R., Cyber Warfare: Implications for Non-International Armed Conflict, International Law Studies, U.S. Naval War College, 2013, Vol. 89.
- Geiss R., Russia's Annexation of Crimea: The Mills of International Law Grind Slowly but they Do Grind, The U.S. Naval War College, 2015.
- Gill T., Classifying the Conflict in Syria, International Law Studies 2016, vol. 92, no 353.
- Glenn, R. W. (2009). Thoughts on "Hybrid" Conflict, in: Small Wars Journal, March 2009.
- Glenn, R., All Glory is Fleeting: Insights from the Second Lebanon War, RAND, Santa Monica 2012.
- Glennon M., The Fog of Law and the Jus Ad Bellum, The Fog of Law Series, Just Security, April 2018.
- Graja C., SOF and the Future of Global Competition, CNA, Washington 2019.
- Gray C., International Law and the Use of Force, Oxford University Press 4th ed. Oxford 2018.
- Gray C., The Protection of Nationals abroad: Russia's Use of Force in Georgia, Constantinides and Zaikos eds., The Diversity of International law 2009.
- Greco G., Cyber-Attacks as Aggression Crimes in Cyberspace in the context of International Criminal Law, European Journal of Political Science Studies, 2020, Vol. 4.
- Green L., The Contemporary Law of Armed Conflict, Juris Publishing 2008.
- Greentree T., America Did Hybrid Warfare Too, War on the Rocks, April 2015.
- Greenwood Ch., International Law and the War against Terrorism, International Law Affairs, 2002, Vol. 78.
- Grewe, W.G. The Epochs of International Law, translated and revised by Michael Byers, 2000.
- Grono N., Fragile States, and Conflict, Speech by the Deputy President of the International Crisis Group, Brussels 27th March 2010.

- Hajjar L., Lawfare and Armed Conflict: Comparing Israeli and US Targeted Killing Policies and Challenges against them, Issam Fares Institute for Public Policy and International Affairs, Research Report, Beirut 2013.
- Hakimi M., and Katz-Cogan J., The Two Codes on the Use of Force, The European Journal of International Law, vol. 27, no. 2, Oxford University Press on behalf of EJIL 2016.
- Hamdan v. Rumsfeld, United States Reports, Cases Adjudged in the Supreme Court at October term 2005, Vol. 548, Washington 2006.
- Hammes, T.X., The Sling and The Stone: On War in the 21st Century, St. Paul: MN Zenith Press, 2004.
- Handel M., Masters of War: Classical Strategic Thought, London Routledge 2001.
- Haque A., Whose Armed Conflict? Which Law of Armed Conflicts? Just Security, 4 October 2016.
- Haque, A., Necessity and Proportionality in International Law (draft), in Larry May (ed), Cambridge Handbook on Just War, 2016.
- Hashim A., State and Non-State Hybrid Warfare, Oxford Research Group "Breaking the Cycle of Violence", 30 March 2017.
- Hashim A.S., State and Non-State Hybrid Warfare, Oxford research Group, March 2017.
- Hayatli Z., Cyber Warfare in International Law, the New Jurist 2018.
- Henckaerts J-M., The Conduct of Hostilities: Target selection, proportionality and precautionary measures under international humanitarian law", in the Netherlands Red Cross, Protecting Civilians in 21st-Century Warfare: Target Selection, Proportionality and Precautionary Measures in Law and Practice, 8 December 2000.
- Henckaerts J.M, Study on Customary International Humanitarian Law: A contribution to the understanding and respect for the rule of law in armed conflict, ICRC review.
- Henry Kissinger, On China, The Penguin Press, New York 2011, Chapter 1.
- Henry S., Exploring the "Continuous Combat Function" Concept in Armed Conflicts: Time for an Extended Application, International Review of the Red Cross, 2018, Vol. 100.
- Hickey J., Challenges to Security Council Monopoly Power over the Use of Force in Enforcement Actions: The Case of Regional Organizations, 10 Ius Gentium, 2004, Vol. 75.
- Hoffman F., 'Hybrid Threats: Reconceptualizing The Evolving Character of Modern Conflict', 240 Strategic Forum, 2009.
- Hoffman F., Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies, December 2007.
- Hoffman, 'Hybrid Warfare and Challenges', 52 Joint Forces Quarterly (2009).
- Hogan J., The Future of War: Cyber-Attacks and Aggression in International Law, Portland State University 2019.
- How is the Term Armed conflict defined by International Humanitarian Law? ICRC Opinion paper, March 2008.
- Howorth J., The European Draft Constitutional Treaty and the Future of European Defense Initiative: A Question of Flexibility, 9 EUR. Foreign Affairs, 2004.
- Hrnjas, M., The United States of America and the Islamic Republic of Iran: An International Armed Conflict of Low Intensity, The Geneva Academy a Joint Center of The Graduate Insitute Geneva and University of Geneva, December 2019.
- Hsiao A., Is China's Policy to Use Force against Taiwan a violation of the Principle of Non-Use of Force under International Law, New England Law Review, 1998.
- Huber, Th., Compound Warfare: That Fatal Knot, U.S. Army Command and General Staff College Press, Fort Leavenworth, Kansas 2002.
- Hubert D. and Weiss Th., The Responsibility to Protect: Supplementary Volume to the Report of the International Commission on Intervention and State Sovereignty, International Development Research Centre, Canada 2001.
- Human Rights Watch Report, Studying Under Fire: Attacks on Schools, Military Use of Schools during the Armed Conflict in Eastern Ukraine, February 11, 2016. Available at: https://www.hrw.org/report/2016/02/11/studying-under-fire/attacks-schools-military-use-schools-during-armed-conflict#
- Hybrid Warfare, Law and The Fulda Gap, in Christopher Ford and Winston Williams (eds.), Complex Battle Spaces, 2019.
- I. Paenson, Manual of The Terminology of The Law of Armed Conflicts and of International Humanitarian Organizations, Bruylant Nijhoff, 1989.
- Iain Scobbie, Lebanon 2006, International Law and the Classification of Conflicts, Edited by Elizabeth Wilmshurst, Chatham House, Oxford University Press, 2012.

- ICISS, The Responsibility to Protect, Ottawa International Development Research Centre, December 2001
- Ignatieff, M., The Warrior's Honor: Ethic War and Modern Conscience, Holt Paper Backs, New York 1998.
- International Humanitarian Law: A Handbook for Commonwealth Parliamentarians, Commonwealth Parliamentary Association (CPA), September 2019.
- Jean Marie Henckaerts and Louise Doswald-Beck, Customary International Humanitarian Law, Vol. I, ICRC 2009.
- Jensen T and Watts S., A cyber Duty of Due Diligence: Gentle Civilizer or Crude Destabilizer? Texas Law Review 2017, Vol 95.
- Johnson, D., the Problem of the Terror Non-State: Rescuing International Law from ISIS and Boko Haram, Brooklyn Law Review, Vol. 84, January 2019.
- Jordan l., Hybrid War: Is the US Army Ready for the Face of 21st Century Warfare, US Army Command and General Staff, 2008.
- Joseph Needham and Robin D. S. Yates, Science and Civilization in China, Vol. 5, Part 6: "Military Technology Missiles and Sieges", Cambridge University Press, Cambridge 1994.
- Joyce S., Along a Shifting Border, Georgia and Russia maintain an Uneasy Peace, NPR 2017, https://www.npr.org/sections/parallels/2017/03/13/519471110/along-a-shifting-border-georgia-and-russia-maintain-an-uneasy-peace?t=1611156869557
- Joyner Ch., and Lotrionte C., Information Warfare as International Coercion: Elements of a Legal Framework, European Journal of International Law ed. 12, 2001.
- Kahn J., Hybrid Conflict and Prisoners of War: The Case of Ukraine (2018). Lieber Institute for Law and Land Warfare Book Series - Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare, ed. by Christopher M. Ford and Winston S. Williams, Oxford University Press, 2018, Forthcoming, SMU Dedman School of Law Legal Studies Research Paper No. 381.
- Kania E., The PLA's Latest Strategic Thinking on the Three Warfare, The Jamestown Foundation, August 2016, Vol. 16, issue 13.
- Kapusta Ph., United States Special Operations Command, White paper: The Gray Zone, September 9, 2015.
- Kelley M., Challenges to Compliance with International Humanitarian Law in the Context of Contemporary Warfare, SIT Graduate Institute, Spring 2013.
- Kemp, G. The Shift from Jus Ad Bellum to Jus Contra Bellum: The Prohibition of the Use of Force in Normative and Institutional Perspective. In Individual Criminal Liability for the International Crime of Aggression, Intersentia Publication, 2015.
- Kenneth Yeager v. The Islamic Republic of Iran, Iran-U.S. C.T.R. of 1987, vol. 17.
- Kilovaty I., ICRC, NATO and the U.S.: Direct Participation in Hacktivities, targeting Private Contractors in Cyberspace under the Law of Armed Conflict, Duke Law and Technology Review, 2016.
- Kimberley T., State responsibility for International terrorism, Oxford University Press 2011.
- Korhonen, O., Deconstructing the Conflict in Ukraine: The Relevance of International Law to Hybrid States and Wars, German Law Journal 2015, vol. 16.
- Kowalski M., Armed Attack, Non- State Actors and a Quest for the Attribution Standard, Polish Yearbook of International Law 2010, Vol. 30.
- Kreb C., A Collective Failure to Prevent Turkey's Operation "Peace Spring" and NATO's Silence on International Law, Blog of the European Journal of International Law, October 2019.
- Kress C., On the Principle of Non-Use of Force in Current International Law, Just Security at Reiss Center on Law and Security, New York September 2019.
- Kress C., On the Principle of Non-Use of Force in Current International Law, Just Security, September 2019, https://www.justsecurity.org/66372/on-the-principle-of-non-use-of-force-in-current-international-law/
- Kretzmer D., The Inherent Right to Self-Defence and Proportionality in Jus Ad Bellum, The European Journal of International Law 2013, Vol. 24.
- Kuzio T. and D'Anieri P., Annexation and Hybrid Warfare in Crimea and Eastern Ukraine, E-International Relations, June 25, 2018. Available at: https://www.e-ir.info/2018/06/25/annexation-and-hybrid-warfare-in-crimea-and-eastern-ukraine/
- Langford, I. Finding Balance between the Conventional and Unconventional in Future Warfare, The Strategy Bridge, 4 December 2018 https://thestrategybridge.org/the-bridge/2018/12/4/finding-balance-between-the-conventional-and-unconventional-in-future-warfare
- Le Hucheng and Zhang Yucheng, "The Utility and Position of Legal Warfare in the Preparation for Military Conflict", Liu and Liu, Xin Junshi Geming Yu Fazhi Jianshe 2002.

- Lekas A., ISIS: The Largest Threat to World Peace Trending Now, Emory International Law Review, 2015-2016, vol. 30.
- Levitin M., The Law of Force and the Force of Law: Grenada, the Falklands, and Humanitarian Intervention, Harvard International Law Journal, 1986, Vol. 27.
- Lewicki, W. Hybrid Warfare in Ukraine- A New Way of Waging War, Articles published at the International Conference: "Hybrid Warfare in Ukraine: Outcomes and Recommendations for Europe and the World", Piotrkow Trybunalski, Poland 2016.
- Lillich R., Forcible Self-Help by States to Protect Human Rights, Iowa Law Review, 1967, Vol. 53.
- Liu I.Y., The Due Diligence Doctrine under Tallinn Manual 2.0, Computer Law and Security Review 2017, Vol. 33.
- Lobel J., The Use of Force to Respond to Terrorist Attacks: The Bombing of Sudan and Afghanistan, Yale Journal of International Law 1999.
- Lotrionte C., State Sovereignty and Self-Defense in Cyberspace: A Normative Framework for balancing Legal Rights, Emory International Law Review, Vol. 26, 2012.
- Lovat H., Negotiating Civil War, The Politics of International Regime Design, Cambridge University Press 2020.
- LTG. Keith B. Alexander, Hearings before the Committee on Armed Services, United States Senate, 111th Congress, Second Session April 2010.
- Luban D., "Just War and Human Rights" Philosophy and Public Affairs 1980, Vol. 9.
- Lubell N., Extraterritorial Use of Force Against Non-State Actors, Oxford Scholarship Online 2010, Part II, Ch. 14.
- Lubell N., Fragmented Wars, Multi-Territorial Operations against Armed Groups, Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare, Oxford University Press, Lieber Series, 2019, Vol 1
- M. Fried, Austro-Hungarian War Aim in The Balkan's During World War I, 2014.
- Macdonald Ch., The Science of War: Sun Tzu's Art of War re-translated and re-considered, Earnshaw Books Ltd, ed. 2017.
- Maganza B., Which role for Hybrid entities involved in multi-parties NIACs? Applying the ICRC's support-based approach to the armed conflict in Mali, Questions of International Law Journal, May 31, 2019, Vol. 59.
- Mark Galeotti, "The 'Gerasimov Doctrine' and Russian Non-Linear War," In Moscow's Shadows (blog), 6 July 2014.
- Martin C., Challenging and Refining the "Unwilling or Unable Doctrine", Vanderbilt Journal of Transnational Law 2019, Vol.52.
- Martin C., Challenging and Refining the "Unwilling or Unable" Doctrine, Vanderbilt Journal of Transnational Law, 2019.
- Mary Ellen O'Connell, Myths of Hybrid Warfare, The Centre of Ethical Education in the Armed Forces, 2015 http://www.ethikundmilitaer.de/en/full-issues/20152-hybrid-warfare/oconnell-myths-of-hybrid-warfare/
- Mary Ellen O'Connell, What is War? An Investigation in the Wake of 9/11, International Humanitarian Law Series, Martinus Nijhoff Publishers, Boston 2012.
- Mattessich W., Digital Destruction: Applying the Principle of Non-Intervention to Distributed Denial of Service Attacks Manifesting no Physical Damage, Colombia Journal of Transnational Law 54, 2016.
- Mazar M., Mastering the Gray Zone: Understanding a Changing Era of Conflict, US Army War College, Strategic Studies Institute, December 2015.
- MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, Multinational Capability Development Campaign MDCD, January 2017.
- Mcdonald N., The Role of Due Diligence in International Law, Cambridge University Press for the British Institute of International and Comparative Law, 2019.
- Melzer N., Civilian Participation in Armed Conflict, Max Planck Encyclopedia of International Law, February 2010..
- Melzer N., Cyber Warfare and International Law, United Nations Institute for Disarmament Research, 2011.
- Melzer N., Interpretive Guidance on the Notion of Direct participation in Hostilities under International Humanitarian Law, ICRC, Geneva 2009.
- Melzer N., Keeping the Balance between Military Necessity and Humanity: A response to four critiques of the ICRC's Interpretive Guidance on the Notion of Direct Participation in Hostilities, International Law and Politics Journal, Vol. 42, 2010.
- Menachem Feder N., Reading the UN Charter Connotatively: Toward a New Definition of Armed Attack, New York University Journal of International Law and Politics, 1987.

- Mendoza J., Cyber Attacks and the Legal Justification for an Armed Response, School of Advanced Military Studies, Kansas 2017.
- Meron Th., On the Inadequate Reach of Humanitarian and Human Rights Law and the Need for a New Instrument, 77 AM. J. INT'L L. 554, 592 (1983).
- Micheal Schmitt & Liis Vihul, Proxy wars in Cyberspace: The Evolving International Law of Attribution, Fletcher Security Review | Vol I, Issue II Spring 2014.
- Milanovic M., The Lost Origins of Lex Specialis: Rethinking the relationship between Human Rights and International Humanitarian Law, Ohlin Ed., in Theoretical Boundaries of Armed Conflict and Human rights, ASIL Studies in International Legal Theory, Cambridge University Press 2016.
- Milanovic, M., Self-Defense and Non-State Actors: Indeterminacy and the Jus ad Bellum, Blog of the European Journal of International Law, February 2010.
- Mills C., France and Article 42(7) of the Treaty on the European Union, House of Commons Library, Commons Briefing papers CBP-7390, November 18, 2015.
- Miracola S., Chinese Hybrid Warfare, The Italian Institute for International Political Studies ISPI, 21 December 2018. Available at: https://www.ispionline.it/it/pubblicazione/chinese-hybrid-warfare-21853
- Miracola, S. Commentary: Chinese Hybrid Warfare, Italian Institute for International Political Studies, Rome December 2018, https://www.ispionline.it/en/pubblicazione/chinese-hybrid-warfare-21853
- Moir L., The Law of Internal Armed Conflict, "Memorandum of 22 March 1996 to the Preparatory Committee for the Establishment of the ICC", Cambridge University Press 2000.
- Moir L., The Law of Internal Armed Conflict, Cambridge University Press, 2002.
- Monaghan A., the "War" in Russia's "Hybrid Warfare", Parameters, Vol. 45, no. 4, Winter 2015.
- Moseley A., "Just War Theory", the Internet Encyclopedia of Philosophy 2009.
- Mosquera A. and Bachmann S., Lawfare in Hybrid Wars: The 21st Century Warfare, Journal of International Humanitarian Legal Studies, Brill-Nijhoff, Vol.7, March 2016.
- Mosquera A. and Bachmann S., Understanding Lawfare in a Hybrid Warfare Context, Articles on NATO Current Challenges, NATO Legal Gazette, October 2016.
- Moynihan H., the Application of International Law to State Cyber-attacks Sovereignty and Non-intervention, Chatham House, International Law Program December 2019.
- Moynihan H., The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention, Chatham House, 2019.
- Mumford A., Proxy Warfare and the Future of Conflict, The RUSI Journal 2013.
- Mumford, A., McDonald, J., Ambiguous Warfare, Report produced for the DCDC, October 2014.
- NATO vs. Russia: How to Counter the Hybrid Warfare Challenge, The National Interest, July 2016.
- Neff, S., War and the Law of Nations. Cambridge University Press, Cambridge 2008.
- Newton, M., Illustrating Illegitimate Lawfare, Case Western Reserve Journal of International Law, 2010, Vol. 43.
- Nicholas Morrow, Sun Tzu, The Art of War (500-300 B.C.), John Hopkins University SAIS, Classics of Strategy and Diplomacy, November 24, 2015.
- Nordstrom C., The Regulation of Cyber Operations Below the Threshold of Article 2(4) of the Charter: An Assessment of Rule 4 of the Tallinn Manual 2.0, Master's Thesis in Public International Law, University of Uppsala, 2019.
- Nye, Joseph S., International Norms in cyberspace, Project Syndicate, 11 May 2015.
- O'Keefe R., The Protection of Cultural Property in Armed Conflict, Cambridge University Press 2006.
- Oppenheim L., Oppenheim's International Law, Vol. 1, 9th ed., Jennings, R. Y. and Watts, A.,New York 1996.
- Ottis R., Proactive Defense Tactics On-Line Cyber Militia, in the proceedings of the 9th European Conference on Information Warfare and Security (ECIW 2010) Thessaloniki - Greece, July 2010.
- Owens W., Dam K and Lin H. (eds), Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyber-Attack Capabilities, The National Academic Press 2009.
- Owens, M., Reflection on Future War, Naval War College Review 2008.
- Peter R. Mansoor, Introduction, Hybrid Warfare in History, Hybrid Warfare, Fighting Complex Opponents from the Ancient World to the Present, W. Murray and P. Mansoor eds., 2012.
- Petras Ch., The Law of Air Mobility- The International Legal Principles behind the U.S Mobility Air Forces, Air Force Law Review, 2010.
- Pfaff A., Strategic Insights: Proxy War Norms, Strategic Studies Institute, The United States Army War College Press, December 2017.
- Pietro Verri, Dictionary of The International Law of Armed Conflict, International Committee of the Red Cross, Geneva 1999.
- Piper D., The General Problem of Defining Aggression: The Legal Control of the Use of Force and the Definition of Aggression, Georgia Journal of International and Comparative Law, 1972.

- Potcovaru A., The International Law of Anticipatory Self-defense and US options in North Korea, 8 August 2017. https://www.lawfareblog.com/international-law-anticipatory-self-defense-and-us-options-north-korea
- Poznansky M., The United Nations and the Accidental Rise of Covert Intervention, Lawfare Blog, June 2020.
- Prescott J., Direct Participation in Cyber Hostilities: Terms of Reference for Like-Minded States, 4th International Conference on Cyber Conflict, NATO CCD COE Publications, Tallinn 2012.
- Provost R., International Human Rights and Humanitarian Law, Cambridge University Press, 2002
- Quenivet N. and Shah-Davis S., International Law and Armed Conflict, Challenges in the 21st Century, T.M.C Asser Press, Hague 2010.
- Qureshi W., International Law and The Application of the Unwilling or Unable Test in the Syrian Conflict, Drexel Law Review, 2018.
- RA Falk, Janus Tormented: The International law of Internal War, International Aspect of Civil Strife, Princeton University Press, 1964.
- Randelzhofer A., Article 51 in Bruno Simma (ed), The Charter of the United Nations: A Commentary, Oxford University Press, 2002.
- Rasevic Z., "Cyber Warfare and International Cyber Law: Whither?", Journal of Criminology and Criminal Law, Belgrade 2020.
- Rath B., The Virtues of Bright Lines: Self-Determination, secession, and External Intervention, German Journal of Law 2015.
- Rattan J., Changing Dimensions of Intervention Under International Law: A Critical Analysis, Sage Open, June 2019.
- Rauta V., Towards a Typology of Non-State Actors in Hybrid Warfare: Proxy, Auxiliary, Surrogate and Affiliated Forces, Cambridge Review of International Affairs, September 2019.
- Reeves Sh. And Barnsby R., the New Griffin of War "Hybrid International Armed Conflicts", Harvard International Review 2013.
- Reichborn-Kjennerud, E., Cullen, P., What is Hybrid Warfare? Norwegian Institute of International Affairs, Policy Brief 2016.
- Reilly M., Hybrid Threat Center of Gravity Analysis: Taking a Fresh Look at ISIL, National Defense University Press, January 26, 2017.
- Reinold, Th., "State Weakness, Irregular Warfare, and the Right to Self-Defense Post- 9/11", American Journal of International Law, Vol. 105.
- Reisman W. and Armtsrong A., "The Past and Future of the Claim of Pre-emptive Self-Defense", Yale Law School Legal Scholarship Repository, 2006.
- Riamei L., The Kurdish Question: Identity, Representation and the Struggle for Self-Determination, 2015.
- Richard A. Clarke and Robert Knake, Cyber War: The Next Threat to National Security and What to Do About It, 2010.
- Roguski P., France's Declaration on International Law in Cyberspace: The Law of Peacetime Cyber Operations, Part I, Opinio Juris, 24 September 2019.
- Roling B., Criminal Responsibilities for Violations of the Law of War, Revue Belge de Droit International, 1976.
- Ronen, Israel, Hizbollah and the Second Lebanon War, 9th Yearbook on International Humanitarian Law, 2006.
- Ronen, Y., "Israel, Hezbollah, and the Second Lebanon War", Yearbook of International Humanitarian Law, Vol. 9, 2006.
- Rudderhof, R., From Classic Wars to Hybrid Warfare, Peace Palace Library, July 27, 2017. https://www.peacepalacelibrary.nl/2017/07/from-classic-wars-to-hybrid-warfare/
- Ruys T., Armed Attack and Article 51 of the UN Charter: Evolutions in Customary law and Practice, Cambridge University Press, New York, 2013.
- Ruys T., The Meaning of Force and the Boundaries of the Jus Ad Bellum- Are "Minimal", Uses of force excluded from UN Charter 2(4), The American Journal of International Law, 2014.
- Sandesh Sivakumaran, the Law of non-International Armed Conflict, OUP Oxford, 2012.
- Sandoz et al. (eds), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, Geneva ICRC 1987.
- Sandoz Y., Swinarski CH. And Zimmerman B. (eds), Commentary on the Additional Protocols, ICRC, Geneva 1987.
- Sari A., and Laura A., Hybrid Threats and the United States National Security Strategy: Prevailing in an "Arena of Continuous Competition", Blog of the European Journal of International Law, January 2018.

- Sari A., Dear Geneva: Let's Talk Hybrid Warfare. A Reality Check, Conference Presentation at Geneva Centre for Security policy (GCSP), 2019.
- Sari A., Hybrid Law, Complex Battlespaces: What's the Use of a Law of War Manual?, in Michael A. Newton ed., The United States Department of Defense Law of War Manual: Commentary and Critique, 2019.
- Sari A., Hybrid Threats and the Law: Concepts, Trends and Implications, Hybrid CoE Trend Report 3, April 2020.
- Sari A., Legal Aspects of Hybrid Warfare, Lawfare Blog October 2015, https://www.lawfareblog.com/legal-aspects-hybrid-warfare
- Sari A., The Council of Europe's Parliamentary Assembly takes on the Legal Challenges of Hybrid Warfare, Lawfare Blog May 2018.
- Sari A., The Mutual Assistance Clauses of the North Atlantic and EU Treaties: The Challenge of Hybrid Threats, Harvard National Security Journal 2019, Vol. 10.
- Sari, A. Blurred Lines: Hybrid Threats and the politics of International law, Strategic Analysis, Hybrid COE 2018.
- Sari, A. Workshop on Legal aspects of Hybrid Warfare, The University of Exeter's Strategy and Security Institute, 16-17 September 2015.
- Sari, A., Hybrid Warfare, Law, and the Fulda Gap, Complex Battle Spaces, The Law of Armed Conflict and the Dynamics of Modern Warfare, Lieber Series, Volume I, Ed. Christopher Ford and Winston Williams, Oxford University Press 2019.
- Sassoli M., Legitimate Targets of Attacks under International Humanitarian Law, Harvard Program on Humanitarian Policy and Conflict Research, June 2003.
- Sassoli Mand Bouview A., How Does Law Protect in War? International Review of the Red Cross, Geneva 1999.
- Sassoli, M. Engaging Non-State Actors: The New Frontier for International Humanitarian Law. In: Exploring Criteria & Conditions for Engaging Armed Non-State Actors to Respect Humanitarian Law and Human Rights Law. Geneva: PSIO, UNIDIR, Geneva Call, 2008.
- Savita M. and Manisha P., A brief study of WannaCry threat: Ransomware attack 2017, International Journal of Advanced Research in Computer Science.
- Schlichte, K., With the State against the State? The Formation of Armed Groups', Contemporary Security Policy 2009.
- Schmitt M. and Vihul l., Respect for Sovereignty in Cyberspace, Texas Law Review, Vol. 95, Issue 7, 2017.
- Schmitt M. and Watts S., Beyond State-Centrism: International Law and Non-state Actors in Cyberspace, journal of Conflict and Security law Published by Oxford University Press 2016.
- Schmitt M., Charting the Legal Geography of NIAC, International Law Studies, U.S. Naval War College, 2014, Vol. 90.
- Schmitt M., Classification of Cyber Conflict, Journal of Conflicts and Security Law, 2012.
- Schmitt M., Deconstructing Direct Participation in Hostilities: The Constitutive Elements, New York Journal for International Law and Politics, 2010.
- Schmitt M., France's Major Statement on International Law and Cyber: An Assessment, Just Security, 16 September 2019.
- Schmitt M., Germany's Positions on International Law in Cyber Space, Part II, Just Security, March 2021. https://www.justsecurity.org/75278/germanys-positions-on-international-law-in-cyberspace-part-ii/
- Schmitt M., The Impact of High Tech and Law Tech Warfare on Distinction, in International Humanitarian Law and the 21st Century's Conflicts: Changes and Challenges, 2005.
- Schmitt M., The Law of Cyber Targetting: Tallinn Paper No. 7, Naval War College- Stockton Center for the Study of International Law, January 2015.
- Schmitt M., The Status of Opposition Fighters in a Non-International Armed Conflict, In Non-International Armed Conflict in the Twenty-First Century, U.S. Naval War College International Law Studies, 2012.
- Schmitt M., Virtual Disenfranchisement: Cyber Election Meddling in the Grey Zones on International Law, Chinese Journal of International law, ed. 19, 2018.
- Schmitt M., Wired Warfare 3.0.: Protecting the Civilian Population during Cyber Operations, International Review of the Red Cross, 2019, Vol. 1010.
- Schmitt, M., Cyber Operations and the Jus ad bellum revised, Villanova Law Review 2011, Vol. 56.
- Schmitt, M., Gray Zones in the International Law of Cyberspace, the Yale Journal of International Law, 2017.
- Schmitt, M., The Law of Cyber Warfare: Quo Vadis? Stanford Law and Policy Review, Vol. 25.

- Schondorf R., “Extra-state armed conflicts: is there a need for a new legal regime?”, New York University Journal of International Law and Politics, Vol. 37, No. 1, 2004.
- Schreuer C., “The Waning of the Sovereign State: Towards a New Paradigm for International Law?” European Journal of International Law 1993.
- Schwarzenberger g., International Law: As Applied by International Courts and Tribunals, The Law of Armed Conflicts, Cambridge University Press 2004.
- Scobbie, Words My Mother Never Taught Me- In Defense of the International Court, American Journal of International Law (AJIL), 2005.
- Sigholm J., Non-state Actors in Cyberspace Operations, Swedish National Defence College, 2016.
- Simma Br., the Charter of the United Nations: A Commentary, Oxford University Press 2012.
- Simon, H., The Myth of Liberum Jus ad Bellum: Justifying War in the 19th Century Legal theory and Political practice, The European Journal of International Law, Vol. 29 no. 1, Oxford University Press 2018.
- Simpson, E., Clausewitz’s Theory of War and Victory in Contemporary Conflict, Exploring War’s Character and Nature, 2018.
- Smith, R., The Utility of Force, The Art of War in the Modern World, Vintage Books, 2007.
- Somer J., Acts of Non-state Groups and the Law governing Armed Conflict, American Society of International Law Insights, 2006.
- Sorensen H. and Back-Nyemann D., Going Beyond Resilience: A Revitalized Approach to Countering Hybrid Threats, Strategic Analysis, Hybrid COE November 2018.
- Spector P., In Defense of Sovereignty, in the wake of Tallinn 2.0, American Journal of International law Unbound 2017.
- Stahn, C. “Jus ad Bellum, Jus in Bello , Jus post Bellum: Rethinking the Conception of the Law of Armed Force”, European Journal of International Law, Volume 17, Issue 5, 1 November 2006.
- Starski P., Right to Self-Defence, Attribution and the Non-State Actor- Birth of the “Unable and Unwilling” Standard, Heidelberg Journal of International Law, Sept. 2015.
- Stewart J., Towards a Single Definition of Armed Conflict in International Humanitarian Law: A Critique of Internationalized Armed Conflict, International Review Red Cross 2003.
- Sun Tzu, The Art of War, Trans. John Minford, New York: Viking, 2002.
- Talmon S., The Various Control Tests in the Law of State Responsibility and the Responsibility of Outside Powers for Acts of Secessionist, Legal Research Paper Series no. 16, University of Oxford 2009.
- Tams, Ch., “The Use of Force against Terrorists”, European Journal of International Law EJIL 2009.
- Tancredi A., The Russian Annexation of the Crimea: Questions relating to the use of force, QIL, Zoom out I, 2014.
- The Judge Advocate General’s Legal Center and School, International and Operational Law Department, Operational Law Handbook, Charlottesville 2008.
- Thurer D., The “Failed State” and International Law, ICRC 31st December 1999, No. 836.
- Torossian B., Fagliano L., and Gorder T., Hybrid Conflict “Neither war nor Peace”, Strategic Monitor 2019, https://www.hcss.nl/pub/2019/strategic-monitor-2019-2020/hybrid-conflict/
- Treverton G., Thvedt A., Chen A., Lee K., and McCue M., Addressing Hybrid Threats, Swedish Defense University and the authors 2018.
- Trinkunas H. and Clunan A., Alternative Governance in Latin America, Routledge Handbook of Latin American Security, vol. 99.
- Turkgenci Y., and Sayatt H., “Command and Control”, Shifting Paradigm of War: Hybrid Warfare, Turkish National Defense University, Istanbul 2017.
- Turns D., Cyber Warfare and the Notion of Direct Participation in Hostilities, Journal of Conflict and Security Law, Oxford University Press 2012.
- United Arab Emirates: A Global Perspective on the Crimes of Aggression, STA Law Firm, 12 March 2019.
- United Kingdom Ministry of Defense, The Manual of the law of Armed Conflict, Oxford University Press 2004.
- Valek P., Is Unilateral Humanitarian Intervention Compatible with the UN. Charter?, Michigan Journal of International Law, 2005, vol. 26.
- Valjataga A., Tracing opinion Juris in National Cyber Security Strategy Documents, NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE), Tallinn 2018.
- Vark R., Legal Complexities in the Service of Hybrid Warfare, Kyiv- Mokyla and Politics Journal 2020, vol. 6.
- Vark R., State Responsibility for Private Armed Groups in the Context of Terrorism, Juridica International, XI, 2006, April 23, 2020.

- Verri, P., Dictionary of The International Law of Armed Conflict, International Committee of The Red Cross, Geneva 1992.
- Vincze V., Taming the Untamable: The Role of Military Necessity in Constraining Violence, ELTE Law Journal 2013.
- Vite S., Typology of Armed Conflicts in International Humanitarian Law: Legal concepts and actual situations, International Review of Red Cross, vol. 91, number 873, March 2009.
- Vlasiuk V., Hybrid War, International Law and Eastern Ukraine, European Political and Law Discourse, Vol. 2, Issue 4, 2015.
- Von Bernstorff J., Drone Strikes, Terrorism and the Zombie: On the Construction of an Administrative Law of Transnational Executions, European Society of International Law (ESIL) Reflections, 2016.
- Von Clausewitz, C., On War 1830, edited and translated by M. Howard and P. Paret, Princeton University Press, New Jersey 1976..
- Von Hirsch, Proportionality in the Philosophy of Punishment, Crime and Justice 1992, Vol. 16.
- Voyger, M. Lawfare- the forgotten element of Russia's hybrid war against the West, Baltic Defense College Tartu Estonia, 22 December 2018, https://www.integrityinitiative.net/articles/lawfare-forgotten-element-russias-hybrid-war-against-west
- Wallace D. and Reeves Sh., The Combatant Status of the "Little Green Men" and Other Participants in the Ukraine Conflict, International Law Studies, U.S. Naval War College, 2015, Vol. 91.
- Wallace D., McCarthy A. and Reeves Sh., Trying to Make Sense of the Senseless: Classifying the Syrian War under the Law of Armed Conflict, Michigan State International Law Review 2017.
- Walzer, M., Just and Unjust Wars: A Moral Argument with Historical Illustrations, 4th ed., Basic Books New York 2006.
- Warren J., Not All Wars are Violent "Identifying Faulty Assumptions for the Information War", Air and Space Power Journal, Winter 2020.
- Watkin K., Controlling the Use of Force: A Role for Human Rights Norms in Contemporary Armed Conflict, American Journal for International Law, 2004.
- Watkin, K., Warriors Without Rights? Combatants, Unprivileged Belligerents, and the Struggle Over Legitimacy. Harvard University Program on Humanitarian Policy and Conflict Research Occasional Papers, 2005.
- Watt, K. Ethics and Hybrid War, The Security Distillery, April 2019.
- Watts, S., Combatant Status and Computer Network Attacks, Virginia Journal of International Law, 2012, Vol. 50.
- Waxman M., Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), The Yale Journal of International Law, 2011, Vol. 36..
- Waxman M., The Caroline Affairs in the Evolving International Law of Self-Defense, 28 August 2018, https://www.lawfareblog.com/caroline-affair
- Weill S., Building respect for IHL through National Courts, ICRC review, 2014, vol. 96.
- Wheatley S., Regulating the Frontiers of Hybrid-Warfare: The International Law on Foreign State Cyber Operations Targeting Democracy, Presented at Conference on "New technologies: New Challenges for Democracy and International Law", University of Cambridge, March 2019..
- Williams P. and Pearlman S., Use of Force in Humanitarian Crises: Addressing the Limitations of UN Security Council Authorization, American University Washington College of Law, 2019.
- Williamson, S., From Fourth Generation Warfare to Hybrid War, U.S. Army War College, Carlisle Barracks, USAWC Class of 2009.
- Wingfield T., The Law of Information Conflict: National Security Law in Cyberspace, Ageis Research Corporation, 2000.
- Wittes B., What is Hybrid Conflict, Lawfare blog, 2015. https://www.lawfareblog.com/what-hybrid-conflict
- Wolf Von Heinegg, Robert Frau And Tassilo Singer, Dehumanization of Warfare "Legal Implications of New Weapon Technology" Springer International Publishing, 2018.
- Work of Grotius or Pufendorf in KA Hessbruegge, The Historical Development of the Doctrines of Attribution and Due Diligence in International Law , New York University Journal of International Law and Politics, 2003, Vol. 265.
- Wortzel L., The Chinese People's Liberation Army, and Information Warfare, United States Army War College Press, March 2014.
- Yoram Dinstein, Non-International Armed conflicts in International Law, Cambridge University Press, 2014
- Yuen D., "Deciphering Sun Tzu", Comparative Strategy 2008, Vol. 27.
- Zollman,J. Naulila 1914, World War I in Angola and International Law: A Study in Post-Colonial Border Regimes and Interstate Arbitration, 2016.

MANUALS, MILITARY DOCTRINES AND CONFERENCES

- A Multinational Capability Development Campaign Project, (MCDC Project), Countering Hybrid Warfare, MCDC, February 2019.
- Announcement of the Aircraft Identification Rules for the East China Sea Air Defense Identification Zone of the People's Republic of China, 13 November 2013
- Application of International Humanitarian Law and International Human Rights Law in an Armed Conflict, Conference by the International Institute of Humanitarian Law, San Remo - Italy 2019.
- Department of Defense, Quadrennial Defense Review Report, Washington, DC: Department of Defense, 2010
- Joint Publication 1-02, Department of Defense: Dictionary of Military and Associated Terms, 8 November, 2010 (Amended through 15 February 2016).
- Letter from the Chief of Naval Operations (Burke) to the United Secretary of State for Political Affairs, Washington 1960 Foreign Relations of the United States, 1958-1960, Cuba, Vol. VI.
- Measures to Eliminate International Terrorism, Statement by the Permanent Mission of the El Salvador to the United Nations on behalf of the Community of Latin American and Caribbean States (CELAC), New York, 3 October 2018
- Ministry of Defence, Deterrence: The Defence Contribution, JDN 1/19, Development, Concepts and Doctrine Centre, Shrivenham 2019
- Munich Security Conference Broadened the Hybrid Concept to Include Diplomatic, Information, Military, Economic, Financial, Intelligence and Law Enforcement
- Office of the General Counsel, U.S. Department of Defense, Law of War Manual 63, December 2016
- Organization for Security and Cooperation in Europe, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyber Space, 2013.
- Panetta L., Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security, New York City, 11 October 2012, United States Department of Defense
- Tallinn Manual on the International Law Applicable to Cyber Warfare 2.0, Schmitt M. and Vihul ed., prepared by the International Group of Experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence, Cambridge University Press 2013
- White House Memorandum of February 7, 2002 on the "Humane treatment of Talban and AL Qaeda detainees", available online: http://www.pegc.us/archive/White_House/bush_memo_20020207_ed.pdf

NEWS ARTICLES

- "White House will not commit to asking Congress for Syrian Strike", The Hill, 25 August 2014. https://thehill.com/policy/defense/215905-white-house-wont-commit-to-asking-congress-for-syria-strike
- Ackerman S., MacAskill E. and Ross A., "Junaid Hussain: British hacker for ISIS believed killed in US air strike", The Guardian, 27 August 2015
- Blair D., Estonia Recruits Volunteer Army of "Cyber Warriors", The Telegraph, 26 April. 2015.
- Branigan T., Google to end Censorship in China over Cyber Attacks, The Guardian, 12 Jan. 2010
- Butler D., Kurds' Advance in Syria Divides U.S. and Turkey as Russia Bombs, Reuters, February 17, 2016. https://www.reuters.com/article/us-mideast-crisis-syria-kurds-idUSKCN0VQ1FR
- Gearan A., "U.S. rules out coordinating with Assad on airstrikes against Islamists in Syria", Washington Post, 26 August 2014. Available at: https://www.washingtonpost.com/world/national-security/us-rules-out-coordinating-with-assad-on-airstrikes-against-islamists-in-syria/2014/08/26/cda02e0e-2d2e-11e4-9b98-848790384093_story.html
- Gerasimov V., The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations, Voyenno-Promyshlenny Kurier (VPK News), February 26, 2013
- Markoff J, Before the Gunfire, Cyberattacks, New York Times, 2008. https://www.nytimes.com/2008/08/13/technology/13cyber.html
- McGuinness D., How a Cyber-attack transformed Estonia, 22 April 2017. https://www.bbc.com/news/39655415
- MH17: Four charged with shooting down plane over Ukraine, BBC News 19 June 2019, https://www.bbc.com/news/world-europe-48691488

- Online Article “Putin says those aren’t Russian forces in Crimea” March 4, 2014. https://www.npr.org/sections/thetwo-way/2014/03/04/285653335/putin-says-those-arent-russian-forces-in-crimea?t=1590235318330&t=1609180949360
- Russian defense commentator Viktor Likovkin, A statement in Nezavisimoe Voennoe Obozrenie, 10 July 2015.
- Russian Hackers Acted to Aid Trump in Election, U.S. says, The New York Times, December 2016, https://www.nytimes.com/2016/12/09/us/obama-russia-election-hack.html?rref_collection%2Fnewseventcollection%2Frussian-election-hacking&action_click&contentCollection_politics&region_rank&module_package&version_highlights&contentPlacement=4&pgtype_collection
- Sciutto J, Crawfor J. and Carter CH., ISIS can Muster between 20,000 and 31,500 Fighters, CIA says, CNN September 12, 2014. http://edition.cnn.com/2014/09/11/world/meast/isis-syria-iraq/
- Shachtman N., Wage Cyberwar against Hamas, Surrender Your PC- Wired 8 January 2009. https://www.wired.com/2009/01/israel-dns-hack/
- Shubert A., Cyber warfare: A different way to attack Iran’s reactors, CNN.com. , November 8, 2011, http://www.cnn.com/2011/11/08/tech/iran-stuxnet/.
- Statement by the Dutch Minister of Defense “Ank Bijleveld”, Government of the Netherlands, Netherlands Defense Intelligence and Security Services disrupts Russian cyber operation targeting OPCW, http://www.defense-aerospace.com/article-view/release/196530/dutch-mod-disrupts-russian-cyber-attacks-on-opcw-in-the-hague.html. October 2018.
- Statement of the Foreign Office Minister, Lord Ahmad of Wimbledon, Foreign Office Minister Condemns North Korean Actor for WannaCry Attacks, December 2017. https://www.gov.uk/government/news/foreign-office-minister-condemns-north-korean-actor-for-wannacry-attacks
- Sweden, International Humanitarian Law in Armed Conflicts, with reference to the Swedish Total Defense System, Swedish Ministry of Defense, January 1991
- Watts C., Extremist Content and Russian Disinformation Online: Working with Tech to Find Solutions, October 2017, https://securingdemocracy.gmfus.org/extremist-content-and-russian-disinformation-online-working-with-tech-to-find-solutions/