DEGREE PROGRAM IN LAW

Course of Public International Law

CYBER THREATS AND NON-STATE ACTORS UNDER IL: MODERN SECURITY CHALLENGES IN THE AGE OF ANONYMOUS, CYBER SUPPORT AND DIGITAL CONFLICTS

SUPERVISOR

Prof.

Christopher Michaelsen

CO-SUPERVISOR

Prof.

Marco Gestri

CANDIDATE

Alessia Tranzillo

ID 160423

Academic Year 2023/2024

TABLE OF CONTENT

LIST OF ABBREVIATIONS

AP: Additional Protocol

DDoS: Distributed Denial of Service

DoS: Denial of Service

EU: European Union

GC: Geneva Convention

IAC: International Armed Conflict

ICRC: International Committee of the Red Cross

ICT: Information and Communication Technology

ICTY: International Criminal Tribunal for the former Yugoslavia

IHL: International Humanitarian Law

IL: International Law

IT: Information Technology

NATO: North Atlantic Treaty Organization

NIAC: Non-International Armed Conflict

OEWG: Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security

TM 2.0: Tallinn Manual 2.0

UN: United Nations

UNC: Charter of the United Nations

UNGGE: Group of Governmental Experts of the United Nations

CHAPTER I

1. INTRODUCTION

Cyberspace and International Law: Regulatory Gaps and the Role of Non-State Actors in a State-Centric Framework

As society advances at an unprecedented rate, legal systems often fail to keep pace with addressing contemporary multifaceted issues. This is particularly noticeable when focusing on the field of technological progress and the extensive adoption of digital technologies, which have become integral to every aspect of human life.[1] Considering the unique characteristics of this sphere – for instance its inherent transnational nature and the involvement of multiple new stakeholders – significant challenges have arisen in developing a regulatory framework able to effectively address emerging risks and safeguarding rights.[2] The potential dangers posed by this regulatory grey area have been tragically underscored by a multitude of incidents occurring across the world.[3] These events have emphasized the urgent

---

[1] Colin B. Picker, 'A View from 40,000 Feet: International Law and the Invisible Hand of Technology' (2001) 23 *Cardozo L Rev* 151-153, 154-156 [hereinafter: "Colin B. Picker (2001)"]; John King Gamble, Charlotte Ku, 'International Law - New Actors and New Technologies: Center Stage for NGOs' (2000) 31 *Law & Pol'y Int'l Bus* 221-224 [hereinafter: "John K. Gamble (2000)"].

[2] *ibid.*; Kubo Mačák 'Unblurring the lines: military cyber operations and international law' (2021), 6(3) *Journal of Cyber Policy*, 411-428, <https://doi.org/10.1080/23738871.2021.2014919> accessed 10 May 2024, [hereinafter: "Kubo Mačák (2021)"]; PL Denagamage, TRMYSB Thalpathawadan, 'International humanitarian law and cyber warfare: sufficiency of international humanitarian law in combating cyber warfare as a new phenomenon' (2015) *South Eastern University Arts Research Session* 46 [hereinafter: "PL Denagamage (2015)"]; Mohammad Saidul Islam, 'Cyber Warfare and International Humanitarian Law: A Study' (2017) 5 *International Journal of Ethics in Social Sciences* 101.

[3] Stéphane Duguin, Pavlina Pavlova, 'The Role of Cyber in the Russian War against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict' (2023) EP/EXPO/A/COMMITTEE/FWC/2019-01/Lot4/1/C/20 [hereinafter: "Stéphane Duguin (2023)"]; Mike Cherney, 'U.S, allies issue rare warning on Chinese hacking group' (The Wall Street Journal 2024) <https://www.wsj.com/politics/national-security/u-s-allies-issue-rare-warning-on-chinese-hacking-group-9eebb0ce> accessed 28 September 2024 [hereinafter: "Mike Cherney (2024)"]; Iftikhar Gilani, 'Deadly cyber-attacks in Lebanon reveals the new face of warfare' (Frontline 2024) <https://frontline.thehindu.com/news/lebanon-hezbollah-cyber-attack-pager-explosions-warfare-israel-gaza/article68654302.ece> accessed 28 September 2024 [hereinafter: "Iftikhar Gilani (2024)"].

need for more effective international legal responses to threats emerging from the digital frontier.[4]

The inherent complexity and diversity of technological tools, the entities involved, and their impact on both individuals and objects pose a distinct set of challenges to the principles of International Law (IL), which have traditionally been rooted in the context of an "offline" reality.[5] A significant hurdle lies in clearly defining the boundaries of the framework within which actions conducted in cyberspace, or through cyber means, can be classified as lawful or unlawful under IL. Challenges largely stem from the alleged inadequacy of traditional principles of IL – for instance, the principle of state sovereignty and its corollaries – when applied to the cyber domain.[6]

While "classical" IL is premised on state-centric interactions, the cyber sphere has emerged primarily through the initiatives of private individuals, corporations, and other non-state actors.[7] This reality fundamentally disrupts the foundational paradigm of IL, where states are the primary subjects and creators of legal systems.[8] In cyberspace, the dominance of non-state actors complicates the enforcement of state sovereignty, resulting in an unprecedented spread of power and control through different actors.[9] This situation is further aggravated by states' inability to effectively regulate or contain cyber activities conducted within and across their territories, highlighting a significant regulatory and enforcement deficit.[10] Additionally, the transnational nature of cyber activities raises complex issues of jurisdiction and extraterritoriality, where the geographical boundaries that underpin traditional IL become blurred and less applicable.[11]

---

[4] Stéphane Duguin (2023); Mike Cherney (2024); Iftikhar Gilani (2024).
[5] Michael N. Schmitt, Sean Watts 'The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare' (2015) 50 *Tex Int'l L J*; 190-194; Kubo Mačák (2021) 411-428; John K. Gamble (2000) 221-224.
[6] Colin B. Picker (2001), 159-160; Michael N. Schmitt, Sean Watts, 'Beyond State-Centrism: International Law and Non-State Actors in Cyberspace' (2016) 21 *Journal of Conflict and Security Law* 595-596 [hereinafter: "Michael N. Schmitt (2016)"].
[7] John K. Gamble (2000) 221-224; Michael N. Schmitt (2016), 595-596.
[8] *ibid*.
[9] *ibid*.
[10] Irène Couzigou, 'Securing cyber space: the obligation of States to prevent harmful international cyber operations' (2018) 32 *Int'l Rev Law Computers & Technology* 37-57 [hereinafter: "Irène Couzigou (2018)"].
[11] *ibid*.

In this context, a core issue lies in the attribution of conduct with regards to cyber activities, specifically when they are carried out by a group of individuals physically located in different parts of the world. The decentralized and often anonymous nature of cyberspace and cyber entities makes it inherently difficult to link cyber operations to a specific state, organization or person, even when such activities appear to have strategic geopolitical objectives.[12] This problem of attribution not only obstructs the enforcement of state responsibility but also undermines the deterrent capacity of the international legal framework, leading to a landscape where states and non-state actors can operate with relative impunity.[13] The absence of clear accountability mechanisms for cyber activities perpetrated by non-state actors creates a profound legal void. Without a standardized framework for holding both state and non-state actors responsible for cyber operations, IL struggles to address violations effectively.[14] Consequently, this legal uncertainty complicates the development of coherent policies, weakens the efficacy of international legal responses, and perpetuates an environment where states and non-state actors can exploit the ambiguities of IL for their own benefit.

In this respect, it can be established that one of the most pressing concerns relates to the proliferation of new cyber entities, whose unique attributes make it challenging to categorize them within the conventional frameworks defined by contemporary IL.[15] Their presence not only complicates the legal landscape but also prompts critical questions regarding the adequacy of the existing legal classifications.[16] Indeed, it is essential to recognize that establishing the legal status of entities engaged in cyber activities represents a crucial first step in identifying the applicable legal regime and defining the scope and limits of the responsibility regime.[17] The lack of regulation has fueled considerable debate on how to legally

---

[12] Jake B. Sher 'Anonymous Armies: Modern Cyber-Combatants and Their Prospective Rights under International Humanitarian Law' (2016) 28 *Pace Int'l L Rev* 264-265 [hereinafter: "Jake B. Sher (2016)"].
[13] Irène Couzigou (2018), 37-57.
[14] *ibid*., 54-55.
[15] Michael N. Schmitt (2016), 595.
[16] *ibid*.
[17] *ibid*.; Alexander Wentker, Jackson Miles, Lawrence Hill-Cawthorne, 'Identifying Co-Parties to Armed Conflict in International Law: How States, International Organizations and Armed Groups Become Parties to War' (2024) Research Paper, *Royal Institute of International Affairs*, 5 <https://doi.org/10.55317/9781784136017> [hereinafter: "Alexander Wentker (2024)"].

hold accountable non-state actors conducting malicious cyber activities against states and populations, especially as these actions can potentially infringe upon human rights, amount to international crimes, or violate protections established under International Humanitarian Law (IHL), the law applying during armed conflicts.[18] The cyber domain's dynamic nature demands a reconsideration of the traditional principles of IL and the establishment of new legal systems that more adequately address the complex interactions of state and non-state in cyberspace.

Navigating the Cyber Frontier: Distinguishing Between Cyber-Terrorism and Cyber-Support in International Law

In particular, recent events have underscored the power wielded by new aggressive digital actors, like Anonymous, and the increasing cyber capabilities of traditional terrorist organizations, such as al Qaeda and ISIS, fueling the debate around the imminent threat of "cyber-terrorism".[19] The actions of most of modern cyber actors are framed as forms of "contentious politics," serving various social, political, or religious purposes, frequently in opposition to governmental entities or policies.[20] Many of these actions are labeled as acts of terrorism, encompassing a wide range of activities – from hacktivism to the use of cyberspace by terrorist organizations to facilitate traditional forms of terrorism.[21] However, the conflation of all such activities under the banner of cyber-terrorism risks oversimplifying the issue and ignores the distinct purposes and implications of different forms of cyber operations.[22]

To address this issue, some scholars advocate distinguishing between cyber-terrorism and hacktivism, suggesting that creating separate categories may reveal a residual area of legality.[23] For example, while acts of cyber-terrorism conducted by

---

[18] Alexander Wentker (2024), 4-5.
[19] Michael Kenney, *Cyber-Terrorism in a Post-Stuxnet World* (Foreign Policy Research Institute 2015) 111-117 [hereinafter: "Michael Kenney (2015)"].
[20] *ibid.*; Doug McAdam, Sidney Tarrow, and Charles Tilly, *Dynamics of Contention* (Cambridge University Press 2001) [hereinafter: "Doug McAdam (2001)"].
[21] Michael Kenney (2015) 117.
[22] *ibid*.
[23] *ibid*.

non-state actors might inherently be considered unlawful under IL, actions conducted by entities acting as proxies, hacktivists, or supporters of state-driven agendas could potentially align with or even be protected under international legal standards, depending on the context. This distinction is vital, as cyber entities classified as engaging in cyber-terrorism may be deemed as operating unlawfully, while those categorized as supporters or proxies might be accorded a different legal treatment under IHL and state responsibility doctrines.[24] As stressed above, addressing this regulatory gap necessitates the development of legal fictions and frameworks that can effectively categorize these actors and their activities within the current legal system, thereby eliminating gray areas of ambiguity. Therefore, by analyzing cyber operations through the conceptual dichotomy of cyber-terrorism versus cyber-activism or support, some IL scholars and practitioners suggest it can be better understood how the classification of cyber entities influences accountability mechanisms and the application of international legal standards.[25]

A variety of perspectives emerge as these issues can be examined through various branches of IL, particularly International Criminal Law, Human Rights Law, and Humanitarian Law. Among these, a critical area of analysis is the impact of cyber intervention during armed conflicts, as regulated by IHL. Accordingly, it is in this context that the distinction between the status of cyber-terrorist and cyber-supporter can assume significant legal relevance, leading to the application of completely different set of rules.

Cyberwarfare and Non-state actors: Investigating the Legal Status of Cyber Organizations Engaged in Contentious Political Actions under IHL

Given the major impact these new realities have on both global and internal conflicts, as well as international stability, scholars have emphasized the need to analyze and address the consequences of weaponizing cyber capabilities. In particular, as warfare becomes increasingly hybrid, over the years military doctrines have evolved recognizing cyberspace as the fifth domain of warfare, thus replacing

[24] Michael Kenney (2015), 117.
[25] *ibid*., 111-117.

the conventional concept of physical "battlefield" with the broader term "battlespace".[26] Recent global events have underlined the expanding multidimensional nature of modern warfare and the growing prominence of the cyber domain, while also revealing a critical gap – and consequently a urgent need – for specific rules and legal frameworks to address cyberwarfare.[27] In this light, particular concerns have been expressed in respect to the increase of non-state actors engaging in cyberattacks and/or conducting cyber operations against states already engaged in conflicts or dealing with ongoing internal tensions.[28]

As military technologies advances and permeate different aspects of warfare, contemporary armed conflicts continue to be increasingly characterized by complex networks of cooperation among states, international organizations, and non-state actors.[29] This complexity poses significant challenges in identifying which entities qualify as parties to a conflict and clarifying the relationships among the various actors involved.[30] Particularly, the ongoing Russia-Ukraine conflict, along with the array of cyber actors supporting both sides, has sparked interest and debate regarding the legal status of these entities, drawing attention from both the public and legal scholars.[31] It is essential to underscore that determining whether a state, armed group, international organization, or other non-state actor possesses party status in an armed conflict transcends theoretical considerations.[32] This determination carries significant legal implications, particularly for the regulation

---

[26] Christian Reuter (ed), Information Technology for Peace and Security: IT Applications and Infrastructures in *Conflicts, Crises, War, and Peace* (Springer Fachmedien Wiesbaden 2019) <http://link.springer.com/10.1007/978-3-658-25652-4> accessed 10 May 2024, 74–77 [hereinafter: "Christian Reuter (2019)"]; R. S. Pawan, '21st century warfare: from "battlefield" to "battlespace"' (Future Wars, 2017) <https://futurewars.rspanwar.net/21st-century-warfare-from-battlefield-to-battlespace/> accessed 20 April 2024; Council of the European Union, *A Strategic Compass for a stronger EU security and defence in the next decade* (Press Release 2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/> accessed 1 May 2024.

[27] Stéphane Duguin (2023); Denys Svyrydenko, Wiktor Możgin, 'Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine' (2022) 17 *Future Human Image* <https://doi.org/10.29202/fhi/17/6> accessed 10 May 2024 39-46 [hereinafter: "Denys Svyrydenko (2022)"].

[28] Jake B. Sher (2016).

[29] Alexander Wentker (2024).

[30] *ibid*.

[31] Alexander Wentker (2024); Ann Väljataga, 'Cyber Vigilantism in Support of Ukraine: A Legal Analysis' (2022) *NATO Cooperative Cyber Defence Centre of Excellence* [hereinafter: "Ann Väljataga (2022)"].

[32] Alexander Wentker (2024), 5.

of armed conflict and the understanding of which legal frameworks apply to specific actors, objects, and actions involved.[33]

In this context, the dichotomy between cyber-terrorism and cyber-support emerges as a particularly insightful lens through which to analyze the role of cyber organizations in armed conflicts. Under IHL, the nature of a cyber group's intervention – whether as a supporter of a state or as independent organized group – can fundamentally alter the classification of the conflict and the corresponding legal regime.[34] This classification has profound implications for the rules and protections governing the actions of such actors.[35] For instance, when a cyber organization conducts acts of terrorism against a state independently of any other country, the confrontation could potentially reach the level of hostilities necessary to classify it as an organized armed group engaged in a non-international armed conflict (NIAC). Alternatively, the same cyber actor might qualify as supporter of a state already engaged in an international armed conflict (IAC) with another state, as part of the irregular armed forces of such state. Each classification invokes a distinct legal framework under IHL, leading to differing rules and obligations for the actors involved.

This ambiguity in categorization underscores the urgent need for clearer definitions and criteria within IHL to address the roles and responsibilities of cyber actors in conflict. Adopting one classification over another not only changes the legal rules applied but also influences accountability mechanisms and the treatment of individuals associated with these cyber entities. As cyber operations continue to blur the traditional boundaries of warfare, the ability of IL and IHL to adapt and provide coherent and consistent guidance will be essential in addressing the challenges posed by modern conflicts and weapons.

---

[33] Alexander Wentker (2024), 5.
[34] Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017) Rules 82, 83 [hereinafter: "TM2.0"].
[35] TM2.0, Rules 82, 83.

1.1. OBJECT AND STRUCTURE OF THE RESEARCH

In light of this framework, this thesis aims to contribute to the current academic debate by analyzing the relevance and the legal regime of different cyber activities qualifying as cyber threats under IL, to subsequently focus on the specific legal implications for non-state actors operating in and through cyberspace with acts of contentious politics. The aim of this research lies in the investigation of one principal question: "How can the legal status of modern cyber non-state actors, and therefore the legal regime of their actions, be delineated within the framework of IL, and particularly IHL?". Accordingly, the study initially examines the issue through the broader framework of IL, before conducting an in-depth analysis within the specific context of IHL and its regulatory provisions.

The analysis will primary introduce the definition of cyberspace, cybersecurity and cyber threats. Having outline three main categories of cyber threats, namely cybercrimes, ideologically motivated cyber operations and cyberwarfare, the research will examine their relevance within the contemporary international legal landscape, emphasizing the applicable legal frameworks, including emerging treaties and customary law. This examination will lay the groundwork for a deeper understanding of the legal challenges and implications surrounding cyber activities in the realm of IL.

As the analysis delves into the legal frameworks, it will address the main challenges encountered when attempting to apply traditional norms and definitions of IL to the unique characteristics of cyberspace, particularly focusing on the difficulties in applying the principle of sovereignty and the law of state responsibility. Among these challenges, the research will delve into the difficulties in attributing the conduct of groups of actors operating within cyberspace, specifically when they are affiliated by states but not under their control. As mentioned above, this ambiguity contributes to a significant lack of accountability, complicating the enforcement of legal norms in this rapidly evolving domain.

Considering that the majority of cyber threats are carried out by non-governmental entities, the study will solely focus on the actions of cyber non-state actors, examining their legal status and the conditions under which their activities may be deemed lawful or unlawful, particularly when such actions are conducted

within the context of politic tension or an armed conflict. Therefore, the research will not address the cyber threats related to the general category of cybercrime, considering the broadness of such concept. The thesis will provide an analysis of non-state actors involvement in politically motivated cyber activities, to subsequently examine the implication of these activities when they have the potential to escalate into warfare or when they are conducted in the context of armed conflicts.

When introducing the category of ideologically driven cyber operations, the analysis will first focus on the dichotomy between cyber-terrorism and hacktivism, typically present in academic literature. Understanding this distinction is vital, as it is a tool not only to shape the legal framework but also to interpret the strategies employed by states and organizations in responding to these modern threats. In investigating the differences and the similarities between the two categories, the research will also stress the main concerns regarding these definitions and the growing convergence of the two types of cyber activities. Subsequently, the study will advocate for the establishment of a new legal category under IL, able to address the regulatory gap. In this light, the concept of cyber-support will be outlined, while advocating for the adoption of a new test to address state responsibility for non-state actors in cyberspace. In doing so, the research will introduce the Anonymous group and its characteristics in order to outline a concrete example of cyber-supporters in modern scenarios.

Having analyzed the issue through the broad lens of IL, the focus of the thesis shifts to a more specific legal domain, namely IHL. Accordingly, in the context of existing or potential emerging conflicts the perpetration of ideologically-driven cyber operations raises serious concerns. Consequently, the study will propose an analysis of the application of the subcategories previously introduced in the context of armed conflicts and its implications under IHL. It is within this context that the distinction between cyber-terrorism, hacktivism and cyber-support acquires concrete legal significance while simultaneously giving rise to additional complexities.

The differentiation between the legal status of cyber-terrorist organizations, hacktivists collectives or cyber-supporter groups plays a pivotal role when

determining the applicability of IHL's rules and principles to cyber operations. Setting aside the category of non-violent and sporadic hacktivist actions, the different categorization between independent terrorist organizations conducting cyber-attacks against a state and hacktivist cyber entities actively supporting a state involved in an existing conflict leads to markedly distinct legal consequences. This categorization not only affects the regime governing the actions of these groups but also determines the legal status of their members under IHL. Thus, a crucial issue that will be examined is the legal status of cyber entities engaging in hostile cyber operations against a state already involved in an armed conflict with another nation. To this end, the research will analyze the case of Anonymous and its actions against Russia in the context of the conflict between Russia and Ukraine, to shed light on this matter.

In the light of the same circumstances, three main possible alternative classifications emerge under the IHL:

1. Hacktivists as civilians directly participating in hostilities: this scenario refers to the cases in which the attacks perpetrated are regarded as acts of hacktivism, thus, the individuals conducing attacks against one of the countries involved in the conflict can be identified in the category of civilians taking part to the hostilities.[36] Some requirements must be fulfilled, namely threshold of harm, direct causation, and belligerent nexus.[37] In this case the individual civilians taking part to the hostilities would lose some of the protections granted under the civilian status, while not acquiring the proper classification of belligerents and the rights and duties connected to it.[38]

2. Cyber organizations as terrorist organized armed groups parties of a NIAC: this scenario pertains to the cases in which a cyber organization – conducting acts

---

[36] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 31 [hereinafter: "API"], art. 51(3); Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609 [hereinafter: "APII"], art. 13(3).

[37] Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law* (International Committee of the Red Cross 2009) [hereinafter: "Nils Melzer (ICRC 2009)"].

[38] *ibid*.

of "contentious politics" against a certain government – engages in protracted cyber hostilities against that state.[39] Since organized armed groups lack the status to lawfully engage in hostilities under IHL, their actions are inherently unlawful and are subject to criminal prosecution both domestically and internationally. In particular, the group's status as a non-state actor involved in a NIAC precludes it from benefitting from some of the protections and obligations set out under IHL for combatants, while rendering its activities generally subject to the scope of counter-terrorism measures.[40]

3. Cyber groups as co-parties of a state involved in an IAC: this scenario involves cyber organizations conducting cyber operations against a state in support of another state, both already engaged in an IAC between them.[41] The activities of such cyber entities, if closely aligned with the strategic and operational goals of the supporting state, may grant them the status of a co-belligerent, making them a party to the armed conflict.[42] This classification could potentially confer a degree of legality to their actions, provided they meet the requirements set out under IHL, including the principles of distinction, proportionality, and military necessity.[43] As a result, their activities would be regulated under IHL's rules governing IACs, rather than being automatically categorized as unlawful acts of aggression or terrorism. On the other hand, the recognition of the status of co-parties can finally permit a more effective regime of accountability for the actions of such cyber-entities whether they conduce or cooperate in unlawful activities.

Considering the characteristics of cyber entities and cyber operations registered in modern panorama and the specific case study at stake, for the purposes of our research, solely the last two scenarios will be investigated. Particularly, in order to investigate the legal status of these cyber-entities under IHL and therefore delineate the legal regime applying, two alternative sub-questions will be investigated.

---

[39] Geneva Convention relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135 [hereinafter: "GCIII"], art. 3.
[40] International Committee of the Red Cross (ICRC), *Customary International Humanitarian Law* (ICRC 2005), Rule 3, Rule 106.
[41] GCIII, art. 2.
[42] API, art. 4.
[43] API, art. 48, art. 51(5)(b), art. 52(2); ICRC, *Customary International Humanitarian Law* (ICRC 2005), Rule 1, Rule 14, Rule 22.

Firstly, "Can a cyber-entity conducting cyber-attacks against a specific state be classified as an organized armed group and, subsequently, be considered a party to a NIAC against that state under Common Article 3 of the Geneva Conventions (GCs)?".[44] The research will analyze the similarities that can be found between the activities and the nature of traditional terrorists groups which have been recognized as organized armed groups engaged in a NIAC against a certain state and cyber organizations conducting acts of contentious politics against a specific government. For this purpose, the requirements of organization and intensity of hostilities will be introduced and analyzed in the context of cyberspace and cyber-operations.[45] Having ascertained the possibility for cyber-entities to be regarded as virtually organized in light of a "progressive" interpretation of the traditional notions of IHL, the research will briefly assess the difficulties in establishing the level of "protracted armed violence" required in cyberspace.

If a cyber-terrorist organization engages in multiple high-intensity cyber operations that result in severe disruption to a state's critical infrastructure, impairment of governmental functions, or widespread and prolonged damage to civilian life, such actions could potentially satisfy the intensity threshold required for classification as a NIAC. However, significant challenges arise when evaluating cyber operations within the framework of existing IHL. One of the primary difficulties lies in distinguishing between physical and non-physical damage; unlike conventional warfare, cyber operations may not immediately result in tangible, physical destruction but can still cause substantial strategic harm. Additionally, issues of attribution and evidentiary proof present further obstacles, as establishing the degree of organization and direct attribution to a specific non-state group is often complicated by the anonymous and decentralized nature of cyber operations.

While establishing the activities of cyber-organizations involved in cyber hostilities against a specific state/population, such as some Anonymous' attacks, do not fall into the definition of cyber-terrorism, the study will also conclude that at

---

[44] GCIII, art. 3; International Committee of the Red Cross (ICRC), Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War (CUP, 2021) (Commentaries on the 1949 Geneva Conventions) [hereinafter: "ICRC Commentary GCIII"].
[45] ICRC Commentary GCIII; TM2.0 Rule 83.

the present day – due to the lack of specific regulation – no cyber-confrontation seems able to achieve the threshold of a NIAC. Although under IL certain of these cyber activities may present the characteristics for categorization as cyber-terrorism, the traditional IHL framework encounters significant limitations. Specifically, it remains problematic to establish a sustained and intense level of violence when hostilities are conducted primarily in cyberspace, where attacks are often non-physical and lack occupation or long-term control of territory. Consequently, despite the potential for cyber groups to achieve effects comparable to those of traditional terrorist organizations behaving like organized armed groups, the absence of a definition of prolonged physical confrontation in cyberspace and the differences between the violence perpetrated offline and online hinders the full application of NIAC status and, thus, equivalent legal treatment under IHL.

Subsequently, the research will address the second sub-question: "Can these cyber-entities be considered co-parties of a state already involved in an IAC against another state?".[46] To move beyond the broad categorization of all cyber organizations as cyber-terrorists without possibility for them to be considered party of a NIAC against the targeted state, this study will demonstrate that many contemporary cyber-groups operate not as independent actors with purely terroristic aims, neither as mere hacktivists groups, but as quasi-aligned entities supporting the interests of a certain state in conflict against the targeted states, thus as cyber-supporters. This nuanced view reveals that these cyber groups often function more as proxies or informal allies within state-centered conflicts, aligning their actions and objectives with those of state actors rather than acting as traditional terrorist organizations. By examining their patterns of coordination, ideological alignment, and logistical support from state actors, this analysis will provide a more accurate portrait of the role and legal characterization of these cyber-entities, challenging the assumption that they act primarily as terrorist groups detached from state influence. The discussion will initially present the possibility to identify these actors as irregular armed forces of a party to an IAC, to subsequently stress the difficulties in applying this norm in cyberspace.[47] Consequently, this study will

[46] GCIII, art. 2.
[47] API, art. 4.

propose the inclusion of cyber-organized resistance groups within the exceptional circumstances under which non-state actors may be recognized as parties to an IAC thereby partially addressing the substantial legislative gap.

Having established the possibility for these non-state actors to be party to an IAC, the research will investigate whether these cyber-entities can fulfil the conditions to be regarded co-parties of the state they are supporting, by demonstrating the existence of a direct connection of the group's acts to the hostilities and a certain degree of cooperation/coordination between the co-parties. In summarizing the findings obtained through the analysis, the research will finally demonstrate that cybergroups which operates as cyber-supporters may indeed be considered co-parties to an ongoing IAC when they meet the aforementioned criteria. Having underscored the implications associated with the acquisition of (co)party status, concluding remarks will highlight the limitations of current predominant approaches and the challenges arising from the prospected evolution of cyber support and cyberwarfare in the future.

Based on the findings of the research, the study will finally summarize the challenges of establishing regulation and accountability for cyber-threats under IL, particularly when the affiliations between the actors involved and states are complex and ambiguous. By analyzing the relevant case study, the research will illustrate that while emerging cyber organizations are frequently perceived as terrorist groups operating through digital means, a more accurate characterization in many instances would be to classify them as cyber-supporters acting in coordination/cooperation of states. The study will argue that, under certain circumstances, a degree of lawfulness for cyber activities conducted by non-state actors can be established, even within the context of armed conflicts, as long as the cyber entity in question satisfies specific criteria and its actions adhere to the overarching principles of IL, including, where applicable, IHL. In engaging with these complex legal questions, this research aims to shed light on the regulatory gaps and ambiguities surrounding cyber operations and the role of cyber actors, ultimately contributing to the development of a coherent international legal framework capable of effectively address these evolving challenges.

1.2. METHODOLOGY

From a methodological standpoint, this study adopts a multifaceted approach to rigorously address the legal complexities surrounding cyber activities and cyber actors. The primary methodology utilized is doctrinal research, which systematically delineates the legal framework and pertinent norms relevant to the subject matter.[48] Doctrinal research is applied throughout the analysis to present the law as a structured set of principles, devoid of consideration for its real-world implementation or impact.[49] This method entails a critical evaluation of international treaties, customary law, jurisprudence, and scholarly commentary to identify and outline the legal structures currently applicable to cyber activities and specifically cyber operations. The analysis scrutinizes these sources to determine the extent to which conventional international legal concepts are being challenged and redefined by cyber operations. In parallel, the study employs a comparative legal analysis to examine divergent international perspectives on the regulation of cyberspace and particularly cyberwarfare.[50] This comparative approach is instrumental in assessing the effectiveness and limitations of existing norms in addressing the evolving dynamics of modern conflicts.[51]

To substantiate this evaluation, the research integrates a case study methodology, leveraging real-world examples to illustrate the practical application and limitations of IL in the cyber domain.[52] This approach consists of analyzing and interpreting data from one or more specific case studies to gather and structure information, allowing for the identification of patterns and underlying assumptions.[53] This method will be used mostly in the second part of this research, when approaching the analysis of cyber operations conducted by non-state actors in the context of an armed conflict. Given the fascinating dynamics at play, the

---

[48] Khushal Vibhute, Filipos Aynalem, 'Legal Research Methods' (2009) 17 *Ethiopian Legal Bief* 70-71 [hereinafter: "Khushal Vibhute (2009)"]
[49] *ibid*.
[50] *ibid*. 32-33, 72-73, 75-85.
[51] Khushal Vibhute (2009), 32-33, 72-73, 75-85.
[52] Philip Langbroek, 'Methodology of Legal Research: Challenges and Opportunities' (2017) 13(3), 13(7) <https://utrechtuniversity.on.worldcat.org:443/atoztitles/link?sid=google> accessed 10 May 2024 [hereinafter: "Philip Langbroek (2017)"].
[53] *ibid*.

relevant legal framework will be applied mainly to the actions of the notorious cyber-entity Anonymous in the context of the Russia-Ukraine conflict,[54] aiming to draw broader implications for similar entities.[55] Specifically, the case study will be used to explore whether the cyber entities characterizing the reality of today, like Anonymous, can be categorized as cyber terrorist groups whose actions would invariably contravene IL, particularly IHL, or whether some of their actions shall be regarded as acts of cyber-support. Subsequently, focusing on IHL, the case study will be used to first investigate whether it would be possible to identify entities like Anonymous as terrorists organized armed groups participating in NIACs against single states. Conversely, it will be used to analyze the circumstances under which such entities might qualify as co-belligerents in IACs, thus potentially positioning them as lawful participants conducting cyber operations within the existing legal framework.

By combining the doctrinal analysis with the case-study method, this research endeavors to provide a sophisticated and nuanced perspective on the capacity of IL to address the multifaceted challenges posed by cyber activities and the expanding role of non-state actors in this context. The insights generated from this examination will contribute to a more precise understanding of when cyber entities may be considered lawful actors within the evolving legal landscape of IL – specifically of IHL – and, consequently, under which conditions some of their activities could be potentially identified as lawful according to the present framework.

In analyzing the outcomes of the application of the law to cyberspace and specifically to the case study, the research will adopt a reform-oriented approach.[56] This involves a critical examination of the current legal framework, aiming to align traditional notions of IL and IHL with the evolving dynamics of cyberspace. The analysis will highlight significant legislative gaps concerning the regulation of cyber activities and the legal status of cyber actors, posing serious concerns for the

---

[54] Dan Milmo, 'Anonymous: The Hacker Collective That Has Declared Cyberwar on Russia' (*The Guardian* 2022) <https://link-gale-com.proxy.library.uu.nl/apps/doc/A695152994/ITOF?u=utrecht&sid=bookmark-ITOF&xid=ab63ae49> accessed 10 May 2024 [hereinafter: "Dan Milmo (2022)"].
[55] Philip Langbroek (2017).
[56] Khushal Vibhute (2009), 26.

future, which will be always more characterized by the use of cyber means and the presence of cyber actors. While delving into the complex question of whether cyber activities and cyber-entities can be considered lawful under IL, and particularly within the scope of IHL, the research will highlight the urgent need for tailored rules to define cyber operations and identify virtual organizations, while also challenging the shortcomings of existing theories on how IL applies to the digital realm. Indeed, the study argues that rigidly adhering to current interpretations – often upheld by the majority of scholars – risks creating legal uncertainties and leaving room for exploitation. To bring these issues into sharper focus, the research focuses on cyberwarfare, aiming to expose legal blind spots and propose stronger safeguards. It ultimately calls for a fresh, systematic reinterpretation of the legal framework, drawing parallels with the classification of irregular armed forces and the concept of co-belligerency. This approach seeks to bridge the gap between traditional law and the realities of cyber operations, offering a clearer path forward for regulating digital participation in armed conflict.

For these purposes, the entire analysis will utilize common interpretive techniques, including literal and contextual or systematic interpretation.[57] As mentioned above, in the absence of a defined set of written regulations concerning cyber-entities and cyberwarfare at the international level, legal principles will be derived from the existing legal framework applicable. This will primarily involve analyzing fundamental treaties, customary laws, and their evolution through the observation of relevant opinio juris and state practice. When interpreting relevant provisions for application to new scenarios, the study will focus not solely on the "ordinary meaning" but predominantly on the "context", "object and purpose" of the terms.[58] Additionally, the examination of state practice and associated opinio juris will facilitate a systematic and progressive interpretation of pertinent customary rules. By integrating all these methodological approaches, the research aims to provide a comprehensive legal analysis that addresses the complexities of

[57] Vienna Convention on the Law of Treaties, opened for signature 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980), art. 31(1), art. 31(3)(c) [hereinafter: "VCLT"].
[58] VCLT, art. 31(1), art. 31(3)(c).

cyber activities and the role of cyber-entities in contentious politics and armed conflicts, contributing to the development of more robust legal frameworks.

1.3. SCOPE AND SIGNIFICANCE OF THE STUDY

This study provides a thorough analysis of the growing number of significant challenges arising from the interplay between IL, digital technologies and global security. Particularly, the examinations put in evidence the crucial need for better and more agile regulatory frameworks to face a rapidly mutating and fluid international landscape.[59] As technological advancement continues to change how individuals, corporations, and states interact – for instance with the advent of artificial intelligence, blockchain technology, and advanced data analytics – the legal frameworks underpinning these interactions often prove to be inadequate to deal with the complex risks and challenges presented by such innovations.[60] Therefore, this research aims to fill an important gap in contemporary legal scholarship by investigating how IL, due to its inherent complexity and comparative slowness in adaptability, is struggling to keep up with the acceleratingly rapid changes that are being produced by technology in virtually all fields of modern life.[61]

As mentioned above, these challenges become specifically pressing within the context of ideologically motivated cyber-attacks, armed conflicts and warfare, where the expanding reliance on digital technologies poses new legal questions.[62] The increasing use of the digital means in this context introduces a series of unprecedented concerns. Among them, it is necessary to highlight the difficulties registered in the regulation of cross-border data flows, in managing the increase of cybercrimes, and in enforcing sovereignty.[63] The main issue lies in the fact that these challenges cannot be effectively addressed by the traditional state-centric

---

[59] PL Denagamage (2015) 46; John K. Gamble (2000) 221-224.
[60] Jamil Afzal, *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (Springer 2024).
[61] Colin B. Picker (2001) 151-156.
[62] Jenny Döge, 'Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime' 48(4) (2010) *Archiv des Völkerrechts* 486-501; PL Denagamage (2015) 46.
[63] Colin B. Picker (2001) 151-156.

legal paradigm, which is poorly suited to handle the inherent transnational nature of digital activities.[64] The absence of clear and harmonized international regulations exacerbates these problems, creating a fragmented legal environment in which jurisdictional loopholes arise, leading to inconsistent protections of fundamental rights and responsibilities.[65]

The significance of this study is further highlighted by its potential to contribute meaningfully to both academic discourse and the development of practical policy solutions. As states and other international actors attempt to regulate cyber activities and create normative standards of behavior in cyberspace, this research offers a detailed evaluation of existing legal structures. By means of this, the study also discusses potential future directions for revising IL in light of the challenges posed by digital security threats, specifically with regards to cyberwarfare. Therefore, the study seeks to enrich the prevailing legal and policy debates with findings that can help develop more resilient and adaptive legal frameworks, which could prove better at safeguarding fundamental rights, ensuring accountability, and fostering a stable and secure digital environment.

By highlighting the interrelation of legal issues in the digital environment, this research calls for an integrated and holistic approach to law reform that takes into consideration flexibility, adaptability, and international cooperation as priorities. The adoption of this view is essential to empower the international legal community in its quest to anticipate and react to new challenges that are emerging in this digital era and, at the same time, make sure that IL retains its validity and effectiveness for current and upcoming developments in technology.

[64] John K. Gamble (2000) 221-224.
[65] *ibid*.

CHAPTER II

2. NEW TECHNOLOGIES, CYBER THREATS AND THE CHALLENGES OF MODERN INTERNATIONAL LAW

The rise of the Internet during the last decades of the 20th century has been recognized as one of the most significant transformative moments of the history of humankind, embodying one of the most revolutionary technologies so far.[66] From its original limitation to the domain of scientific research, the Internet has rapidly grown into a critical basis of modern life, touching almost all aspects of human activity.[67] This evolution has been underpinned by the steady advance of available technologies that have driven inclusivity and usage for users from various socio-economic backgrounds. In particular, it must be remarked that the past couple of decades have been characterized by a process of integration of information and communication technologies (ICTs) and media-platforms. This phenomenon has generated great convergence of the informational, social and technological dimensions.[68] This convergence has given rise to a global dimension which seems unbounded by traditional geographic or political frontiers, as a distinct dimension of physical reality.[69]

The increasing dependency of both state and non-state actors on digital infrastructures has made computers and interconnected networks indispensable in a broad spectrum of essential operations.[70] As this reliance deepens, so do the vulnerabilities associated with digital failures and the opportunities available to actors' intent on exploiting these systems.[71] Non-state actors, including hackers, organized groups, and terrorist organizations, are especially poised to use cyber

---

[66] Katarzyna Chałubińska-Jentkiewicz, *Cyberspace as an Area of Legal Regulation* In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) 'Cybersecurity in Poland' Springer, Cham 23-24 https://doi.org/10.1007/978-3-030-78551-2_2 [hereinafter: "Katarzyna Chałubińska-Jentkiewicz (2022)"].
[67] *ibid*. 23-24.
[68] *ibid*. 23.
[69] *ibid*.
[70] Irène Couzigou (2018), 37-38.
[71] *ibid*.

capabilities as potent offensive tools in the international arena.[72] This trend is generating particular concerns as transboundary cyber operations are now more feasible than ever, often carried out at minimal cost, with rapid deployment, and frequently eluding detection.[73] Recent incidents have underscored the substantial risks posed by harmful cross-border cyber operations, which threaten both government entities and private sector actors alike.[74] Given these risks, it is critical to establish a foundational understanding of what constitutes cyberspace and to clarify the definitions of cyber threats before proceeding with a deeper analysis of their characteristics and legal implications.

In light of this framework, this Chapter aims to firstly provide the definitions of cyberspace, cybersecurity and cyber threats to subsequently introduce the relevant legal framework and the challenges related to the difficulties in disciplining the intersection of new technologies to traditional rules of IL. In particular, the study will focus on the difficulties in applying the principle of sovereignty to cyberspace and its corollaries, specifically the rules established under the law of state responsibility. In this respect, the study will advocate for the adoption of new approaches to address responsibility of states for the conduct of cyber non-state actors, considering the difficulties in tracking the specific link between states and cyber entities, due to the inherent nature of cyberspace and cyber activities.

2.1. CYBERSPACE, CYBER SECURITY AND CYBER THREATS

In IL, the precision of definitions plays a fundamental role in shaping the scope and enforceability of legal norms, especially within the complex domain of cyberspace. In particular, the term "cyberspace" and the various classifications of "cyber threat" have gained critical importance, as their conceptual clarity directly affects the applicability and reach of international legal frameworks. Cyberspace itself is an expansive, borderless virtual realm that defies conventional jurisdictional boundaries, therefore testing traditional understandings of

[72] Irène Couzigou (2018), 37-38.
[73] *ibid*.
[74] *ibid*.; Stéphane Duguin (2023).

sovereignty and state responsibility.[75] Similarly, defining cyber threats involves navigating a range of activities – from direct cyber operations aimed at disrupting or seizing control over critical infrastructure to indirect actions that may erode national security or destabilize essential state functions.[76] These distinctions are not merely academic; they determine which legal frameworks – whether IHL, human rights obligations, or criminal law norms – govern such conduct and affect the attribution of responsibility to state and non-state actors alike. Therefore, the establishment of clear and comprehensive definitions is not only a preliminary legal task but a strategic necessity in order to address and discipline cyber threats, phenomena which are increasingly blurring the lines between war and peace.

In this light, this study will first establish the definitions necessary for our analysis, to subsequently examine how IL and its definitions can evolve to address the novel and multiplex challenges presented by cyberspace and cyber means.

2.1.1. Cyberspace

The term cyberspace first emerged in the 1980s, as an amalgamation of the words "cybernetics" and "space".[77] William Gibson introduced this term for the first time in his novel Neuromancer in 1984.[78] While originally limited to the realm of science fiction, the concept of cyberspace has become central to contemporary reality.[79] In particular, Gibson's early description of cyberspace gained significant fame over time because it highlighted key essential characteristics that remain relevant today: its boundless nature in terms of time and space, its virtual and complex nature, and its capacity to compress a huge amount of information into a unified digital ecosystem.[80]

---

[75] Filip Radoniewicz, *Cyberspace, Cybercrime, Cyberterrorism* (2022) In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) 'Cybersecurity in Poland' Springer, Cham 33 https://doi.org/10.1007/978-3-030-78551-2_2 [hereinafter: "Filip Radoniewicz (2022)"].
[76] Igor Duić, Vlatko Cvrtila, Tomislav Ivanjko (eds), 'International Cyber Security Challenges', *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics* (MIPRO) (2017) 1525-1529 [hereinafter: "Igor Duić (2017)"].
[77] Filip Radoniewicz (2022), 33.
[78] *ibid.*; François Delerue, *Cyber Operations and International Law* (Cambridge University Press 2020) 10 [hereinafter: "François Delerue (2020)"].
[79] François Delerue (2020), 10.
[80] Filip Radoniewicz (2022), 33.

Cyberspace is a highly complex concept, encompassing a wide interconnected digital environment that goes beyond national borders and operates through nets of ICTs.[81] Despite the term cyberspace being central to scholarly and policy discussions for years, no universally accepted definition can be found. Nevertheless, various key documents at both national and international levels have sought to outline parameters and principles that shape an understanding of cyberspace.[82] These efforts, while varied in approach, jointly contribute to defining cyberspace's legal and operational boundaries, and reflect an ongoing attempt to clarify the implications of this domain for sovereignty, security, and legal responsibility in IL.

In academic literature, cyberspace has been traditionally conceptualized as the virtual environment created by interconnected digital networks, where information and communication occur through various technological infrastructures such as the Internet, telecommunications systems, and computer networks.[83] This definition of cyberspace focuses exclusively on its technological dimension, omitting any consideration of its social dimension and its central user: humanity. Furthermore, it prioritizes the hardware infrastructure as the primary foundation of cyberspace, emphasizing the pivotal role of the Internet while neglecting the equally critical contribution of software systems.[84] This narrow perspective fails to capture the complex interplay between the technological and human elements that collectively shape the cyberspace environment.

Focusing on the international legal framework, a comprehensive definition can be extrapolated by the large number of documents and legislation elaborated by the North Atlantic Treaty Organization (NATO) through the years. Particularly, in 2010 the NATO Cooperative Cyber Defence Centre of Excellence in Tallinn

[81] Filip Radoniewicz (2022), 33.
[82] *ibid*.
[83] Tomasz Zdzikot, *Cyberspace and Cybersecurity* (2022) In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) 'Cybersecurity in Poland' Springer, Cham. https://doi.org/10.1007/978-3-030-78551-2_2 [hereinafter: "Tomasz Zdzikot (2022)"].
[84] *ibid*.

suggested that: "[c]yber-space is a time-dependent set of interconnected information systems and people/users who interact with those systems".[85]

In 2019, NATO provided a more accurate definition by describing cyberspace as: "[t]he global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data".[86]

What makes these definitions innovative and comprehensive is their inclusion of not just elements of physical hardware – such as computers, servers, and communication devices – but also data exchanges and interactions that characterize human engagement.[87] It is crucial to point out that cyberspace encompasses far more than the virtual environment itself; it also includes the diverse range of activities that are performed outside what is strictly considered digital domain but impact it. Cyberspace involves both actions which are intrinsic to the digital realm (such as data exchanges and network communications), and external activities facilitated by digital tools able to cause visible effects in the physical world. Examples of these external impacts include disruptions to critical infrastructure or the manipulation of information with profound social or political ramifications. This duality – combining virtual actions with their real-world effects – renders cyberspace a unique domain where the digital and physical spheres converge.

2.1.2. Cyber Security

While the online world offers an exceptional environment to tackle communication, business, and innovation challenges like never before, it also

---

[85] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications.* (2010) In: 'Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April', Reading: Academic Publishing Limited 267-270 <https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/> accessed on 4 November 2024; Katarzyna Chałubińska-Jentkiewicz (2022), 26.

[86] NATO Glossary of Terms and Definitions AAP-06(2019) 37 <https://www.coemed.org/files/stanags/05_AAP/AAP-06_2019_EF.pdf> accessed on 30 October 2024.

[87] Tomasz Zdzikot (2022); Alexander G. Crowther, 'National Defense and the Cyber Domain' (2017) *The Heritage Foundation* 82-97.

brings along a wide range of misuses and disturbances.[88] This reality has underlined the need to formulate concrete standards and provisions, so as to assure the intactness, privacy, and normal operation of the digital systems existing in this field.[89] Thus, the notion of "cybersecurity" has evolved through time in response to such problems.[90]

By definition, cybersecurity is a collective term for the multitude of tactics, regulations and technologies aimed at the protection of information systems, digital networks and data from unauthorized access, disruption or harm. [91] The cybersecurity concept digs deeper than safeguarding technical prerequisites in information technology and communication; it is rather a multifaceted orienting phenomenon that incorporates the global legal, political, and strategic dimensions of the digital world.[92] To the extent that they have become dependable components of economy, governance, and daily life, points of heavy reliance are also potential targets.[93] Examples of the devastating potential of modern cyber-threats include the growing amount of sophisticated cyber-attacks targeting critical infrastructures, such as energy grids, healthcare infrastructures, financial institutions, and governmental services.[94] Considering the increasing dependency of these vulnerable infrastructures on ICTs services, such cyber-attacks have proved capable of significantly disrupt and destabilize national governance, essential services and entire societies.[95]

The risks flowing from the vulnerabilities of ICTs systems and their pervasiveness call for the implementation of effective cybersecurity strategies, both

---

[88] Katarzyna Chałubińska-Jentkiewicz (2022), 28.
[89] Scott J. Shackelford, Scott Russell, Andreas Kuehn, 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors' (2016) 17(1) *Chicago Journal of International Law* [hereinafter: "Scott J. Shackelford (2016)"].
[90] *ibid*.
[91] Thakur Kutub, 'An Investigation on Cyber Security Threats and Security Models.', *Institute of Electrical and Electronic Engineers (IEEE) 2nd International Conference on Cyber Security and Cloud Computing* (IEEE 2015) 307-308; The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, OJ EU C 2014.32.19., http://www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf
[92] *ibid*.
[93] *ibid*.
[94] Katarzyna Chałubińska-Jentkiewicz (2022), 2-3.
[95] *ibid*.

nationally and internationally.[96] These include measures to be taken to prevent the threats to cybersecurity and plans in place to come up with an efficient response in case of such an attack.[97] Effective management of cybersecurity is, therefore, the primary means by which critical risks are mitigated to ensure the stable continuity of state functions. Along these lines, a global endeavor to achieve translational cybersecurity is needed, as cyberspace is inherently transnational and the interconnected nature of its vulnerabilities requires global cooperation and establishment of international rules.[98]

Accordingly, failure to adequately manage national cybersecurity increases the risks to interfere with international peace and security.[99] Threats to cybersecurity today come in diverse forms that encompass the likes of state-sponsored cyber espionage, large-scale ransomware operations, and the activities of non-state actors who exploit cyber space for malicious reasons or, on the contrary, to support human rights or cause human emancipation.[100] The militarization of cyber space, particularly in the context of geopolitical disputes, intensifies the existing tensions between states, but also non-state actors, and thereby creates new and dangerous ways of conflict escalation.[101]

Recent cases of large-scale malicious cyber operations have drawn attention to the impact of cyber-attacks and retaliatory actions in intensifying the pressure on already fragile international relations.[102] Moreover, the inherent asymmetry of cyber threats – where resource-limited entities or individuals can inflict disproportionate harm compared to traditional means – challenges the application of rules disciplining accountability and deterrence in IL. This reality reveals the urgency of developing a cohesive global framework for regulating state and non-

---

[96] Mary Ellen O'Connell, Louise Arimatsu, Elizabeth Wilmshurst, 'Cyber Security and International Law' *International Law Meeting Summary* (Chatham House 2012) 3-12 [hereinafter: "Mary Ellen O'Connell (2012)"].
[97] *ibid*.
[98] *ibid*.
[99] Mika Kerttunen, Saskia Kiisel (eds), 'Norms for International Peace and Security: The Normative Frameworks of International Cyber Cooperation' (ICT4Peace Foundation 2015) https://ict4peace.org/wp-content/uploads/2020/05/16496284.pdf accessed on 10 November 2024 [hereinafter: "Mika Kerttunen (2015)"].
[100] *ibid*.
[101] Mary Ellen O'Connell (2012), 3-12.
[102] *ibid*., 3-5.

state conduct in cyberspace. The absence of such a framework risks that legal ambiguities continue to enable vicious actors to exploit gaps in accountability.[103]

Cybersecurity represents a critical legal and geopolitical issue at the heart of contemporary international dynamics. Addressing cybersecurity challenges involves advanced technological defenses against threats and the establishment of legal frameworks and global mechanisms to sustain the stability and robustness of cyberspace. Notably, a secure cyberspace is indispensable for achieving the broader purposes of avoiding conflicts and consolidating stability in an interconnected highly unpredictable global system.[104] Thus, cybersecurity is not simply a technique that aims to reduce the technological risks, but it is the bedrock of international peace and security, thus enabling cyberspace to maximize its benefits without being obscured by the harms.

2.1.3. Cyber Threats

Cybersecurity is the foundational process of digital infrastructure protection and risk mitigation. Nevertheless, considering the numerous vulnerabilities associated with cyber technologies and the speed of innovation in this field, cybersecurity is particularly susceptible to breaches.[105] The alarming issue lies in the fact that cyber threats pose significant risks of harm, not only individual systems but also to state sovereignty, economic stability and the international order.[106]

Accordingly, dealing with cyber threats has been recognized today as the most immediate concern in the process of maintaining international peace and security. These threats are not confined to any spatial or legal geography, but omnipresent in the digital dominium that is more of a non-place and, thus, they challenge the traditional notions of jurisdiction and sovereignty.[107] As a consequence, critical issues arise in maintaining IL effective when approaching the novel and varied uses of sophisticated technologies emerging, specifically when cyber threats require the

---

[103] Mary Ellen O'Connell (2012), 3-12.
[104] Mika Kerttunen (2015).
[105] Igor Duić (2017), 1525-1529.
[106] *ibid*.
[107] *ibid*.

application of the rules regarding accountability, for state and non-state actors, and the principles governing armed conflicts.[108]

Fundamentally, the notion of cyber threats encloses the wide range of malicious activities conducted through cyberspace in order to compromise the safety, trustworthiness and efficiency of digital systems and networks.[109] These threats exploit weaknesses in the digital landscape, often targeting the integrity, confidentiality, or availability of data and infrastructure.[110] What makes cyber threats particularly concerning is not only their increasing frequency but also their ability to disrupt the foundational elements of contemporary society – economies, governance structures, and public trust – thereby creating profound challenges for international relations and collective security frameworks.[111]

Cyber threats materialize predominantly through cyber operations and cyberattacks, which represent distinct but overlapping means of executing hostile activities in cyberspace.[112] Cybers operations can be defined, in a general way, as the use of digital means and methods for offensive or defensive purposes, including operations of reconnaissance, espionage, or developing cyber capabilities for later use.[113] In contrast, cyberattacks specifically consist of intentional actions aimed at producing immediate and tangible harm.[114] Cyberattacks can take many forms, such as acts of sabotage, unauthorized access to sensitive information, the spread of ransomware, or disruption of critical digital services using Distributed Denial of Service (DDoS) attacks, among other strategies.[115] More broadly, a cyberattack can also refer to an organized/coordinated effort to alter, disrupt, or dismantle adversary computer systems, networks, or the data and software that reside on or travel through these systems.[116]

---

[108] Igor Duić (2017), 1525-1529.
[109] *Canadian Centre for Cyber Security - An Introduction to the Cyber Threat Environment* (Communications Security Establishment 2022).
[110] *ibid*.
[111] *ibid*.
[112] TM 2.0.
[113] Herbert S. Lin, 'Offensive Cyber Operations and the Use of Force' (2010) 4 *JNat'l Sec L & Pol'y*, 63-86.
[114] *ibid*.; Michael Kenney (2015) 113.
[115] Michael Kenney (2015) 113.
[116] *ibid*.

A more detailed breakdown of the definition and discipline of cyber operations and cyberattacks – particularly under the lens of IHL– will be provided in Chapter IV.

For analytical purposes, cyber threats will be classified under this study into three main categories: cybercrimes, ideologically-driven cyber operations, and cyberwarfare.

1. Cybercrimes refers to a broad category of illicit activities conducted via computers, networks, or digital devices, encompassing various offenses such as identity theft, financial fraud, and unauthorized data breaches, typically driven by personal or economic motives. According to a comprehensive definition proposed in academic literature, cybercrime encompasses "any crime that is facilitated or committed using a computer, network, or hardware device" where the computer may serve as the agent, facilitator, or target of the crime.[117]

2. Ideologically motivated cyber operations/attacks represent a distinct category of activities occurring in and through cyberspace, characterized by their political, social, or ideological objectives, rather than economic or personal motivations.[118] These actions are best understood as forms of "contentious politics" conducted by non-state actors to advocate for diverse political, social, or religious causes, often challenging or opposing governmental policies and decisions.[119] The use of digital tools to advance such agendas distinguishes them from other cyber activities, underscoring their role as a destabilizing force in the digital domain.[120] Accordingly, the aim of these operations consists in exploiting the unique attributes of the digital environment for the purpose of shaping public perception, interfere with the functioning of societies, or further specific social and political objectives.[121] Predominantly carried out by non-state actors, such operations often involve groups of individuals coordinating their efforts.[122] In many instances, these

---

[117] Sarah Gordon, Richard Ford, 'On the definition and classification of cybercrime' (2006) 2 *Journal in Computer Virology* 13-20.
[118] Thomas J Holt, Joshua D. Freilich, Steven M. Chermak, 'Exploring the subculture of ideologically motivated cyber-attackers' (2017) 33(3) *Journal of Contemporary Criminal Justice* 212-233 [hereinafter: "Thomas J Holt (2017)"].
[119] Michael Kenney (2015) 117-128; Doug McAdam (2001).
[120] Michael Kenney (2015) 117-128.
[121] Michael Kenney (2015) 117-128; Thomas J Holt (2017), 212-233.
[122] *ibid*.

actors mature into structured and sophisticated cyber entities, thus making their classification under the existing legal framework extremely difficult.[123] In particular, it has been noted that these activities typically arise in the context of ongoing or pre-existing conflicts involving states, populations, or other non-state actors – highlighting once again the strongly ideological nature behind this type of actions.[124]

Within this group, two principal subcategories can be identified: cyber-terrorism and hacktivism.[125] Cyber-terrorism represents the more severe manifestation of these actions, in which cyber capabilities are used to instill fear, coerce governments or populations, or disrupt critical infrastructure to achieve ideological or political goals.[126] These activities align closely with the traditional understanding of terrorism but are designed to exploit the vulnerabilities and features of cyberspace, amplifying their disruptive potential.[127] Conversely, hacktivism has historically been associated with non-violent efforts to advocate for social or political causes, such as exposing governmental misconduct or challenging corporations' activities.[128] However, in its modern forms, hacktivism has increasingly evolved into a phenomenon that blurs the line between traditional activism and more extreme ideological forms of attacks, as it has been registered that this type of actions today increasingly lead to direct or indirect manifestations of violence.[129]

In addition, contemporary hacktivist operations are always more often conducted by structured cyber groups which display a multitude of characteristics common to those of traditional armed groups.[130] These organizations frequently operate in support of states or specific populations, engaging in ideologically driven cyber operations aligned with the strategic objectives of a particular state or

---

[123] Thomas J Holt (2017), 212-233; Michael Kenney (2015), 117-128.
[124] *ibid*.
[125] Michael Kenney (2015), 117-128.
[126] *ibid*. 121-128.
[127] *ibid*.
[128] *ibid*. 117-121.
[129] *ibid.*
[130] *ibid*.

political entity.[131] Nevertheless, unlike traditional state-sponsored actors, these groups usually operate without fulfilling the legal criteria required to be classified as under the overall or effective control of a state, thus existing in a legal grey zone as independent supporters.[132]

What is particularly concerning is the growing convergence between modern forms of hacktivism and cyberterrorism.[133] The methods, organization, and ideological goals of some hacktivist groups are becoming increasingly similar to what is described as cyberterrorism, complicating attempts to identify a clear distinction between the two categories.[134] This vague line not only tests the limits of the lack of specific legal regulations on non-state actors' behavior in cyberspace, but also underlines the urgent need to re-examine the applicability of existing legal norms. This increase in organized cyber groups that do not fit into the conventional categorizations indicates the necessity to adjust the actual international legal framework in order to deal with the complexity of ideologically motivated cyber-attacks and their consequences.[135]

3. The term cyberwarfare has been mostly used to describe the deployment of cyber capabilities, predominantly by states or state-affiliated entities, to achieve military or strategic objectives in the context of armed conflicts or to destabilize adversaries during peacetime, potentially triggering new conflicts.[136] Although basically political in nature, cyberwarfare is distinguished by its distinction from ideologically driven activities such as cyber terrorism or hacktivism. Its key features include the usual state-directed nature of the attacks and the focus on advancing national security or military interests, rather than representing individual or group dissent.[137]

---

[131] Michael Kenney (2015); Scott J. Shackelford, Richard B. Andres, 'State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem' (2011) 42 *Geo J Int'l L* 971-1016 [hereinafter: "Scott J. Shackelford (2011)"].
[132] Scott J. Shackelford (2011), 971-1016.
[133] Michael Kenney (2015), 117-128.
[134] *ibid*.; Scott J. Shackelford (2011), 971-1016.
[135] *ibid*.
[136] Michael Kenney (2015), 114-117; Mette Eilstrup-Sangiovanni, 'Why the World Needs an International Cyberwar Convention' (2018) 31 *Philos Technol* <https://doi.org/10.1007/s13347-017-0271-5> accessed 11 November 2024, 382-384 [hereinafter: "Mette Eilstrup-Sangiovanni (2018)"].
[137] *ibid*.

Nonetheless, increasing non-state actors' participation in the conduct of cyber operations further complicates the already blurred legal construct and operating environment.[138] These actors often operate in a legal gray zone, neither fully under state control nor completely independent, raising complex issues concerning attribution, proportionality, and their legal classification under IHL.[139] In addition, it has been highlighted how cyberwarfare, in contrast to traditional warfare, moves beyond physical battlefields, making it easier to target vital civilian infrastructure, such as energy networks, financial institutions, and healthcare systems, thereby blurring the lines between military and civilian targets.[140]

This increasingly hybrid nature of warfare, where digital tools intersect with traditional military strategies, highlights the urgent need to reevaluate the application and interpretation of IHL principles to cyberspace.[141] Ensuring that norms of attribution and accountability remain effective in this context is crucial to preserving the integrity and effectiveness of IL.[142] A more detailed examination of the concept of cyberwarfare and the challenges posed to the applicability of IHL in this context will be explored in Chapter 4.

Grasping the differences and nuances of these classifications is key in formulating effective legal strategies against cyber threats. Each of these categories demands tailored approaches that balance the interests and rights involved. By situating cyber threats within their broader political and legal contexts, the study will better analyze the challenges posed by this complex yet indispensable domain.

2.2. INTERNATIONAL LEGAL FRAMEWORK

2.2.1. Applicability of IL to Cyberspace: A New Legal Domain?

When approaching these issues, one of the first questions arising is whether IL provides an effective framework for regulating the matter and safeguarding

---

[138] Scott J. Shackelford (2011), 971-1016.
[139] *ibid*.
[140] *ibid*.; Mette Eilstrup-Sangiovanni (2018) 379-407.
[141] *ibid*.
[142] Mette Eilstrup-Sangiovanni (2018), 379-407.

international stability from the potentially devastating impacts of cyber threats. As a matter of fact, IL is widely recognized as the cornerstone of the modern international legal order and plays a crucial role in preserving global peace and security.[143] Its principles and mechanisms provide a foundational framework for addressing emerging challenges, including those posed by cyberspace and cyber threats.[144]

Given its comprehensive scope, IL offers a potentially effective framework for regulating cyber operations/attacks and mitigating the risks associated with cyber threats.[145] Accordingly, it is widely accepted that many legal issues pertaining to cyber operations/attacks at their core are linked to existing international legal instruments and principles.[146] These include the provisions of the United Nations Charter (UNC) of 1945, the Geneva Conventions of 1949 along with their Additional Protocols, and, crucially, the customary rules of international law regarding state responsibility for internationally wrongful acts, as systematically codified by the International Law Commission of the United Nations.[147] These instruments collectively form the legal foundation for regulating malicious behaviors in cyberspace.

The transformative nature of cyberspace, however, presents unique challenges to the application of IL.[148] Cyber threats, while often originating within the boundaries of individual states, possess an inherently transnational character,

---

[143] François Delerue (2020), 1-13.
[144] *ibid*.
[145] *ibid*.
[146] *ibid*.
[147] United Nations, Charter of the United Nations (adopted 26 June 1945, entered into force 24 October 1945) 1 UNTS XVI [hereinafter: "UNC"]; 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 [hereinafter: "GCI"]; Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 85 [hereinafter: "GCII"]; GCIII; 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 31 [hereinafter: "GCIV"]; API; APII; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem (Protocol III) (adopted 8 December 2005, entered into force 14 January 2007) 2404 UNTS 261 [hereinafter: "APIII"]; International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001) UNGA Res 56/83 (12 December 2001), annex, UN Doc A/RES/56/83 [hereinafter: "ARSIWA"]; François Delerue (2020), 13.
[148] François Delerue (2020), 1-13.

capable of disrupting not only national security but also global stability.[149] This is particularly evident when considering the distinctive features of cyber activities, such as their speed, anonymity, and the difficulty of attribution.[150] These characteristics amplify their capacity to undermine international peace and stability on an unprecedented scale, highlighting the pressing need for an international legal framework capable of addressing these threats.[151]

This necessity has triggered a continuing controversy on the question of whether or not it is appropriate to consider cyberspace as a space with specific norms and principles of IL or, instead, as an inseparable part of traditional domains as land, sea, air and outer space.[152] This debate underscores the broader question of how IL can remain effective and relevant in the face of rapidly evolving technologies.[153] The aspects, features and characteristics of the cyberspace and cyber activities, as well as their widespread use in all areas of activity, have stimulated some authors to consider it as a separate sphere, especially in the context of military application.[154] This idea gained some credibility during the Gulf War of 1991 – commonly referred to as the first "information war" – when it was first argued that cyberspace was the fifth domain of war, along with land, sea, air and outer space.[155] This thesis, now widely accepted, emphasizes cyberspace as an operational environment.[156] Nonetheless, not all scholars agree with this classification. According to this minor thesis, it is not possible for cyberspace to be treated as a separate domain.[157] As a consequence, traditional rules of IL are applicable to cyber activities to the extent that these activities target persons or objects located in the other four traditional domains.[158] On the basis of this point of view, considering

---

[149] Mette Eilstrup-Sangiovanni (2018), 382-388.
[150] *ibid*.
[151] *ibid*.
[152] 'Cyberwar: War in the Fifth Domain', The Economist (1 July 2010) www.economist.com/ node/16478792; Christy, Marx, *Battlefield Command Systems of the Future* (The Rosen Publishing Group 2005) 14; Yaroslav Radziwill, *Cyber-Attacks and the Exploitable Imperfection of International Law* (Brill & Martinus Nijhoff Publishers 2015) 13; François Delerue (2020), 10; Christian Reuter (2019).
[153] François Delerue (2020), 11-13; Christian Reuter (2019)
[154] Katarzyna Chałubińska-Jentkiewicz (2022), 23-24; Christian Reuter (2019).
[155] *ibid*.
[156] *ibid*.
[157] François Delerue (2020), 11-13.
[158] *ibid*.

cyberspace's interconnected nature, it is impossible to identify cyberspace as an independent area. Contrarily, this interconnectivity makes it an extension of existing dimensions, rather than an independent sphere.[159]

To briefly address this debate, it is necessary to distinguish between two critical issues: the applicability of IL to cyberspace and its suitability in regulating all types of cyber activities.[160] While it is broadly accepted in both academic and state practice that IL extends to cyberspace and cyber operations, significant uncertainties persist regarding how specific norms should be applied and enforced within this context.[161] For instance, in its 2013 and 2015 reports, the United Nations Group of Governmental Experts (UNGGE) affirmed that existing IL, particularly principles derived from the UNC, applies to state conduct in cyberspace, emphasizing that states have jurisdiction over cyber infrastructure within their territories.[162] Subsequently, numerous states have reaffirmed this stance through their submissions to the United Nations (UN) Secretary-General and the articulation of international and national strategies on cyber defense and cybersecurity.[163]

---

[159] François Delerue (2020), 11-13.
[160] *ibid*.
[161] *ibid*.
[162] United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report A/68/98 (2013) 19 <https://undocs.org/A/68/98>; United Nations General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report A/70/174 (2015) 13(24) <http://undocs.org/A/70/174>.
[163] UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (9 September 2013) UN Doc A/68/156/Add.1; UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 June 2014) UN Doc A/69/112; UNGA, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (18 September 2014) UN Doc A/69/ 112/Add1; *See, for instance:* Italy, 'Italian Position Paper on International Law and Cyberspace' (Ministry of Foreign Affairs and International Cooperation 2021)https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberscybe.pdf; Australia, 'Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity' (Department of Home Affairs 2016) 7, 28, 40-41 https:// cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf; France (SGDSN), 'Stratégie nationale de la Cyberdéfense [*Revue stratégique de cyberdéfense*]' (Secrétariat général de la défense et de la sécurité nationale (SGDSN) and Economica 2018) 82, 85, 87 www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/; France, 'International Law Applied to Operations in Cyberspace [*Droit international appliqué aux opérations dans le cyberespace*]' (Ministère des Armées 2019) https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations +in+cyberspace.pdf; The Netherlands, 'Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace' and 'Appendix: International Law in Cyberspace' (Ministry of Foreign Affairs 2019)

Nonetheless, cyberspace's distinct attributes – such as its intangibility, the anonymity of actors, the rapid pace of technological change, and the cross-border nature of its activities – pose substantial challenges to the practical implementation of existing legal rules and therefore to the suitability of them.[164] This complexity is compounded by the lack of consensus among states on how to interpret and apply these norms in cyberspace.[165]

Consequently, a balanced approach is needed – one that recognizes cyberspace as both an independent domain with unique features and an interconnected network deeply embedded within the traditional domains of land, sea, air, and outer space.[166] While it is true that existing IL provides a foundational framework for addressing cyber activities, the development of new, domain-specific legal instruments is essential to address the gaps created by cyberspace's novel characteristics. These instruments must account for the dual nature of cyberspace, which simultaneously functions as a distinct sphere of activity and an integrative network influencing all other domains.[167] In this light, a mixed interpretation offers a pragmatic way forward. Cyberspace can be viewed as a new domain when its unique attributes – such as its borderless nature and its ability to enable operations that transcend traditional geographic constraints – justify tailored legal rules.[168] At the same time, where existing norms are suitable, they should be applied to ensure coherence and

---

https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentarydocuments/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace; Russian Federation, 'Doctrine of Information Security of the Russian Federation' (2016) 34 www.mid.ru/en/foreign_policy/offi cial_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163; United Kingdom, 'National Cyber Security Strategy' (2016) 63 www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021; François Delerue (2020), 2; 'BRICS Leaders Xiamen Declaration' (2017 BRICS Summit, 5 September 2017) https://www.bricschn.org/English/2017-09/05/c_136583711_2.htm para 56 accessed 14 December 2024.

[164] François Delerue (2020) 11-13.

[165] Kubo Mačák, 'Is the International Law of Cyber Security in Crisis?' *2016 8th International Conference on Cyber Conflict (CyCon* 2016), 127-139, doi: 10.1109/CYCON.2016.7529431. accessed on 10 November 2024 [hereinafter: "Kubo Mačák (2016)"].

[166] Daniel Ventre, *Cyberespace et acteurs du cyberconflit* (Lavoisier & Hermes 2011) [hereinafter: "Daniel Ventre (2011)"] 87-88.

[167] Daniel Ventre (2011), 87-88.

[168] Katarzyna Chałubińska-Jentkiewicz (2022), 23-24; Christian Reuter, (ed), *Information Technology for Peace and Security: IT Applications and Infrastructures in Conflicts, Crises, War, and Peace* (Springer Fachmedien Wiesbaden 2019) <http://link.springer.com/10.1007/978-3-658-25652-4> accessed 10 May 2024.

continuity in the international legal order.[169] This dual perspective allows for the development of a nuanced regulatory framework capable of addressing the complexities of cyberspace while maintaining the relevance of traditional IL.

2.2.2. New International Instruments For Cyber Regulation

In addition to the general principles of IL, a partial specific regulation of cyber activities is provided by sectoral and regional treaties.[170] Between these instruments, relevant documents are the 1992 Constitution of the International Telecommunication Union, the 2001 Budapest Convention on Cybercrime and its 2006 Additional Protocol on Xenophobia and Racism, the 2009 Shanghai Cooperation Organization's Information Security Agreement, the 2014 African Union Convention on Cyber Security and Personal Data Protection, the 2019 European Union (EU) Cybersecurity Act, the 2022 EU Directive on Security of Network and Information Systems (EU NIS) 2, and the 2023 EU Cyber Resilience Act.[171] While these instruments mark important steps in regulating specific aspects of cyberspace, their scope remains limited.[172] They primarily address narrow issues, such as disruptions to telecommunications networks or the development of norms for some specific states' activities in cyberspace. Nevertheless, they leave critical

---

[169] François Delerue (2020) 11-13.
[170] Kubo Mačák (2016), 132.
[171] Constitution of the International Telecommunication Union (concluded 22 December 1992, entered into force 1 July 1994) 1825 UNTS 143 [hereinafter: "ITU Constitution"]; Council of Europe, Convention on Cybercrime [signed 23 November 2001, entered into force 1 July 2004] ETS 185 [hereinafter: "Budapest Convention"]; Council of Europe, Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems [opened for signature 28 January 2003, entered into force 1 March 2006] ETS 189; Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security [signed 16 June 2009, entered into force 5 January 2012] ('Yekaterinburg Agreement'); African Union Convention on Cyber Security and Personal Data Protection [signed 27 June 2014] AU Doc EX.CL/846(XXV); Kubo Mačák (2016), 132; Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 [hereinafter: "Cybersecurity Act 2019"] PE/86/2018/REV/1; Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 [hereinafter: "NIS 2 Directive"]; European Parliament and Council, 'Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 COM (2020) 823 final.
[172] Kubo Mačák (2016), 132-133.

gaps unaddressed.[173] Additionally, many of these instruments suffer from limited membership or ratification, therefore undermining their applicability and effectiveness.[174] Supplementing the abovementioned list, other non-binding yet influential instruments have been developed to promote standards and protocols around cyber stability. In particular, relevant documents are the Tallinn Manual 2.0 (TM 2.0), the 2018 Paris Call for Trust and Security in Cyberspace, and the North Atlantic Treaty Organization (NATO) Comprehensive Cyber Defence Policy of 2021.[175] These instruments have gained considerable relevance over the years, contributing to a shared understanding of the application of IL in this evolving domain and offering guidance on the formulation of tailored regulations for cyber activities. However, their classification as soft law – non-binding legal sources – raises significant concerns about their enforceability and practical effectiveness[176]. Despite their normative value and influence in shaping state behavior and international consensus, their lack of binding authority limits their ability to compel and ensure compliance, leaving their overall efficacy subject to debate.[177]

When focusing on the specific categories of cyber threats under discussion – cybercrimes, ideologically-motivated cyber operations/attacks, and cyberwarfare – the inadequacies of this regulatory framework become increasingly obvious. In particular, while cybercrimes driven by personal or economic aims are subject to more robust international legal instruments, such as the Budapest Convention and regional documents (e.g. EU Directives) – which provide a quite comprehensive framework for combating offenses like hacking, fraud, and child exploitation online[178] – no equivalent tools exist to specifically address ideologically-motivated cyber operations/attacks or cyberwarfare.[179] Therefore, the regulatory gap is particularly evident in addressing cyber activities that fall outside traditional

---

[173] Kubo Mačák (2016), 132-133.
[174] *ibid*.
[175] TM 2.0; *Paris Call for Trust and Security in Cyberspace* (adopted 12 November 2018) https://pariscall.international/en/ accessed 4 November 2024 [hereinafter: "*Paris Call (2018)*"]; North Atlantic Treaty Organization (NATO), *Comprehensive Cyber Defence Policy* (2021) https://www.nato.int/cps/en/natolive/topics_82798.htm accessed 4 November 2024.
[176] François Delerue (2020), 13-27.
[177] *ibid*.
[178] Budapest Convention; *For instance, see*: NIS 2 Directive.
[179] Thomas J Holt (2017), 212-233; Mette Eilstrup-Sangiovanni (2018), 382-388.

categories of crime but still pose significant threats to international security and stability.[180]

For ideologically-driven cyber operations, which include hacktivism/cyber support and cyber terrorism, existing soft law instruments attempt to fill the void left by the absence of binding agreements.[181] Initiatives such as the 2018 Paris Call for Trust and Security in Cyberspace and the Norms, Rules, and Principles for Responsible State Behavior in Cyberspace, developed under the auspices of the UNGGE, provide non-binding guidelines that promote norms of responsible behavior and encourage cooperative measures among states.[182] These instruments aim to establish standards for behavior in cyberspace, emphasizing the need for accountability and transparency, despite they lack the enforceability and legal authority of hard law.[183]

Comparably, also when focusing on cyberwarfare the regulatory landscape remains predominantly shaped by soft law.[184] In particular, the TM 2.0 offers one of the most detailed interpretations of how IL, and specifically IHL, might apply to cyberspace and cyber conflicts.[185] This document has gained considerable influence, offering guidance on key issues of IL and IHL, such as attribution and the conduct of hostilities.[186] However, since its implementation depends on voluntary adherence, it lacks the power to enforce compliance by states or individuals. Aside from this precious source, the 2021 Report of the Open-Ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) and subsequent UN processes have also encouraged confidence-building measures and voluntary commitments among states; however, also these mechanisms lack the authority to establish binding obligations.[187]

---

[180] Thomas J Holt (2017), 212-233; Mette Eilstrup-Sangiovanni (2018), 382-388.
[181] François Delerue (2020), 13-27.
[182] *Paris Call (2018)*; UNGGE, *Norms, Rules, and Principles for Responsible State Behaviour in Cyberspace,* Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace (2015).
[183] *ibid*.; François Delerue (2020), 13-27.
[184] Mette Eilstrup-Sangiovanni (2018), 381-405.
[185] TM 2.0. Part IV.
[186] *ibid*.
[187] UN General Assembly*, Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, (2021) UN Doc*

Given the evolving nature of these threats, with non-state actors increasingly assuming a central role, the absence in regulation and the gap in protection are nowadays particularly significant.[188] Traditional rules of IL, such as those governing state responsibility, are often insufficient to address scenarios involving non-state cyber actors operating independently or presenting ambiguous links with state authorities.[189] These actors, whether ideologically driven or politically aligned, frequently exploit the lack of clear attribution and accountability mechanisms, complicating efforts to classify and regulate their activities under IL.[190] Accordingly, while general principles of IL – including those governing sovereignty, state responsibility, and the prohibition of the use of force – continue to apply to cyber activities, these principles were not designed to address the unique characteristics of cyberspace and, therefore, their application remains contested and uneven.[191] In this context, the unwillingness of states to develop specific binding rules for addressing cyber threats appears to have created a "regulatory vacuum".[192] This void has enabled non-state entities to take advantage of the absence of oversight, often reshaping the norms and operational dynamics of cyberspace to their advantage.[193] This phenomenon is closely tied to the increasing reliance of non-binding instruments in shaping the rules governing cyberspace.[194] This reliance on soft law highlights a broader challenge: while such instruments offer flexibility and adaptability, they leave critical questions unresolved, particularly regarding the accountability of non-state actors, such as cyber organizations or loosely affiliated groups, that often operate in the "gray zone" between state control and independent agency.[195] The absence of hard law mechanisms for these categories underscores

---

A/76/135; UNGGE*, Final Report of the 2019-2021 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (2021) UN Doc A/76/135;* UN Open-Ended Working Group on the Use of Information and Communications Technologies in the Context of International Security (OEWG)*, 'Final Report' (2021) UN Doc A/75/818.*

[188] Michael Kenney (2015), 111-120.

[189] Peter Margulies, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 *Melb J Int'l L* 496-501 [hereinafter: "Peter Margulies (2013)"].

[190] Peter Margulies (2013), 496-501.

[191] *ibid*.

[192] Kubo Mačák (2016), 131-139.

[193] *ibid*.

[194] *ibid*.

[195] Peter Margulies (2013), 496-519.

the urgent need for an international consensus on binding regulations to ensure a robust and enforceable framework governing ideologically driven cyber operations and cyberwarfare.[196] Until then, soft law remains the primary mechanism for shaping behavior and addressing emerging threats in these domains.

Consequently, while cyberspace falls under the remit of IL, the current regulatory framework is insufficient to comprehensively address the multifaceted challenges posed by cybercrimes, ideologically driven operations, and cyberwarfare.[197] This underscores the urgent need for a more unified and robust international legal framework capable of addressing the complex realities of cyber threats in the modern era.[198]

2.2.3. The Growing Prominence Of Soft Law

The regulation of cyber threats under IL has increasingly relied on soft law instruments, reflecting the unique challenges posed by the rapidly evolving and highly complex nature of cyberspace.[199] Unlike traditional hard law, which is grounded in binding treaties and formal agreements, soft law offers the flexibility necessary to address the diverse and fast-changing realities of cybersecurity.[200] The rigid and often time-consuming processes required to develop and implement hard law make it unsuitable to keep pace with emerging threats, such as cybercrime, ideologically motivated cyber operations, and cyberwarfare. In contrast, soft law instruments, including voluntary guidelines, norms of responsible behavior, and non-binding agreements, provide a more agile and collaborative framework for addressing these challenges.[201]

One of the key reasons for the growing prominence of soft law in this field is the increasing centrality of non-state actors in cyber activities.[202] Non-state entities, including cybercriminal networks, hacktivist organizations, and even private

---

[196] Kubo Mačák (2016), 132-133.
[197] *ibid*.
[198] *ibid*.
[199] François Delerue (2020), 13-27.
[200] *ibid*.
[201] *ibid*.
[202] ibid., 21-24; Kubo Mačák (2016), 132-134.

companies, play a significant role in shaping the dynamics of cyberspace.[203] These actors often operate across jurisdictions, complicating the enforcement of hard law and necessitating a more cooperative and adaptable approach.[204] Soft law mechanisms, such as the Paris Call for Trust and Security in Cyberspace and the UN General Assembly resolutions on cybersecurity, allow states to engage with non-state actors and foster inclusive dialogues aimed at promoting best practices and building trust.[205] Such frameworks are better suited to accommodate the diverse interests and capacities of both state and non-state stakeholders, offering a platform for voluntary compliance and collaboration without the formal obligations of treaties.[206] Moreover, soft law has demonstrated its utility in establishing foundational norms and confidence-building measures that contribute to stability in cyberspace.[207] For example, the norms developed by the UN Group of Governmental Experts (UNGGE) on responsible state behavior in cyberspace, while non-binding, have significantly influenced the international discourse by affirming the applicability of existing IL to cyberspace and proposing practical measures to reduce risks of conflict.[208] These norms, combined with regional initiatives and multi-stakeholder platforms, demonstrate how soft law can bridge gaps in hard law by providing guidance on issues where consensus on binding rules is lacking.

However, the growing reliance on soft law also underscores the tension between flexibility and enforceability.[209] While soft law allows for adaptation and innovation, its non-binding nature can lead to inconsistent implementation and divergent interpretations, particularly when addressing controversial issues such as state attribution for cyberattacks or the classification of cyber operations under

---

[203] Mary Ellen O'Connell (2012), 3-12.
[204] *ibid*.; Peter Margulies (2013), 496-519.
[205] *Paris Call (2018)*; UN General Assembly Resolutions on Cybersecurity, UNGA Res 73/27 (5 December 2018) UN Doc A/RES/73/27, UNGA Res 74/28 (12 December 2019) UN Doc A/RES/74/28.
[206] *Paris Call (2018)*; UN General Assembly Resolutions on Cybersecurity, UNGA Res 73/27 (5 December 2018) UN Doc A/RES/73/27, UNGA Res 74/28 (12 December 2019) UN Doc A/RES/74/28; François Delerue (2020), 21-24.
[207] *ibid*.
[208] TM 2.0.
[209] François Delerue (2020), 24-26.

IHL.[210] This challenge is exacerbated by differing state interests and priorities, as seen in the varying levels of commitment to soft law initiatives like the TM 2.0 or the Global Commission on the Stability of Cyberspace's Norms.[211]

By facilitating dialogue, promoting voluntary compliance, and enabling the active engagement of non-state actors, soft law opens the way for a more inclusive and flexible framework for cyberspace governance.[212] However, it remains imperative for states to reassert their central role in the formulation of IL, particularly to establish a coherent and binding set of rules governing cyber activities.[213] Additionally, states must adopt a more assertive approach in articulating their interpretations of how existing international law applies to cyber-related issues.[214] As cyber threats continue to expand in both scale and complexity, the interplay between soft law and hard law will be pivotal to ensure that IL remains responsive and effective in respect to technological advancements.[215]

2.3. MAIN CHALLENGES OF INTERNATIONAL LAW's APPLICATION TO CYBER THREATS

2.3.1. The Increasing Role Of Non-State Actors And The Crisis Of The State-Centered System

As mentioned above, one of the foremost challenges in both the application and development of international legal norms concerning cyberspace arises from the growing prominence of non-state actors. Historically, IL has been shaped by a state-centric approach, in which states were recognized as the primary bearers of rights and obligations.[216] This framework emerged in a context where states held exclusive control over the resources, infrastructure, and authority necessary to

---

[210] François Delerue (2020), 24-26.
[211] Tech Accord, *TM 2.0: Principles for Tackling Cyber Threats* (2021) https://cybertechaccord.org/tm2-0/ accessed 30 November 2024; Global Commission on the Stability of Cyberspace, *Advancing Cyber Stability: Final Report* (November 2019) https://cyberstability.org/report/ accessed 30 November 2024.
[212] François Delerue (2020), 24-26.
[213] Kubo Mačák (2016), 138-139.
[214] ibid.
[215] *ibid*.
[216] Cedric Ryngaert, 'Non-State Actors: Carving out a Space in a State-Centred International Legal System' (2016) *The Netherlands International Law Review* 185-189.

impact international peace and security.[217] In contrast, non-state actors were largely marginalized, perceived either as agents acting on behalf of states or as entities with negligible independent influence.[218] However, the advent of the digital age has profoundly disrupted this paradigm.[219] Cyberspace, characterized by its borderless, decentralized, and highly interconnected nature, has become a domain in which non-state actors operate also independently, often with capabilities that compete or even surpass those of states.[220] This shift has exposed significant deficiencies in the existing international legal framework, which remains largely ill-equipped to address the complexities posed by these entities. As a result, the actions of non-state actors in cyberspace are reshaping not only the application of IL but also the assumptions underpinning its foundational principles.[221]

The empowerment of non-state actors in cyberspace is unprecedented, specifically with regard to cyber threats. In contrast to traditional forms of security-threats or conflicts – where military strength, territorial control, and economic resources limited the influence of non-state actors – cyberspace offers a level playing field.[222] Armed with relatively low-cost but highly sophisticated technologies, entities such as hacktivist groups, transnational corporations, and terrorist organizations are now capable of conducting cyber operations with significant geopolitical and economic consequences.[223] For instance, access to advanced software, artificial intelligence, and global communication networks enables these actors to launch coordinated cyber-attacks, disrupt critical infrastructure, steal sensitive information, and influence political processes – all with minimal physical presence or logistical support.[224]

---

[217] Michael N. Schmitt (2016), 595-596.
[218] *ibid*.
[219] *ibid*.
[220] *ibid*.
[221] François Delerue (2020), 21-24.
[222] Michael N. Schmitt (2016), 595-611.
[223] *ibid*.; Math Noortmann, Cedric Ryngaert, 'Introduction: Non-state Actors: International Law's Problematic Case' in Math Noortmann and Cedric Ryngaert (eds), *Non-state Actor Dynamics in International Law: From Law-Takers to Law-Makers* (Ashgate 2010) 1-2.
[224] Pierluigi Paganini, *Cybersecurity and Critical Infrastructures: The Role of the EU in Tackling Cyber Threats* (CSSII, 2022) https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Paganini_Pierluigi.pdf accessed 14 December 2024 [hereinafter: "Pierluigi Paganini (2022)"].

Prominent examples illustrate this growing influence. Groups like Anonymous, known for their ideologically-driven "hacktivist" campaigns, have orchestrated high-profile destructive and disruptive attacks on government institutions, corporations, and international organizations.[225] Similarly, terrorist organizations exploited cyberspace to disseminate propaganda, recruit operatives, and even orchestrate cyber-attacks, bypassing traditional state-centric mechanisms of regulation and control.[226] Meanwhile, multinational corporations managing key components of the global internet infrastructure, such as data centers and communication networks, have found themselves involved in cyber conflicts, sometimes as targets of state-sponsored attacks and other times as reluctant participants in national cyber strategies.[227]

As previously noted, the emergence of a multitude of structured cyber non-state actors has notably escalated their interactions with states, underscoring the increasing relevance of public IL in regulating and addressing these dynamics.[228] The principles that once governed state-to-state relations are now being tested by actions taken by non-state entities that operate independently or with minimal state support.[229] This transformation complicates the application of existing legal norms and principles, primarily drafted to address interactions between states rather than between states and non-state actors.[230] Therefore, the growing influence of non-state actors in cyberspace underscores the inadequacies of the current legal framework and its state-centric structure.[231]

2.3.2. The Challenges Of Applying Traditional IL Paradigms: Sovereignty, State Responsibility And Attribution

In particular, the prominence of non-state actors in cyberspace disrupts traditional rules of IL rooted in state sovereignty and territorial jurisdiction, notably

---

[225] Pierluigi Paganini (2022), 9; Michael Kenney (2015), 117-121.
[226] Michael Kenney (2015) 121-128.
[227] Virginia Franke Kleist, 'Global Multinational Organizations: Unintended Threats from Nation-State Cyberwarfare' (2021) 24(4) *Journal of Global Information Technology Management* 229-234.
[228] François Delerue (2020), 17-26.
[229] *ibid*.; Michael N. Schmitt (2016), 595-611.
[230] Michael N. Schmitt (2016), 595-611.
[231] *ibid*.

state responsibility and attribution.[232] The unique features of cyberspace and the actors operating within it profoundly complicate the interpretation and practical application of the principle of sovereignty – a cornerstone of IL.[233] The complexities surrounding its implementation in the digital realm have cascading effects, influencing numerous facets of the broader international legal framework and exposing its inadequacies in addressing the dynamics of this new domain.[234]

Unlike conventional domains, where geographic boundaries provide more defined parameters for legal governance, cyberspace is mainly perceived as a transnational, decentralized, and borderless realm.[235] Accordingly, the erosion of sovereignty in cyberspace firstly stems from its borderless nature.[236] Non-state actors can carry out cyber operations across multiple jurisdictions without ever leaving their physical locations.[237] This ability significantly undermines the territorial foundations of sovereignty, creating challenges for states attempting to assert their authority in cyberspace.[238] For instance, a cyber-attack originating in one state may simultaneously target critical infrastructure in multiple countries, bypassing traditional jurisdictional boundaries, and vice versa.[239] Thus, it is evident that the lack of territorial constraints complicates enforcement mechanisms and disrupts the conventional framework that ties legal accountability to geographic borders.[240]

This disruption of sovereignty is intrinsically connected to the various challenges that arise in the application of state responsibility rules to cyber non-state actors and transnational cyber threats.[241] Firstly, under customary international

---

[232] Michael N. Schmitt (2016), 595-611; Peter Margulies (2013), 496-501.
[233] Peter Margulies (2013), 497; UNC, art. 2(1), art. 2(4); ARSIWA, art. 2, art. 4; *Corfu Channel Case* (United Kingdom v Albania) (Merits) [1949] ICJ Rep 4, 35 [hereinafter: "*Corfu Channel Case*"]; *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14, 202-205 [hereinafter: "*Military and Paramilitary Activities in and against Nicaragua*"].
[234] Peter Margulies (2013), 497-519.
[235] Filip Radoniewicz (2022), 33.
[236] Patrick W Franzese, 'Sovereignty in Cyberspace: Can It Exist?' (2009) 64 *Air Force L Rev* 1, 1-24 [hereinafter: "Patrick W Franzese (2009)].
[237] *ibid*.
[238] *ibid*.
[239] *ibid*.
[240] *ibid*.
[241] Michael N. Schmitt (2016), 597-607.

law states are obligated to ensure that their territory is not used to harm other states – a duty encapsulated in the principle of due diligence.[242] However, in the context of cyberspace, this principle appears often unenforceable.[243] Non-state actors frequently exploit the transnational nature of cyberspace, operating in jurisdictions with weak cybersecurity infrastructure or insufficient political will to regulate their activities.[244] In some instances, states may even tacitly support or condone such activities for strategic gain, further complicating the enforcement of legal obligations.[245] For example, cyber operations that destabilize adversaries may be indirectly beneficial to the state harboring the non-state actors, even if it does not exercise direct control over them.[246]

This directly links to the issue of attribution, one of the most challenging aspects of IL with regards to cyberspace.[247] Attribution refers to the process of identifying the perpetrator of a cyber operation and determining their relationship to a state.[248] For the purposes of this discussion, the focus will be on attributing the actions of cyber organizations to states, rather than attributing individual actions within these groups.

Under customary international law, as codified in the Articles on the Responsibility of States for Internationally Wrongful Acts (ARSIWA), a state shall be held responsible for any internationally wrongful act committed by its organs or by people/entities exercising governmental functions.[249] Additionally, the conduct of a non-state entity or group can be attributed to a state even if that entity is not formally considered an organ of the state, provided that the state exercises direction and/or control over the entity or group when carrying out the act in question.[250] This principle is enshrined in Article 8 of the ARSIWA, which states:

---

[242] *Corfu Channel Case*, 22; *Pulp Mills on the River Uruguay* (Argentina v Uruguay) [2010] ICJ Rep 14, 101; *Opuz v Turkey* App no 33401/02 (ECtHR, 9 June 2009) 128-130; ARSIWA, art. 2; UNC, art. 2.
[243] Michael N. Schmitt (2016), 597-607.
[244] *ibid*.
[245] *ibid*.
[246] *ibid*.
[247] *ibid*.; Scott J. Shackelford (2011), 971-992.
[248] TM 2.0, Rule 11.
[249] ARSIWA, art. 4, art. 5.
[250] ARSIWA, art. 8.

"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."[251]

Based on this provision, a variety of theoretical frameworks have been developed over time to clarify the conditions under which the conduct of non-state actors may be attributed to a state. These include the "effective control" and the "overall control" tests.[252] The effective control test has been extensively examined in judicial decisions, especially in cases before the International Court of Justice (ICJ), and remains the most commonly applied criterion.[253] It requires evidence of a high degree of direct control of the state over the non-state actor in relation to a specific act. The overall control test, on the other hand, has emerged over time from the jurisprudence of other international courts – in particular the International Criminal Tribunal for the former Yugoslavia (ICTY) – to establish state responsibility in cases where a state exercises a broader, less direct form of control over a non-state actor.[254] It takes into account a broader range of activities, such as general support and strategic direction, to determine whether state responsibility can be invoked.[255] Both tests are critical in understanding the extent of state accountability for actions carried out by groups or entities that are not formally part of the state apparatus but are nevertheless under its control.[256]

---

[251] ARSIWA, art. 8.
[252] *Military and Paramilitary Activities in and against Nicaragua*, 115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia and Herzegovina v Serbia and Montenegro) (Merits) [2007] ICJ Rep 43, 400 [hereinafter: "*Application of the Convention on the Prevention and Punishment of the Crime of Genocide*"]; *Application of the International Convention on the Elimination of All Forms of Racial Discrimination* (Georgia v Russia) (Preliminary Objections) [2011] ICJ Rep 70, 155 [hereinafter: "*Application of the International Convention on the Elimination of All Forms of Racial Discrimination"]*; *Prosecutor v Duško Tadić* (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-A (2 October 1995) 70 [hereinafter: "*Prosecutor v Duško Tadić*"].
[253] *Military and Paramilitary Activities in and against Nicaragua*, 115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, 400.
[254] *Prosecutor v Duško Tadić*, 70; *Application of the International Convention on the Elimination of All Forms of Racial Discrimination*, 155.
[255] *ibid*.
[256] *Military and Paramilitary Activities in and against Nicaragua*, 115; *Application of the Convention on the Prevention and Punishment of the Crime of Genocide*, 400; *Application of the International Convention on the Elimination of All Forms of Racial Discrimination*, 155.

In this regard, it becomes immediately apparent that these tests, originally designed with traditional non-state actors in mind, fail to capture the complexities of cyberspace, where non-state actors, including hacktivist, cyber-terrorist groups, cybercriminals, and even private entities, can engage in sophisticated operations that blur the lines of state responsibility.[257] It is essential to underline that, unlike traditional forms of security-threat or conflict – where physical evidence and observable actions provide clarity – cyber operations are inherently clandestine or covered by anonymity.[258] Techniques such as encryption, spoofing, and the use of proxy servers obscure the origin of attacks, making it exceedingly difficult to determine whether a non-state actor acted independently or under the direction of a state.[259] Many cyber-attacks, while seemingly independent, reveal implicit or explicit links to state actors. Non-state entities often receive support, whether through resources, tacit approval, or strategic alignment, creating a complex web of relationships.[260]

In this context, the dynamics of cyberspace seem to challenge and even reverse conventional assumptions about the relationship between states and non-state actors. A closer examination of recent developments over the past few decades reveals a growing trend in which cyber organizations, rather than being controlled by states, often play an active role in advancing state interests. In many instances, these non-state actors operate with considerable autonomy, while states, in turn, may tacitly endorse or covertly encourage their activities.[261] This allows states to benefit from the outcomes of cyber operations, all the while avoiding direct responsibility or accountability for the actions of these cyber entities.[262]

This increasing phenomenon presents a complex challenge for attribution within the existing legal framework, which continues to rely on tests that are clearly

---

[257] Scott J. Shackelford (2011), 971-992; Michael Kenney (2015), 117-128.
[258] *ibid*.
[259] *ibid*.; Joan Feigenbaum, Aaron Johnson, Paul Syverson, 'A Model of Onion Routing with Provable Anonymity' in *Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007* (Springer 2007) 57–71 [hereinafter: "Joan Feigenbaum (2007)"].
[260] Scott J. Shackelford (2011), 971-992; Michael Kenney (2015), 117-128; Joan Feigenbaum (2007), 57-71.
[261] *ibid*.
[262] *ibid*.

inadequate to address the evolving interactions between states and cyber non-state actors. The traditional methods of attribution, designed for more conventional contexts, struggle to account for the unique nature of cyber operations and the decentralized structure of cyber actors, underscoring the need for an updated approach to effectively discipline these relationships.[263]

2.3.3. The Unsuitability Of The Control Test For State Responsibility In Cyberspace: The Sliding Scale Approach

The challenges faced by modern IL in addressing cyber threats become especially evident when examining the applicability of the control tests for attribution under the law of state responsibility.[264] Although the overall control test may appear more flexible than the effective control test, and therefore applicable, both remain increasingly inadequate in the context of cyberspace.[265] The main criticisms are rooted in their inability to address the intricate nature of cyber operations and the often-ambiguous relationships between states and cyber non-state actors.[266] The inherent nature of cyberspace facilitates anonymity and decentralization, which complicate the identification of actors responsible for cyber activities.[267]

Cyber threats conducted by private groups supported by or coordinating with states present a unique challenge: while these attacks and the singular individuals composing the groups are generally more difficult to trace compared to traditional kinetic attacks, for the state offering assistance it is often easier to secretly control or coordinate these groups and their actions.[268] This duality arises because cyber operations can be conducted anonymously, with the non-state actors maintaining plausible deniability, allowing the supporting state to shield itself from direct

---

[263] Scott J. Shackelford (2011), 971-992.
[264] Peter Margulies (2013), 496-519; Scott J. Shackelford (2011), 971-992.
[265] *ibid*.
[266] *ibid*.
[267] *ibid*.
[268] Peter Margulies (2013), 496, 500-501, 503-504, 519; Scott J. Shackelford (2011), 971-975; David D. Clark, Susan Landau, 'Untangling Attribution' (2011) 2 *Harvard National Security Journal* 531, 533 [hereinafter: "David D. Clark (2011)"].

attribution, while still benefiting from the outcomes of such activities.[269] This "attribution asymmetry" undermines the control test, which requires clear evidence of direct state control or oversight of non-state actors' actions.[270]

As a consequence, the second criticism regards the concept of plausible deniability, which is especially relevant in cyberspace.[271] Accordingly, states can easily disassociate themselves from the actions of non-state actors engaged in cyber operations, either by providing covert support or by inciting these actors to carry out attacks while maintaining a distance from direct involvement.[272] This strategic detachment allows states to avoid accountability under the traditional models of control, which rely on more explicit connections between the state and the non-state actor's actions.[273]

Thirdly, the relationship between states and non-state actors in cyberspace is evolving in ways that challenge the traditional notions of control. Unlike the conventional state-to-non-state dynamic, where non-state actors are typically subordinate to state interests, there is a growing trend where non-state actors in cyberspace seems to operate independently but actually aim to align with or further the objectives of states, supporting the latter.[274] This shift raises significant questions about the applicability of the control test, as it fails to capture scenarios where states benefit from the actions of non-state actors without exercising direct control over their conduct while receiving active support.[275]

In light of these complexities, it is clear that IL must evolve to address the realities of modern cyber interactions, ensuring that accountability mechanisms remain robust and relevant.[276] The traditional control test, as it stands, is increasingly unable to capture the multifaceted nature of cyberspace and the intricate ways in which states and non-state actors engage in cyber operations.[277] As cyber threats evolve and the actions of non-state actors in cyberspace become

---

[269] Scott J. Shackelford (2011), 971-975; David D Clark (2011), 531, 533.
[270] Peter Margulies (2013), 496, 500-501.
[271] *ibid*., 503-504, 519; Scott J. Shackelford (2011), 971-975.
[272] *ibid*.
[273] Peter Margulies (2013), 503-504, 519; Scott J. Shackelford (2011), 971-975.
[274] Scott J. Shackelford (2011), 971-1016; Michael Kenney (2015), 117-128.
[275] *ibid*.
[276] *ibid*.
[277] Peter Margulies (2013), 496-519; Scott J. Shackelford (2011), 971-992.

more sophisticated, there is an urgent need for a more tailored and nuanced approach to the attribution of cyber operations. [278]

In addressing the limitations of both the effective control and overall control tests in the context of cyberspace, several alternative theories have been developed to better account for the unique dynamics of cyber operations. Among these, two particularly noteworthy approaches are the "virtual control" approach and the "sliding scale" theory.[279]

The virtual control approach advocates for a broader interpretation of state influence. Nonetheless, this approach mainly refers to the overall control test requirements while suggesting to reverse the burden of proof on the state allegedly controlling the cyber organization.[280] In contrast, the sliding scale theory introduces a flexible but structured framework, allowing for the assessment of varying degrees of state involvement or coordination with non-state actors, from direct control to indirect support or facilitation.[281]

When comparing these approaches, the sliding scale theory appears to offer a more appropriate and effective solution, as it allows for the recognition of different levels of state control based on the specific circumstances surrounding the actions in question.[282] This theory acknowledges that states may exercise indirect influence over non-state actors, without undermining the core principle of state sovereignty.[283] By considering the degree of state involvement within the context of each situation, the sliding scale theory strikes a balance between holding states accountable for their actions and respecting their autonomy.[284] Accordingly, a flexible but structured approach, such as the sliding scale theory, offers several advantages in the establishment of accountability for cyber operations.[285]

---

[278] Peter Margulies (2013), 496-519; Scott J. Shackelford (2011), 971-992.
[279] *ibid*.
[280] Peter Margulies (2013), 514-519
[281] *Oil Platforms* (Islamic Republic of Iran v. United States of America) (Separate Opinion of Judge Higgins) [2003] ICJ Rep 161 [hereinafter: "*Oil Platforms*"]; Scott J. Shackelford (2011), 990-993.
[282] Scott J. Shackelford (2011), 990-993.
[283] *ibid*.
[284] Scott J. Shackelford (2011), 990-993; Lee A. Bygrave, *International Law and the Internet* (Oxford University Press 2016); David P. Fidler, *Cybersecurity and International Law* (Oxford University Press 2015); Ariana J. B. Mitchell, *Cybersecurity and International Law: Policy Options for a Global Regime* (2017).
[285] *ibid*.

Firstly, unlike the rigid control tests, which necessitate clear evidence of direct state control, the sliding scale model recognizes that states may exercise varying degrees of influence over non-state actors.[286] This influence can range from minimal support to direct and substantial involvement.[287] Specifically, it allows for the consideration of indirect forms of state involvement, such as providing logistical support, encouragement, or ideological backing to non-state actors engaged in cyber activities.[288] Even if a state does not maintain direct control over an actor, its facilitation or endorsement of that actor's actions can still be considered into the attribution process.[289] This helps account for the complexities of cyber interactions, where influence may not always take the form of direct orders or oversight.[290]

Secondly, the sliding scale approach involves a contextual assessment of the relationship between states and non-state actors.[291] By examining factors such as the level of coordination, the resources provided, and the intent behind a state's actions, this model offers a more comprehensive understanding of how states may benefit from cyber operations without directly orchestrating them.[292] This contextual analysis is vital in cyberspace, where the boundaries between different types of cyber activities – such as cybercrime, cyberterrorism, and state-sponsored warfare – are often blurred.[293]

Thirdly, the sliding scale theory proves to be particularly adaptable to the evolving dynamics of modern reality, where the traditional roles between states and non-state actors are increasingly reversed. In the cyber domain, it is often cyber organizations that proactively support state interests, rather than being directly controlled by the state.[294] This shifting reality challenges conventional attribution frameworks, which rely heavily on direct state control over non-state actors. The sliding scale theory ensures that states can still be held accountable for cyberattacks even when they lack direct control over the actions of non-state actors but benefit

---

[286] *Oil Platforms*, 161; Scott J. Shackelford (2011), 990-993.
[287] *ibid*.
[288] *ibid.*
[289] *ibid.*
[290] TM 2.0, Rule 11.
[291] *ibid*.
[292] *ibid*.
[293] *ibid*.; Michael Kenney (2015), 117-128.
[294] Michael Kenney (2015), 117-128.

from their support in a cooperative or mutually advantageous relationship.[295] By broadening the criteria for attribution, this theory aligns more effectively with the complexities of state and non-state partnerships in the cyber sphere, thus promoting accountability without neglecting the evolving nature of modern international peace and security threats.[296]

Finally, in the realm of IHL, the sliding scale approach holds particular significance.[297] As cyber operations and cyberattacks become increasingly integral to contemporary warfare, legal frameworks governing armed conflict must evolve to remain adaptive and responsive to these emerging forms of hostilities. The involvement of non-state actors in armed conflicts adds further complexity, as understanding the precise relationship between a non-state organization and the states involved becomes essential for determining the nature of the conflict – whether it is international or non-international – and, consequently, the applicable legal rules and protections.[298]

The sliding scale approach offers a critical tool for addressing this challenge by considering varying degrees of state influence and control over non-state actors, including indirect or partial forms of involvement. By accounting for the contextual dynamics and diverse forms of cooperation between states and cyber organizations, the sliding scale approach enhances the ability to establish state accountability and ensures that legal frameworks governing armed conflicts remain effective, comprehensive, and relevant in the digital age.[299]

In this respect, it is necessary to underline that the TM 2.0 – despite not explicitly adopting the sliding scale approach to attribution – engages with the complexity of cyber operations and state involvement, suggesting a more flexible and contextualized framework for attribution.[300] In Rule 11, the TM 2.0 addresses the issue of attribution of cyber operations conducted by non-state actors to states under IL.[301] It explains that attribution is determined by the extent of a state's control or

---

[295] Scott J. Shackelford (2011), 971-1016.
[296] *ibid*.
[297] *ibid*. 990-1016.
[298] GCI, art. 2, art. 3.
[299] GCI, art. 2, art. 3; Scott J. Shackelford (2011), 971-1016.
[300] TM 2.0, Rule 11; Peter Margulies (2013), 496-519.
[301] TM 2.0, Rule 11.

direction over the cyber operation, thus referring to the concepts of effective and overall control. Nevertheless, the Manual distinguishes between various levels of state involvement, ranging from direct control to a more indirect form of involvement.[302]

Therefore, although the TM 2.0 does not formally adopt the sliding scale approach, it acknowledges the necessity of considering varying degrees of state involvement when attributing cyber operations. This approach recognizes that a state does not need to exercise effective control in the traditional sense to be linked to the actions of non-state actors. Instead, attribution can be based on a range of influences, whether direct or indirect, that the state may exert over the cyber operation.[303] In this way, the Manual implicitly accommodates a more nuanced approach, reflecting some key aspects of the sliding scale model.

In conclusion, the sliding scale approach provides an essential legal framework for attributing responsibility in cyberspace, addressing the complexities of modern cyber operations and state-sponsored cyber threats.[304] By recognizing that states may influence non-state actors in varying degrees and by allowing for a contextual analysis of these relationships, the sliding scale offers a more comprehensive and adaptable method for ensuring accountability in cyberspace. It enhances the application of IL, specifically IHL, ensuring that legal frameworks can effectively respond to the evolving nature of cyber threats and the changing dynamics of state and non-state interactions in the digital age.

Chapter Conclusive Remarks

In conclusion, this Chapter has provided an essential overview of the key concepts related to cyberspace, cyber security, and the various cyber threats that challenge modern international law. It has examined how IL applies to cyberspace, the emerging regulations, and the growing prominence of soft law in this domain. Additionally, it has explored the significant challenges international law faces in

---

[302] TM 2.0, Rule 11.
[303] *ibid*.
[304] *Oil Platforms*, 161; Scott J. Shackelford (2011), 971-1016.

addressing cyber threats, particularly with the increasing role of non-state actors and the evolving complexities around state responsibility in cyberspace.

As attention shifts to the next Chapter (III), the focus will move to ideologically motivated cyber-attacks, specifically those that are sporadic in nature. This section will delve into how cyber-terrorism and hacktivism have traditionally been the only categories used to classify such attacks. Building on the complexities discussed in this Chapter, it will argue for the establishment of a new legal category – cyber support. This category aims to capture the role of non-state actors engaging in politically motivated cyber operations, which do not neatly fit the existing definitions of cyber-terrorism or hacktivism. This approach seeks to offer greater clarity regarding the legal challenges posed by modern cyber threats.

Looking ahead, the following Chapters will explore the escalation of ideologically motivated cyber operations into cyberwarfare, examining how these attacks can evolve into armed conflicts or take place within the context of ongoing conflicts. This Chapter will build on the preceding discussions, offering a deeper understanding of the intersection between cyber operations and IL, also in the context of warfare.

CHAPTER III

3. IDEOLOGICALLY-MOTIVATED ATTACKS: CYBER-TERRORISM, HACKTIVISTM OR CYBER-SUPPORT?

In light of the framework presented in the previous Chapter, it is evident that a concerning trend in current landscape regards the growing presence and influence of non-state actors conducting cyber operations/attacks against states or governmental entities. Over the last decades, it has been registered that most of cyber entities operating in modern panorama carry out cyber operations which are ideologically motivated.[305] The growing prevalence of this type of cyber operations/attacks combined the rapid advancements of modern technologies, have significantly affected the scale and nature of cyber threats and transnational conflicts.[306]

As previously mentioned, two main phenomena emerge as alarming threats to international security and peace: ideologically motivated cyber operations and cyberwarfare. The two categories are strictly connected, since the escalation of more sporadic acts of contentious politics can evolve into cyberwarfare or affect it. Therefore, the study will firstly analyze the issues related to the legal status of cyber entities carrying out cyber-attacks which are more isolated in nature – thus ideologically-drive cyber operations – to subsequently focus on the perpetrations of such acts in the context of cyberwarfare.

When referring to ideologically motivated cyber threats academic literature typically identifies two main subcategories, namely cyber-terrorism and hacktivism. Although, the two classifications seem to be well-distinguished at first glance, nowadays their characteristics appear to be increasingly overlapped, adding further complexity to the classification and regulation of such activities.[307] In light of this, a third hybrid category emerges as a convergence between these two groups

[305] Michael Kenney (2015).
[306] *ibid*.
[307] *ibid*.

of activities. This middle ground reflects a fusion of the characteristics of both categories, while underscoring the growing complexity of these types of cyber activities and the pressing need to reinterpret and adapt the existing legal and policy frameworks to address these evolving challenges in an effective way.

Furthermore, challenges arise in respect to the legal status of these entities due to the group-based nature of these operations. Accordingly, the need of a certain level of cooperation is crucial to the effectiveness of these attacks, as individual actions alone lack the power to destabilize governments or similar significant actors. Particularly, most of the entities conducing these type of operations present peculiar characteristics which position them between independent groups and state-affiliated organizations, causing huge difficulties in identifying their legal status and, thus, in ensuring legal accountability for their actions.[308]

On the basis of these premises, this Chapter aims to provide an in-depth analysis of the two main groups of ideologically motivated cyber operations and attacks under IL. Specifically, the study will primary define cyberterrorism and hacktivism, to subsequently introduce the idea of cyber-support and, therefore, explore the emerging convergence between these two phenomena into new forms of cyber intervention. Understanding these dynamics becomes crucial to determine the impact these activities have on global security and peace and the implications of their classification under IL.

3.1. NAVIGATING THE FINE LINE BETWEEN CYBER-TERRORISM AND HACKTIVISM

As introduced in Chapter II (*see* 2.1.3.), the category of ideologically driven cyber operations/attacks refers to a multitude of politically contentious activities carried out in and through cyberspace by groups of individuals, with the intent to promote specific political, social, or ideological agendas.[309] Two main antithetical subcategories emerge: cyber-terrorism and hacktivism.[310] The term cyber-terrorism is used to describe the most extreme form of ideologically driven attacks – despite

[308] Michael Kenney (2015); Scott J. Shackelford (2011).
[309] Michael Kenney (2015) 117-128; Doug McAdam (2001); Thomas J Holt (2017) 213-233.
[310] *See* Chapter II, 2.1.3.

remaining inadequately defined to this day. In contrast, hacktivism was initially understood as the opposite of the spectrum, encompassing those politically hostile actions which interfere with state functions and international or national stability without causing direct violence.[311] Nonetheless, recent developments have highlighted the challenges in distinguishing between the two categories, as they appear to share more overlapping traits over time. In order to navigate the fine line between cyber-terrorism and hacktivism, this study will firstly outline their characteristics, emphasizing both their similarities and the factors that set them apart, to subsequently introduce their merging points.

3.1.1. Definitions

Cyber-terrorism

The term cyber-terrorism refers to the "convergence of terrorism and cyberspace", where digital technologies become both targets and weapons.[312] This ambivalent nature of digital technologies characterizes cyber-terrorism and permits to distinguish it from conventional terrorism and the use of cyberspace for traditional acts of terrorism.[313] Prior to exploring the specific definition of cyber-terrorism and the debates surrounding it, it is essential to underline that at the present-day no universal definition of terrorism has been established under IL. It is therefore essential to first determine what will be defined as an *act of terrorism* for the purposes of this study.

According to the UN General Assembly Resolution 49/60 (1994) on the Measures to Eliminate International Terrorism, acts of terrorism can be defined as:

---

[311] Michael Kenney (2015) 117-128.
[312] Dorothy E Denning, 'Cyberterrorism' (Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, 23 May 2000) http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html accessed 11 January 2025 [hereinafter: "Dorothy E Denning (2000)"]; Barry Collin, 'The Future of Cyberterrorism' (1997) *Crime and Justice International*, March, 15-18 http://www.cjimagazine.com/archives/cji4c18.html accessed 11 January 2025; Michael Kenney (2015) 121.
[313] Michael Kenney (2015) 121.

"[c]riminal acts intended or calculated to provoke a state of terror in the general public, a group of persons or particular persons for political purposes […]".[314] In addition, Article 2(1)(b) of the International Convention for the Suppression of the Financing of Terrorism (1999) specifies that an act of terrorism is:

"[a]ny act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act."[315]

On the basis of this understating of the concept of terrorism, *cyber-terrorism* can be described as the intentional use of digital means to carry out harmful acts, with the aim of coercing governments or international organizations, spreading fear and terror through populations and undermining critical systems of modern societies for political purposes.[316] These activities share the same objectives of traditional forms of terrorism, while differentiating for their specific use of cyber tools to exploit the vulnerabilities of cyberspace.[317]

In particular, a central feature of terrorism is the intent to cause large-scale harm. In the context of cyberspace, this objective is typically achieved through the use of technical skills to target and disrupt critical infrastructures, such as energy grids, communication networks, and health systems.[318] In addition, it has been noted that acts of cyber-terrorism, as conventional terrorist acts, are usually carried out by structured groups of individuals which present a certain degree of internal organization and share common political or social objectives and agendas.[319]

While the fear of terrorism and the alarmism on the topic continue to grow, an increasing amount of people argue cyber-terrorism represents the main threat of this

---

[314] United Nations General Assembly, 'Measures to Eliminate International Terrorism' (adopted 9 December 1994) UNGA Res 49/60, UN Doc A/RES/49/60, para 3.
[315] International Convention for the Suppression of the Financing of Terrorism (adopted 9 December 1999, entered into force 10 April 2002) 2178 UNTS 229, art 2(1)(b).
[316] Michael Kenney (2015) 121-122.
[317] *ibid*.
[318] *ibid*.
[319] *ibid*., 122.

century.[320] What is particularly concerning is that, unlike traditional terrorism, cyber-terrorists can exploit the unique characteristics of cyberspace – such as anonymity, speed and low operational costs – to execute attacks that can cause similar or even greater levels of disruption.[321] Specifically, concerns arise in light of the growing interdependence of critical and essential infrastructures to digital technologies and the escalating sophistication of cyber-criminal tools, which together expand the potential for large-scale damage.[322] It was back in 1991 when in the first researches on the topic it has been warned that: "[t]omorrow's terrorist may be able to do more with a keyboard than with a bomb".[323]

Nevertheless, while it is undeniable that these cyber threats are becoming increasingly insidious and dangerous, it has been also noted how the term cyber-terrorism is often misused. States have frequently manipulated the concept of terrorism – and cyber-terrorism – to gain international consent for their unlawful actions against groups considered as political opponents or perceived as threats to their stability. This appears to be one of the reasons why a universally accepted definition has yet to be established under IL, as the lack of clarity serves the interests of states by allowing them to act more freely against their "enemies".[324] This situation results in legal uncertainty and huge difficulties in assessing whether acts of contentious politics should be labeled as cyber-terrorism or whether they should be classified under different legal categories.

Hacktivism

The concept of hacktivism also derives from the marriage of two terms, namely "hacking" and "activism".[325] The term *hacking* generally refers to "the activity of

---

[320] Michael Kenney (2015), 111-122; Joshua Green, 'The Myth of Cyberterrorism' (*Washington Monthly* 2002) http://www.washingtonmonthly.com/features/2001/0211.green.html accessed 10 January 2025; Gabriel Weimann, 'Cyberterrorism: The Sum of All Fears?' *Studies in Conflict and Terrorism*, 28.2 (2005), 131.
[321] Michael Kenney (2015) 121-126.
[322] Dorothy E Denning (2000), 20-23.
[323] *ibid.*; National Research Council, *Computers at Risk: Safe Computing in the Information Age* (National Academy Press 1991).
[324] *ibid*.
[325] Dorothy E. Denning, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', *Global Problem-Solving Information Technology and Tools* (1999) 23 https://nautilus.org/global-problem-solving/activism-hacktivism-and-cyberterrorism-the-internet-

getting into someone else's computer system without permission in order to find out information or do something illegal".[326] On the other hand, *activism* alludes to "the use of direct and noticeable action to achieve a result, usually a political or social one".[327] As a consequence, *hacktivism* describes the activity of breaking into computers systems – thus, gaining unauthorized access to computer systems and other digital technologies – in order to manipulate or damage them, with the aim of pursuing a certain social or political cause, as a form of digital civil disobedience.[328]

It is important to underline that also traditional activism can involve the use of the Internet, yet remaining distinct from hacktivism.[329] Accordingly, conventional activism often involves a non-disruptive use of the Internet, to advocate for a certain cause or to promote a specific agenda.[330] In contrast, hacktivism refers only to such hacking techniques that target selected digital systems with the aim of disrupting their normal functioning in support of a certain ideal or objective, typically without causing significant levels of harm.[331]

Focusing on "pure" hacktivism, hacktivists can be divided into two main groups: those who misuse cyberspace and those who abuses of it.[332] The first category refers to an impropriate or unethical use of cyber means and digital systems which causes not significant harm – but still considerable social or economic damage, for instance.[333] Contrarily, the second group refers to a more aggressive and violent version of hacktivism, capable of causing high levels of damage and disruption to promote social and political causes.[334] In respect to this

---

as-a-tool-for-influencing-foreign-policy-2/. accessed 3 January 2025 [hereinafter: "Dorothy E. Denning (1999)"].

[326] Cambridge Dictionary, 'Hacking' (CUP) accessed 13 January 2025 https://dictionary.cambridge.org/dictionary/english/hacking.

[327] Cambridge Dictionary, 'Activism' (CUP) accessed 13 January 2025 https://dictionary.cambridge.org/dictionary/english/activism.

[328] Michael Kenney (2015), 117-118; Dorothy E. Denning (1999), 13; Stefano Baldi, Eduardo Gelbstein, Jovan Kurbalija, *Hacktivism, Cyber-Terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace* (*DiploFoundation* 2003) 23 https://books.google.it/books?id=oKS2RtaKDm8C accessed 14 January 2025 [hereinafter: "Stefano Baldi (2003)"].

[329] Dorothy E. Denning (1999), 2.

[330] *ibid*.

[331] *ibid*.

[332] Stefano Baldi (2003), 23.

[333] *ibid*., 23-28

[334] *ibid*., 23-30.

more radical form of hacktivism, the line between hacktivism and cyber-terrorism grows increasingly blurred.[335]

Before delving into the debate regarding the convergence of these phenomena and the difficulty in disciplining these new forms of cyber threats under IL, it is essential to accurately point out their common characteristics as well as their distinguishing factors.

3.1.2. Common Characteristics And Distinguishing Factors

Common characteristics

When examining the shared traits of these two types of cyber activities, the first evident common factor lies in their ideological motivation, which shapes their acts and agendas.[336] As previously mentioned, these activities fall under the category of ideologically motivated cyber operations, as they are not conducted for personal gain or economic reasons but rather to advance social and political purposes.[337] In particular, they are both inherently rooted in political motivations. Accordingly, both hacktivists and cyber-terrorists seek to impact on economic and social systems and diminish governments' stability or ability to control specific state functions, to advocate for their cause. Additionally, they both aim to achieve global media attention, to gain material and ideological support for their actions from the above, shaping public perception to draw attention to their causes and programs.[338]

In this light, another defining characteristic is that both phenomena are grounded in asymmetric dynamics, since their adversaries typically include states, governmental entities or vast groups of individuals – actors which would traditionally hold a stronger position in traditional settings. Nonetheless, considering the unique attributes of the digital domain, the relationship between these actors is reversed in cyberspace.[339] Hacktivists and cyber-terrorist are able to exercise comparable, if not greater, power and influence in cyberspace, due to the

---

[335] Stefano Baldi (2003), 23.
[336] Michael Kenney (2015) 111-128.
[337] Chapter 2, 2.1.3.
[338] Michael Kenney (2015) 111-128; Stefano Baldi (2003), 17-42.
[339] Stefano Baldi (2003), 7-19.

lower operations costs and to the potentially more profound impact their actions can have on their targets.[340]

In this regard, a subsequent significant similarity between the two categories can be found in the tools and techniques used to carry out their attacks and achieve their programs.[341] Accordingly, they both act primarily through Denial of Service (DoS) or Distributed Denial of Service (DDoS) attacks, through which they disrupt digital systems or services, by flooding them with massive volume of traffic.[342] Through these attacks, they render the targeted systems unavailable in order to achieve financial loss, reputational damage, and military advantage or capability loss, for instance.[343] In addition, they use other common techniques, such as: websites defacement, typically to alter the normal functioning of a site to show a political message; data breaches and phishing attacks, thought which they proceed to the leak of sensitive, personal and protected information; malware deployments and Cross-Site Scripting (XSS), to infect system with malicious software and exploit the vulnerabilities of these systems to access or damage data.[344]

Finally, a common characteristic can be found in the fact that these types of activities are typically conducted by groups of individuals which present a certain degree of coordination or cooperation. Accordingly, for both categories operational coordination is not merely incidental, as it appears essential to achieve large-scale results. Without the ability to act in an organized and structured manner, the success of these operations would be significantly diminished.[345]

Distinguishing factors

While cyber-terrorism and hacktivism share a multitude of common traits, they also present a series of significant distinguishing factors. Firstly, although it is widely accepted they are both driven by political reasons and they often use the same tools, it is essential to recognize the different intentions behind their actions

---

[340] Stefano Baldi (2003), 7-19.
[341] *ibid*., 17-19.
[342] *ibid*., 17-42; Michael Kenney (2015) 111-128; Dorothy E. Denning (1999), 1-24.
[343] *ibid*.
[344] *ibid*.
[345] Michael Kenney (2015) 111-128; Stefano Baldi (2003), 7-42.

and how these serve their agendas and objectives. As previously mentioned, cyber-terrorists use destruction and intimidation as tools to spread fear and terror among the population, which is their primary method to achieve their political goals. [346] Contrarily, hacktivists commonly seek to disrupt and embarrass specific targets to raise awareness and stimulate public reflection on their causes.[347] Consequently, a distinction can be draw between cyber-attacks which inflict severe damage on critical infrastructure or financial systems to instill fear through the population and less violent cyber operations used as a form of digital protest.[348] While the former relies on terror and violence against people, property or critical infrastructures to accomplish their objectives, the latter employs disruption to merely inconvenience their victims, as a form of communication.[349]

As a result, another important distinction lies in the choice of targets for their attacks. Considering that cyber-terrorism aims to cause widespread disruption and fear to coerce governments and populations, cyber-terrorists usually target a broad and indiscriminate range of entities at the same time.[350] In particular, their main focus is on critical infrastructures and vital state services, as their destruction or destabilization can effectively create a climate of terror.[351] In contrast, when analyzing hacktivists' activities, it can be observed how they select more carefully their targets on the basis of the cause they are supporting.[352] Specifically, hacktivists operations commonly focus on attacking corporate entities or governmental institutions liked to economic and social services, usually to expose them for corruption or to advocate for more transparency and accountability.[353]

Another difference can be found in the organizational structure. Although it has been previously mentioned that both activities require the coordination of a considerable group of people to achieve successful results, the two categories of groups present different degree of cooperation between their members. When

---

[346] Michael Kenney (2015), 121.
[347] *ibid*.
[348] *ibid*., 121-122.
[349] *ibid*.
[350] *ibid*.
[351] *ibid*.
[352] Stefano Baldi (2003), 19.
[353] *ibid*., 19-29.

focusing on terrorism, it is evident that these groups typically present a more structured organization. These types of entities are typically based on a hierarchical model, in which some members are identified as leaders and give commands to the other members of the group.[354] Nonetheless, it must be noted that cyber-terrorist groups differ from traditional organizations as they present a more decentralized structure.[355] When referring to hacktivist collectives, while it is true that they are characterized by a high level of coordination between their members, their organizational model is typically based on a horizontal structure, in which all the members are generally considered equal.[356]

Ultimately, the two groups differ with regards to their legal regulation. While over the last decades terrorism has been recognized as a dangerous threat to international peace and security, hacktivism is not yet disciplined at the international level. This discrepancy reflects the underlying perception of the two phenomena: terrorism is universally considered illegal as the core aim of terrorist actions is to cause psychological coercion and physical violence; hacktivism – despite involving an illegal unauthorized access to digital systems – is often considered as a mere form of activism, especially when directed to oppressive or not democratic governments or when it is conducted against violations of human rights.[357] In particular, cyber-terrorism benefits from a certain degree of regulation due to the existence of a multitude of legal and political documents concerning offline terrorism.[358] Contrarily, hacktivism, while occasionally recognized as a potential threat when it fits into other legal categories related to cybercrimes, form

---

[354] Maura Conway, 'Terrorism and IT: Cyberterrorism and Terrorist Organisations Online' (Paper presented at the International Studies Association Annual International Convention, Portland, Oregon, 2003), 10-12 [hereinafter: "Maura Conway (2003)"].
[355] Maura Conway (2003), 10-12.
[356] Stefano Baldi (2003), 17-30.
[357] *ibid*.
[358] United Nations General Assembly, 'Measures to Eliminate International Terrorism' (adopted 9 December 1994) UNGA Res 49/60, UN Doc A/RES/49/60; International Convention for the Suppression of Terrorist Bombings (adopted 15 December 1997, entered into force 23 May 2001) 2149 UNTS 256; International Convention for the Suppression of the Financing of Terrorism (adopted 9 December 1999, entered into force 10 April 2002) 2178 UNTS 229; United Nations Security Council, UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373; United Nations Security Council, UNSC Res 1566 (8 October 2004) UN Doc S/RES/1566.

part of a gray zone, since it lacks of specific regulation under IL.[359] Some measures can be taken against who conduces these activities, but these are mostly limited to the national or regional level.[360] This means that only states or regions having adopted detailed cyber-security policies and specific legal frameworks can effectively act against these threats.

3.1.3. Where Boundaries Fade: The Merging of The Two Categories

At first glance the differences and similarities between the two classes of actions appear to be clear and distinct. Nevertheless, when analyzing the events occurring worldwide, some of their defining characteristics become more blurred than they initially seem. One of the most evident areas of overlap lies in the intent behind their actions. Nowadays, most entities recognized by media and general public as cyber-terrorists carry out cyber-attacks with the aim of generating chaos and fear to undermine state authority and influence public opinion, rather than create severe psychological coercion and cause physical violence for their own sake.[361] Today this pure fear-driven motivation cannot be found in any of the attacks registered across the globe.[362] In contrast, some of the most famous hacktivist groups are conducing operations which are increasingly intrusive and violent.[363] Specifically,

---

[359] Council of Europe, *Convention on Cybercrime* (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185; United Nations, Draft United Nations Convention against Cybercrime, finalized by the Ad Hoc Committee on 9 August 2024, pending adoption by the General Assembly. United Nations Office on Drugs and Crime, 'Hacktivism' (E4J University Module Series: Cybercrime) https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/hacktivism.html accessed 15 January 2025; API, art. 51(2), art. 51(3).

360 For instance: Italy, Codice Penale (Italian Penal Code), Regio Decreto 19 October 1930, n. 1398, revised 2024; art. 615-ter (unauthorized access to computer systems); art. 617-quater (illegal possession of data); art. 617-quinquies (disruption of computer systems); Italy, Codice di Procedura Penale (Italian Code of Criminal Procedure), Decreto del Presidente della Repubblica 22 September 1988, n. 447, revised 2024, art. 270-271 (investigations into cybercrimes); Italy, Draft Decree on Hacking (2024) Reuters; Privacy International and CILD, 'Call to Amend DDL Orlando on Hacking' (2024) Liberties; European Parliament and Council, Directive 2013/40/EU on attacks against information systems, adopted 12 August 2013 [2013] OJ L 218/8; European Union, *Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694* (Cyber Solidarity Act) [2025] OJ L 5/1; European Commission, *Cybercrime*, Migration and Home Affairs, last update 31 October 2024.

[361] Michael Kenney (2015), 121-128.

[362] *ibid*.

[363] *ibid*., 117-121.

hacktivist actions typically aim to embarrass and disrupt their targets to gain attention on a specific ideal. However, their actions have evolved from symbolic acts of protests to activities effectively capable to spread fear and terror through the population, creating a state of psychological coercion.[364] As a result, the intentions behind the two categories appear to converge more and more, due to the similar psychological impact they both have the potential to generate.

This is strictly connected to the second point of convergence: the consequences of their attacks. As mentioned above, cyber-terrorism has been often related to large-scale destruction, the targeting of vital infrastructures like energy grids, transportation systems or communication networks.[365] These assaults are intended to sow chaos, undermine governments, and destroy public confidence in state institutions and authority.[366] Contrarily, hacktivism was originally characterized by lower-stakes acts like mere website defacements or temporary service interruptions.[367] Nonetheless, the nature of their acts has evolved considerably since. In particular, hacktivist groups of today appear to conduce extremely disrupting cyber-attacks, targeting mainly healthcare systems or public safety networks and technologies, thus targeting critical infrastructures and vital state functions.[368] Also considering that they typically use the same tools and strategies, the level of violence and the severity of the consequences of their attacks on the society appear to be always more similar.

Finally, another merging characteristic lies in the organizational structures of these entities. As previously mentioned, both cyber-terrorist and hacktivist groups necessitates of the cooperation of a certain amount of people to be effective. Despite hacktivist model of coordination differs significantly from traditional terrorist organizations, more similarities can be found with cyber-terrorist entities.[369] Specifically, while traditional terrorist groups commonly operate through a hierarchical organization with centralized leadership and long-term plans, cyber-

---

[364] Michael Kenney (2015), 120.
[365] *ibid*. 121-122.
[366] *ibid*., 121-127; Stefano Baldi (2003), 33-34.
[367] Michael Kenney (2015), 117-121; Stefano Baldi (2003), 23-30.
[368] *ibid*.
[369] Maura Conway (2003), 10-12.

terrorist organizations exhibit a more flexible and decentralized structure, due to the inherent features of cyberspace and cyber capabilities.[370] On the other hand, hacktivists networks are increasingly trending toward more cohesive and organized systems of action, often under the guidance of some members of the group.[371]

This trend of convergence makes it even more difficult to differentiate between cyber-terrorism and hacktivism.[372] Closer in intent, impact, and organization, these groups raise difficult questions for existing legal and policy paradigms currently used to mitigate them. Recognizing this partial overlap will be important as we strive to develop a more sophisticated understanding of their activities and of IL's ability to effectively respond to these emergent threats.

3.2. CYBER-SUPPORT: A NEW DIMENSION UNDER THE LAW OF STATE RESPONSIBILITY

Having analyzed the features of the two antithetical categories and their points of convergence, this study suggests to forsake the rigid definitions of cyber-terrorism and hacktivism as opposing ends of the spectrum, to embrace an additional middle-ground category that can encompass a broad range of cases – one that could include most of the cyber entities in modern scenario, as many do not align with the two narrow definitions presented above. Accordingly, it has been observed that, at present, most non-state actors conducing politically motivated cyber operations target states or governmental entities in support of a certain country or population, typically those fighting for self-determination or against violations of sovereignty.

These entities do not properly fit neither in the category of cyber-terrorists – since their aim is not to spread fear and coerce governments purely for the sake of psychological coercion and physical violence – nor into the one of hacktivists – given the violent nature of their action and their frequent connection to a specific state whose interest they support. In the light of this framework, the concept of cyber-support emerges as a hybrid category.

---

[370] Maura Conway (2003), 10-12.
[371] Michael Kenney (2015), 117-121.
[372] *ibid*. 117-128.

3.2.1. Shaping The Future: The Rise Of Cyber-Supporters

The concept of cyber-support not only indicates an increasing overlap between cyber-terrorism and hacktivism, but introduces a new chapter in the relationship between non-state actors and both the states they support and the ones they oppose. Despite the lack of specific recognition of cyber-supporter legal status in academic literature and international documents, this study advocates for the establishment of this new legal category to address the regulatory gap and ensure legal accountability at the international level.

For the purposes of this research, cyber-supporters are defined as digital fighters who undertake actions that contribute providing critical resources – technical, financial, or ideological – to governments or particular interests in contentious politics. These supporters might not always be the hands that pull off cyber-attacks, but also the ones who help propagate, boost, or validate the actions of other entities, typically states or oppressed populations. Contrarily, they can also be the main perpetrators of the attacks, while coordinated and supported by other states or entities.

Their activities can involve lending expertise in encryption, coordinating between multiple cyber-actors to cause more effective disruption, and target specific entities to diminish other states' authority and capabilities. Facilitation of such activities can enable national and subnational units of government entities to overcome technical pathologies, expand their operational footprints, or scale their ideological messages. Thus, even if cyber-supporters themselves do not always execute violent cyber-attacks, their endeavors remain central to maintaining and worsening the cyber-campaigns of the groups they support. On the other hand, they can also directly carry out intrusive and destructive cyber-operations, in support of a specific country or political cause.

Cyber-support refers to more than simply spreading fear or causing disruption, moving into the realm of direct political engagement, where cyber-supporters also contribute to broader geopolitical tensions or conflicts. In this regard, cyber-supporters seem to be moved by similar objectives of hacktivists groups, while perpetrating more severe and widespread attacks, almost reaching the level of

cyber-terrorist organizations. Accordingly, this implies primary the cases in which the digital architecture of oppressive regimes or authoritarian governmental entities become main target for groups promoting pro-democracy actions, supporting human rights or sovereignty claims. Their aim is not only to inspire terror in the public but to sap the state of its strength, make its functions unstable and to erode its monopoly over information and communication. Cyber-attacks, used in this way, provide a strike against a larger political opponent, typically a state, as a form of digital resistance that serves broader political goals.

3.2.2. Enhancing The Enforcement Of State Responsibility

The shift from less intrusive and complex models of acts of contentious politics toward targeted and sophisticated engagement in cyberspace, as the ones just mentioned, muddies the waters of a legal system in which states were the central subjects and responsible under IL. The involvement of this new type of supporters blurs the lines between state and non-state actors in interesting ways, generating huge difficulties in the application and interpretation of the rules of state responsibility. Since these entities are frequently aligned with the political objectives of a specific nation or group, it raises the question of whether and how the states they support can be held accountable for their actions.

In this context, the study suggests to analyze whether such groups could be held responsible under IL through the sliding scale approach, which has been introduced in Chapter II.[373] This approach offers a finer-grained capture of the link between states and non-state actors, which can span from tacit endorsement to active facilitation of cyber operations and attacks.[374] Thus, the sliding scale theory appear to be a useful tool to assess the level of state complicity in respect of hostile attacks apparently conducted by non-state actors. It recognizes that states might not always directly coordinate or sponsor cyber-attacks but that they may nonetheless afford

[373] See Chapter II, 2.3.3.
[374] Scott J. Shackelford (2011), 990-993; Lee A. Bygrave (2016); David P. Fidler (2015) Ariana J. B. Mitchell (2017).

different levels of reciprocal support within entities conducting cyber operations in a certain context.[375]

On the lowest end of the scale, states can willfully ignore the actions of their cyber-supporters, giving them no formal endorsement, while neither deterring them nor intervening against them, as a tacit approval.[376] At the top end of the scale, states may pro-actively facilitate cyber campaigns by providing resources, training or intelligence, effectively reining in their activities to achieve an intended strategic outcome.[377] For example, a state might clandestinely spur cyber-activists to work on undermining the digital infrastructure of a foreign enemy, creating plausible deniability while pursuing its geopolitical goals. Through the application of the sliding scale approach, in this scenario the state's indirect involvement may reach the level to attribute responsibility for such cyber-attacks to the state under IL.

Therefore, the sliding scale approach allows for a subtler analysis of the legal and political implications of cyber-support. It acknowledges the diversity of state connection to their cyber-supporters and how the degree of involvement may, depending on the level of the connection, implicate the state for the effects of those actions.[378] These dynamic challenges the classical understanding of notions of state sovereignty and non-interference, since cyber-support can be considered a form of indirect aggression or interference in internal affairs of another state. In this regard, some legal scholars argue that, to the extent that cyber-operations or cyber-support is seen as sufficiently linked to a state's foreign policy goals, it may incur global responsibilities for violations of IL, like the ban on the use of force or interference in the affair of another state.[379]

Overall, cyber-supporters play an important role in the context of ideologically-motivated cyber-attacks. Although they do not always carry out the cyber-attacks themselves, their support is essential for perpetuating and magnifying the

---

[375] Scott J. Shackelford (2011), 990-993; Lee A. Bygrave (2016); David P. Fidler (2015) Ariana J. B. Mitchell (2017).
[376] *ibid*.
[377] *ibid*.
[378] *ibid*.
[379] *ibid*.

operations and strategies of the state they assist. In light of this, using a sliding scale approach to analyze the spectrum of state responsibility on a case-by-case basis enables legal scholars and policy experts to engage more meaningfully with the nuanced dynamics of these situations. Such an approach would be more flexible and context-specific in applying and adjusting IL's rules to the complex and dynamic relationship between states and non-state cyber-actors.[380] It creates a legal structure through which the international community can continue to hold states accountable for their complicity in cybercrimes and/or cyber conflicts, even whether they try to dissimulate their actions through the complicity of non-state actors.

3.2.3. Case Study: Anonymous [381]

To gain a deeper understanding of the issues at hand, this research will incorporate a case study. Specifically, it will focus on the Anonymous group, widely recognized as one of the most influential and active cyber entities, conducing ideologically motivated cyber-attacks in the modern era. While Anonymous' members have been often identified as cyber-terrorists from the general public and media, some scholars contend that their actions fall under the category of hacktivism, elevating it to unprecedent levels.[382] In order to better understand the debate surrounding the groups' classification, the research will now provide a brief overview of their rise and characteristics.

The online group Anonymous has originated from the discussion platform "4chan" between 2003 and 2004.[383] The "b" section of the platform, which allows posts on any topic, from adult content to politics, was the initial gathering place for

---

[380] Scott J. Shackelford (2011), 971-1016.
[381] The following subsection is drawn from the Master's Thesis I authored for Utrecht University as part of the Double Degree Program in Public International Law in collaboration with LUISS University. This work constitutes an integrated thesis, developed in accordance with the academic standards and requirements of the Double Degree Program.
[382] Michael Kenney (2015), 118.
[383] Russell Buchan, 'Cyber Warfare and the Status of Anonymous under International Humanitarian Law' (2016) 15(4) *Chinese Journal of International Law*, 741-742 [hereinafter: "Russell Buchan (2016)"]; Angelo Stirone, 'Hacking and International Humanitarian Law' (2020) *Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict* 3(1/2), 124 [hereinafter: "Angelo Stirone (2020)"].

some of the first Anonymous members.[384] Over the years, individuals within this digital community, commonly referred to as "Anons", have started to engage in discussions on current issues, establish shared objectives, and subsequently carry out cyber activities targeting specific individuals or entities for "lulz".[385] This term has been used to describe the activity of deriving entertainment from others' expense while also drawing attention to a particular cause.[386]

The movement quickly expanded to other communication channels and chat services, such as Internet Relay Chat systems (like Anonnet, AnonOps, and AnonPlus), as well as regional forums (like Anonita, YourAnonUsa, and AnonNewsDE).[387] Since the creation of the group, Anonymous has presented itself as a collective of individuals with shared beliefs who leverage the online realm for protest activities, by protecting their identities through anonymity.[388]

The iconic Anonymous logo is indeed modeled after the United Nations emblem, by featuring a globe within a laurel wreath and a headless figure in a suit and tie, symbolizing anonymity and decentralization.[389] Another identifying symbol is the Guy Fawkes mask, which members wear publicly and in social media communications to conceal their identities.[390] The mask references Guy Fawkes, a 17th-century figure known for attempting to bomb the House of Lords.[391]

In its early stages, the group gained global attention by targeting the Church of Scientology, through the Project Chanology.[392] This marked the beginning of their organized efforts taking on a political dimension.[393] Anonymous later launched

---

[384] Angelo Stirone (2020), 124.
[385] Russell Buchan (2016), 741-742.
[386] *ibid*.
[387] Angelo Stirone (2020), 124.
[388] Text Anon, 'We are Anonymous. We do not forgive. We do not forget' (Dazed, 2013) [hereinafter: "*Anonymous Manifesto*"], accessed 10 May 2024, <https://www.dazeddigital.com/artsandculture/article/16308/1/we-are-anonymous-we-do-not-forgive-we-do-not-forget>
[389] Anonymous Logo (*1000Logos*, 2024) <https://1000logos.net/anonymous-logo/#:~:text=Meaning%20and%20history,symbol%20of%20anonymity%20and%20decentralization> accessed 10 May 2024.
[390] *ibid*.
[391] *ibid*.
[392] G. Sands, What to Know About the Worldwide Hacker Group 'Anonymous' (*ABCNews*, 2016) <https://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302> accessed 10 May 2024 [hereinafter: "G. Sands (2016)"]; Stirone (2020), 124.
[393] *ibid*.

Operation Payback in support of WikiLeaks and its founder, Julian Assange, against opponents of Online Copyright Infringement Liability Limitation Act.[394] The group initially targeted Aiplex Software, to further attack several anti-copyright infringement organizations, such as the Motion Picture Association of America, and several law firms involved in copyright infringement prosecutions.[395] This operation involved a massive DDoS attack, engaging over 7,000 participants and lasting several days.[396] Botnets, or networks of compromised computers, were used to overwhelm targets with a flood of requests, disrupting or halting their services.[397]

The group have continued to gain notoriety through the launch of massive cyber-attacks on major private entities like PayPal, MasterCard, Sony and all the main companies or banks that have frozen Assange's accounts or denied him service.[398] By late 2010, the Anonymous movement had grown beyond the confines of 4chan, emerging as a formidable online "army".[399] Upon agreeing to support a particular cause, group members engage in discussions to identify potential targets.[400] Subsequently, they analyze the cyber vulnerabilities of the chosen target and decide on the appropriate cyber operation to achieve the desired disruption or harm, such as website defacement, DDoS attacks, data modification or deletion, exfiltration and leakage of sensitive information, among others.[401] Those planning to launch a cyber-attack will either procure or develop the necessary computer malware

---

[394] G. Sands (2016); Stirone (2020), 124.; Operation Payback, <https://www.youtube.com/watch?v=kZNDV4hGUGw> accessed 10 May 2024.
[395] 'Operation Payback', *Radware* <https://www.radware.com/security/ddos-knowledge-center/ddospedia/operation-payback/> accessed 10 May 2024.
[396] Angelo Stirone (2020), 124.
[397] *ibid*.
[398] Russel Buchan (2016), 742. Mathew J. Schwart, 'Anonymous: 10 Things We Have Learned In 2013' (*DarkReading*, 2013) <https://www.darkreading.com/cyberattacks-data-breaches/operation-payback-feds-charge-13-on-anonymous-attacks> accessed 10 May 2024.
[399] Angelo Stirone (2020), 124; G. Coleman, Our Weirdness Is Free, <https://canopycanopycanopy.com/contents/our_weirdness_is_free> accessed 10 May 2024.
[400] Buchan (2016), 741-742; Parmy Olsen, 'We are Anonymous: Inside the Hacker World of LulzSec', *Anonymous and the Global Cyber Insurgency* (2012) [hereinafter: "Parmy Olsen (2012)"].
[401] *ibid*.

themselves, or rely on proficient members within the group to obtain or create the malware on their behalf.[402]

Consequently, the group has moved up to the next level by targeting governmental organizations such as the CIA, NATO, and governments accused to perpetrate violent actions against self-determination and pro-democracy demonstrators in Tunisia, Libya, and Uganda during the Arabic spring.[403] In addition, in 2012 the group was actively involved in facilitating the revolution of the people of Egypt, after President Mubarak shut down the internet. While the specific aims and objectives of Anonymous may vary, the primary focus of the group has been demonstrated to revolve around safeguarding fundamental human rights, including the rights to self-determination, liberty, freedom of expression, and association.[404]

The severity of Anonymous' actions and its political involvement in the fight for human rights escalated in November 2012, when they engaged in a "cyberwar" against Israel's online infrastructure in response to the severe civilian casualties occurred in Gaza, and again in 2014 – when Israeli military forces were again deployed into Gaza worsening the humanitarian crisis – through the implementation of more sophisticated, intrusive and widespread cyber-attacks.[405] Particularly, the online profiles of high-ranking Israeli government officials were hacked, leading to the exposure of their private information on the web.[406] In addition, cyber attackers defaced several government websites, including those of the Ministries of Education and Finance, by exposing the cruelties of Israeli forces in Palestine directly on the websites.[407]

Between the multitude of cyber-operations conducted by the group over the years, another remarkable operation that has been launched by the group is the

---

[402] Angelo Stirone (2020), 124; G. Coleman, Our Weirdness Is Free, <https://canopycanopycanopy.com/contents/our_weirdness_is_free> accessed 10 May 2024.
[402] Buchan (2016), 741-742; Parmy Olsen (2012).
[403] Russell Buchan (2016), 742.
[404] *ibid*., 741-742.
[405] *ibid*., 742-743; David Gilbert, '#OpSaveGaza: Anonymous Continues Cyber-Campaign Knocking Israeli Ministry of Defence Website Offline' (*International Business Times*, 2014) <www.ibtimes.co.uk/opsavegaza-anonymous-continues-cyber-campaign-knoc king-israeli-ministry-defence-website-offline-1457580> accessed 10 May 2024.
[406] *ibid*.
[407] *ibid*.

#OpParis, in November 2015, during which the cyber-organization attacked the notorious terrorist group ISIS.[408] Despite being significantly affected by the numerous arrests in the United States during the early 2010s, the collective has returned to be highly active again following the murder of George Floyd in 2020.[409] In the meantime, since 2014 Anonymous has started conducting cyber-attacks against Russia, in favor of Ukraine's sovereignty and the right of self-determination of its people.[410] The group's attacks against Russia intensified in 2022, after the escalation of the confrontations and the beginning of the invasion of Ukraine.[411]

While they appear to be driven by "activist" intentions, their participation in the conflict between Russia and Ukraine has shown a notable increase in the complexity and potential for large-scale harm of their attacks. In addition, the blurred dynamics characterizing the group's affiliation with Ukraine and the support provided to its IT Army illustrates the complex relationship between these types of entities and states, determining huge difficulties in assessing responsibility for their actions. More information regarding the cyber-confrontation occurring between Anonymous Russia and Ukraine will be presented in the subsequent Chapter. In light of this framework, this cyber entity and its operations appear to be a clear illustration of the blurred convergence between hacktivism and cyber-terrorism. In light of this, the Anonymous group serves as a fitting example of cyber-supporters.

Chapter Conclusive Remarks

Considering the rapid evolvement of digital technologies and the proliferation of cyber non-state actors conducing always more violent attacks against national and international stability, serious concerns arise in respect to the future consequences of these activities in light of the lack of regulation and, thus, of legal

---

[408] Russell Buchan (2016), 742-743; Andrew Griffin, 'Anonymous War on ISIS: Online Activists Claim to have Foiled Terror Attack on Italy as Part of "Operations ISIS"' (*The Independent*, 2015) <https://www.independent.co.uk/tech/anonymous-war-on-isis-online-activists-claim-to-have-foiled-terror-attack-on-italy-as-part-of-operation-isis-a6788001.html> accessed 10 May 2024.
[409] David Molloy and Joe Tid, 'George Floyd: Anonymous hackers re-emerge amid US unrest' (*BBC* 2020) <https://www.bbc.com/news/technology-52879000> accessed 10 May 2024.
[410] Denys Svyrydenko (2022), 40.
[411] *ibid*.

accountability. In particular, significant fears emerge with regards to the dangerous potential of cyber groups' intervention against vital state functions and infrastructures, which has become apparent with the events occurred in the last decade. In addition, the blurred relationship intercurrent between these types of entities and states present auxiliary difficulties in assessing legal responsibility for such actions. As discussed above, the current legal framework does not offer suitable legal categories and rules to discipline the dynamics of today. While states delay in establishing a widely-accepted legal response, a new interpretation of the existing rules must be found in order to mitigate the consequences of it.

Having examined the characteristic and legal classifications related to the conduct of ideologically motivated cyber operations which are sporadic in nature, the study will now focus on the consequences of the escalation of these activities into forms of cyberwarfare. Accordingly, it is in this context that main concerns arise, since the reiterated intervention of cyber groups into international or national conflicts have demonstrated to be able cause similar, if not greater, harm and loss than conventional non-state actor's participation. Additionally, the different legal classification of cyber groups' involvement under IHL – depending on their relationships with the state they oppose and the one they act in support with – leads to the application of diverse legal regimes and rules for both states and non-state actors. Therefore, the identification of the legal status of cyber non-state actors involved in acts of cyberwarfare becomes even more vital in this context.

CHAPTER IV [412]

4. INTERVENTION OF CYBER NON-STATE ACTORS IN TIME OF WAR

While the preceding Chapters provided a foundation on the issues related to the proliferations of cyber entities in modern scenarios and their threats to international security and peace, this Chapter transforms the scope from the broader IL context to the more specific framework of IHL. Accordingly, Chapter II introduced the significant definitions and addressed the challenges cyber threats pose to conventional doctrines of IL, such as state sovereignty and attribution. Subsequently, Chapter III focused on one of the main cyber threats of the modern era: ideologically motivated cyber operations. In this respect, the study has outlined the characteristics of the main legal subcategories by investigating cyber-terrorism and hacktivism, to consequently advocate for the recognition of a new emerging phenomenon which presents points of convergence of the two subgroups, namely cyber-support. These discussions underscored the difficulties in identifying the legal status of cyber non-state actors under IL and the concerns related to the increasing political involvement of such entities, which highly complicates the recognition of the intricate interplay between states and non-state actors, thus their accountability, and deeply influences international relations.

Having examined these cyber operations and legal categories in respect to isolated or sporadic attacks aiming at achieving specific political and social goals, in this Chapter the analysis shifts to the context of armed conflict, where the legal and practical implications of these types of operations become particularly concerning. Specifically, the subsequent Chapters investigate how the legal classifications and challenges previously outlined apply when ideologically driven cyber operations/attacks escalate to armed conflict or when they are conducted in

[412] The following Chapters (IV, V and VI) are drawn from the Master's Thesis I authored for Utrecht University as part of the Double Degree Program in Public International Law in collaboration with LUISS University. This work constitutes an integrated thesis, developed in accordance with the academic standards and requirements of the Double Degree Program.

the context of an ongoing conflict. This is not a purely hypothetical situation; recent events have underscored the potential and actual dangers associated with these scenarios, raising significant concerns, especially with respect to the applicability of IHL to cyberspace and cyber non-state actors. By examining the implications of the transfer of the legal categories previously introduced in the context of armed conflicts, the subsequent Chapters will better analyze the difficulties in assessing the legal status of such entities and the consequences of the different classification under IHL.

Before delving into the second main part of this research, it is necessary to briefly define some introductory concepts to facilitate a comprehensive grasp of the legal framework. Specifically, this Chapter will commence by providing a definition of cyberwarfare, concept which will be clarified through the examination of the application of IHL within cyberspace. Subsequently, the study will delineate the characteristics of cyber-operations and cyber-attacks pertinent to the research objectives in the specific context of IHL. Having already introduced Anonymous' characteristics and history, this Chapter will also present the relevant facts of the digital conflict intercurrent between Russia, Ukraine, Anonymous and the multitude of cyber non-state actors involved. In doing so, the study aims to elucidate the group's engagement in this specific conflict, in order to give us solid basis to consequently analyze the involvement of these types of cyber actors in cyber hostilities. In particular, the case study will be used to assess whether entities operating like the ones at stake shall be assimilated to terrorist organized armed groups or whether they shall be regarded as cyber-supporters, and thus, co-belligerents of other states or entities in ongoing conflicts.

4.1. CYBERWARFARE

Having already introduced the term cyberwarfare in the classification of cyber threats, it is now essential to better establish what is included in its notion. Given the absence of a universally accepted definition under IL, it is imperative to first introduce the definition of cyberwarfare that will be utilized for our analysis. While the general term warfare refers to the conduct of military hostilities in the context of an armed conflict, the notion of cyberwarfare will be used to refer to the conduct

of hostilities through cyber means and methods, to which IHL applies.[413] To understand the complexities of this term, the research will now underline what is included in the notion of cyberwarfare by identifying how IHL applies in cyberspace.

4.1.1. Applicability Of IHL In Cyberspace

In respect to the application of the IHL framework, it is crucial to emphasize that this branch of law is applicable only upon the determination of the existence of an armed conflict, which may be either international or non-international in nature.[414] As enshrined in Article 2 of the Geneva Conventions (GCs), an armed conflict of international character can be defined as any resort to armed violence between states.[415] While, under Common Article 3 GCs, an armed conflict of non-international nature can be established when there is protracted armed violence between governmental forces and an organized armed group or directly between armed groups.[416] It is important to emphasize that, regardless of the means or methods of warfare employed, IHL applies to the targeting of any person or object occurring during an armed conflict.[417]

Although originally shaped on the basis of an "offline" world, it is now widely acknowledged that these regulations also apply in the realm of cyberspace.[418] Nevertheless, it is important to acknowledge that not every military activity carried out in cyberspace can be directly classified as cyberwarfare. In light of the applicable legal framework, as interpreted by the International Group of Experts (IGE) in the Tallin Manual 2.0 (TM2.0), cyberwarfare mainly refers to two categories: cyber-operations executed in the context of an ongoing confrontation which has already reached the level of armed conflict; cyber-attacks which have

---

[413] Nils Melzer, *Cyberwarfare and International Law* (UNIDIR Resources, 2011), 4 [hereinafter: "Nils Melzer (2011)"].
[414] GCIII, art. 2, art. 3; *Prosecutor v Tadić* (*Trial Chamber*), Case No IT-94-1-T, Judgment, International Criminal Tribunal for the Former Yugoslavia (ICTY), 7 May 1997, [hereinafter: '*Tadić Judgement'*].
[415] GCIII, art. 2.
[416] GCIII, art. 3.
[417] TM2.0, Rule 92.
[418] *ibid*., Part IV.

reached the threshold of recourse to 'armed force between States' for IACs, or 'protracted armed violence' between governmental forces and organized armed group in respect of NIACs.[419]

Considering the broadness of the discussion and the scope of this research, the analysis will solely concentrate on two of the presented scenarios. Chapter IV will examine whether the cyberattacks under consideration align with the second category, by investigating whether the cyber-hostilities occurred between Anonymous and Russia have reached the threshold to establish a NIAC. Subsequently, Chapter V will focus on the same cyber-threats, analyzing them as cyber-operations carried out within the context of an ongoing IAC, namely the conflict between Russia and Ukraine.

4.1.2. Cyber-Operations And Cyber-Attacks Under IHL

Having presented the concept of cyberwarfare, it is essential to shortly introduce the characteristics of cyber-attacks that are encompassed by IHL and will consequently be the focus of our research. The concept of "attack" holds significant importance within IHL, as it presents the basis for a multitude of core regulations regarding the rights and duties arising during armed conflicts.[420] In this regard, the widely accepted definition of attack provided under Article 49(1) of the Additional Protocol I to the Geneva Conventions (API) has triggered several issues when first applied to cyber-operations.[421]

According to Article 49(1), "attacks means acts of violence against the adversary, whether in offence or defence."[422] Although it may initially appear challenging to identify cyber-attacks that meet the necessary threshold, it is now well established under IHL that "acts of violence" are not confined to actions involving kinetic force.[423] The scope of the notion of "attack" lies on the violence

---

[419] TM2.0., Rules 80, 82, and 83.
[420] *ibid*., Rule 92.
[421] API, art. 49(1).
[422] *ibid*.
[423] Yoram Dinstein, 'Computer Network Attacks and Self-Defense', in Michael Schmitt and Brian O'Donnell (eds), *Computer Network Attack and International Law* (2002), 373 [hereinafter: "Yoram Dinstein (2002)"]; Michael Schmitt (2011), 6-7.

of the consequences of the attack and not on the nature of the activities conducted.[424]

Accordingly, the IGE has defined a cyber-attack falling under the scope of IHL 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."[425] The term "cause" extends beyond the impacts on the targeted cyber system to include any foreseeable damage, destruction, injury, or death.[426] While cyber-attacks typically do not involve direct physical force, they can still lead to significant harm to individuals or objects. Nonetheless, it has been clarified that operations targeting data can also be classified as attacks under IHL, despite the targets being non-physical entities.[427]

When an attack on data leads to foreseeable harm or destruction of physical objects or individuals, those entities become the "object of attack", thereby categorizing the operation as an attack.[428] In this regard, operations targeting data that are essential for the functioning of physical objects may also qualify as attacks.[429] Accordingly, the IGE extensively debated whether causing a cyber-interference in respect to the functionality of an object may amount to damage or destruction under the presented framework.[430] The majority of the Experts believed that such interference qualifies as attack if physical components need replacement for functionality restoration.[431] The Group also discussed the scenarios in which reinstalling the operating system or specific data is necessary for the targeted cyber infrastructure to function as intended.[432] Whether the operation deleting or altering

---

[424] Yoram Dinstein (2002), 373; Michael N. Schmitt, 'Cyber Operations and the Jud Ad Bellum Revisited' (2011) 56 *Vill L Rev* 569 [hereinafter: "Michael N. Schmitt (2011)"].
[425] TM2.0, Rule 92; Giovanni Biggio, *Humanizing the Law of Cyber Targeting: Human Dignity, Cyber-Attacks and the Protection of the Civilian Population* (PhD thesis, University of Sheffield 2019) [hereinafter: "[Giovanni Biggio (2019)]".
[426] TM2.0, Rule 92, 5.
[427] *ibid*., 6.
[428] *ibid*.
[429] *ibid*.
[430] *ibid*.
[431] *ibid*., 10.
[432] *ibid*. 11.

data renders the infrastructure unable to function as designed, it shall be regarded as an attack according to the majority of Experts.[433]

Additionally, cyber-operations causing large-scale disruptions without physical damage have been taken into consideration, by concluding that they cannot be regarded as attacks under IHL.[434] In light of the specific characteristics of cyber-confrontations, some scholars have agreed to extend even more the scope of the definition through a systematic "effects-based" interpretation.[435] In particular, it has been noted that, when defining military objects, Article 52(2) API clearly put on the same level "total or partial destruction" with "capture and neutralization" of military objects.[436] Consequently, by combining Article 49(1) with Article 52(2) API, it is evident that the term "attack" shall be understood to encompass not only actions resulting in acts of violence, but also every operation that seeks to render military objectives ineffective in order to gain a definite military advantage.[437]

As anticipated above, it is important to underline that the definition of cyber-attack is not the parameter to establish whether cyber-operations are governed by IHL.[438] Despite cyber-attacks being the most common form of cyberwarfare, also cyber-operations not reaching the threshold of attack under Article 49(1) API can fall under the scope of IHL whether they are conducted in the context of an ongoing armed conflict.[439] In this respect, the applicability of the relevant legal framework depends on whether the operations at stake constitute "hostilities" within the meaning of IHL.[440] A cyber-operation is considered to be part of hostilities whether it directly inflicts the required level of harm (direct causation) and it is intentionally conducted to benefit one party in a conflict while disadvantaging the opposing party

---

[433] TM2.0, Rule 92, 11.
[434] *ibid*., 13.
[435] Knut Dörmann, 'The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint', in Karin Byström (ed.), *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, 17–19 November 2004, Stockholm Sweden*, (Swedish National Defence College, 2004), 16 [hereinafter: "Knut Dörmann (2004)"].
[436] *ibid*.; Nils Melzer (2011), 26; API, art. 52(2).
[437] Nils Melzer (2011), 25-26; TM2.0, Rules 80-92.
[438] TM 2.0, Rules 80, 82, 83, 92.
[439] *ibid*., Rule 82.
[440] *ibid*.

(belligerent nexus).[441] Consequently, cyber operations intended to disrupt or disable an enemy's radar or weapons systems, logistical supplies, or communication networks are considered part of hostilities and must adhere to IHL regulations on conduct during conflict, despite not resulting in physical damage.[442] Similarly, cyber activities consisting in infiltrating an enemy's computer network to erase targeting information, alter military commands, or tamper with, encrypt, exploit, or destroy critical data that negatively impacts the opponent's ability to wage war, fall under the IHL framework.[443]

4.2. ANONYMOUS AND THE RUSSIA-UKRAINE CONFLICT

As previously stated, the research will be conducted through the use of the case-study method, by focusing on Anonymous' behavior and its operations conducted against Russia in the context of the conflict between the latter and Ukraine. Having introduces the group's characteristics in the previous Chapter, it is now essential to highlight the relevant facts of the conflict occurring between Russia, Ukraine, Anonymous and the multitude of cyber actors involved – specifically with regards to the most active phase of the conflict in 2022 – to proceed with the investigation on the status of these new emerging actors under IHL.

4.2.1. The Russia-Ukraine Cyber-Confrontations

The hostilities between Russia and Ukraine commenced in February 2014 when Russia annexed Crimea and started supporting militants in the Donetsk and Luhansk People's Republics against Ukrainian military forces, sparking a fierce conflict that extended across the Donbas region.[444] Since the early stages of the conflict, cyber warfare has been a crucial component.[445] Russian state-linked

[441] Nils Melzer (2011), 27-28.
[442] *ibid*.; TM2.0, Rule 80.
[443] TM2.0, Rule 80.
[444] *ibid*.
[445] *ibid*.

groups like "Sandworm" have been allegedly involved in numerous hostile cyber-activities targeting Ukrainian governmental, military, and civilian systems.[446]

Significant events include the *NotPetya* "ransomware" attack, which affected Ukrainian governmental networks and businesses, eventually spreading internationally and causing an estimated $10 billion in losses in 2016.[447] The conflict also saw major cyber sabotage against essential civilian infrastructure, such as the cyberattacks on the Ukrainian power grid by BlackEnergy and Industroyer malwares in December 2015 and December 2016, which impacted hundreds of thousands of civilians.[448]

Nevertheless, the turning point of the cyber-conflict can be linked to the events occurring immediately after the official invasion of Ukraine started.[449] Accordingly, from January 2022 to September 2023, the CyberPeace Institute recorded a total of 2,776 cyber incidents perpetrated by 106 distinct threat actors.[450] On one hand, Russia's suspected cyber activities have continued to increment, involving a combination of DDoS attacks, wipers, and other malware.[451] On the other hand, an increasing number of cyber operations have been executed by non-state actors in support of Ukraine, including the Cyber Partisans of Belarus (CPB), Anonymous and various other entities or individual hackers.[452]

In particular, immediately after the invasion, on 24 February 2022, Anonymous has officially communicated on Twitter – today "X" – the beginning of its cyberwar

---

[446] Giovanni Biggio (2024), 4.
[447] *ibid.*; Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyber Attack in History' (*Wired*, 2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 29 May 2024.
[448] Giovanni Biggio (2024), 4; Pavel Polityuk, Oleg Vukmanovic, and Steven Jewkes, 'Ukraine's Power Outage Was a Cyber Attack: Ukrenergo', (*Reuters*, 2017) <https://www.reuters.com/article/world/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BB/> accessed 29 May 2024.
[449] Anh V. Vu, and others, 'Getting Bored of Cyberwar: Exploring the Role of Low-Level Cybercrime Actors in the Russia-Ukraine Conflict' (Proceedings of the ACM on Web Conference, 2024), 1596 [hereinafter: "Anh V. Vu (2024)"].
[450] CyberPeace Institute, 'Cyber Attacks in Times of Conflict, Platform #Ukraine' (2023) <https://cyberconflicts.cyberpeaceinstitute.org/> accessed 29 May 2024 [hereinafter: "CyberPeace Institute (2023)"]
[451] Giovanni Biggio (2024), 4-5.
[452] *ibid.*; Väljataga, Ann, 'Cyber Vigilantism in Support of Ukraine: A Legal Analysis' (2022) *NATO Cooperative Cyber Defence Centre of Excellence* [hereinafter: "[Ann Väljataga(2022)"].

against Russia.[453] On the same day, the members of the group targeted hundreds of Russian and Belarussian databases, Russian governmental websites and state media outlets, such as the notorious Russia Today.[454] During the following days, several essential governmental websites were taken down or compromised (e.g. the Kremlin and the Ministry of Defence), sensitive data of governmental offices were collected, Russian military information was released and messages against Russian propaganda were spread all over Russian websites and media.[455]

Among the various targets, the Russian agency Roscosmos, responsible for overseeing satellite operations in space, was attacked, leading to its paralysis.[456] Anonymous focused its efforts on targeting the largest possible number of strategic official entities and government institutions of the Russian state.[457] In reaction, one of the most active pro-Russian cyber-organizations, KillNet, has claimed to have shut down Anonymous' website.[458] Nevertheless, the group immediately denied the allegations and continued to carry out attacks against Russia and its cyber-supporters.[459] Simultaneously, on 26 of February 2022, the Minister of Digital Transformation and First Vice Prime Minister of Ukraine, Mykhailo Fedorov, instituted via Telegram a proper Ukrainian IT Army, by invoking the support of any professional in the field.[460]

---

[453] Anonymous @YourAnonOne, (Twitter, 2022) <https://x.com/YourAnonOne/status/1496965766435926039?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496965766435926039%7Ctwgr%5E2b2839cb70395f2111429a52331a3adc1f0ce352%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia> accessed 20 April 2024; Dan Milmo (2022).

[454] Peter Ray Allison, 'The cyber security impact of Operation Russia by Anonymous' (*ComputerWeekly.com*, 2022) <https://www.computerweekly.com/feature/The-cyber-security-impact-of-Operation-Russia-by-Anonymous> [hereinafter: "Peter Ray Allison (2022)"].

[455] *ibid*.; Anonymous @YourAnonOne, (*Twitter*, 2022) <https://x.com/YourAnonNews/status/1510494900713840641> and <https://x.com/YourAnonNews/status/1497574730282541060> accessed 10 May 2024.

[456] Denys Svyrydenko (2022), 44.

[457] *ibid*.

[458] CheckPoint Research Team, 'Fake News of Cyber Attacks Fast-Spreads, as Conflict between Russia and Ukraine Escalates' (*CheckPoint*, 2022) <https://blog.checkpoint.com/security/hacktivism-in-the-russia-ukraine-war-questionable-claims-and-credits-war/> accessed 30 May 2024.

[459] *ibid*.

[460] Mikhailo Fedorov, 'We Are Creating an IT Army' (*Twitter*, 2022) <https://x.com/FedorovMykhailo/status/1497642156076511233> accessed 20 April 2024.

The Minister's appeal for assistance garnered substantial international support, reportedly attracting 400,000 individuals to join the IT Army during its first week of establishment.[461] Indeed, the IT Army's hybrid structure is able to merge the operational efficiency of a formal government agency with the flexibility of a volunteer force.[462] The IT Army asserted responsibility for numerous cyber operations targeting Russian entities, such as the Moscow Stock Exchange and Sberbank.[463] Simultaneously, Russian cyber-actors launched several disruptive and destructive cyberattacks against Ukrainian targets and their supporters through the use of 12 different variants of malwares, impacting all the relevant sectors of the country.[464] Some of these attacks were attributed to the Armageddon group, which has been demonstrated to be linked to Russia's Federal Security Service (FSB).[465]

In early March, cyberattacks on local government websites spreading false information about Ukrainian surrender were reported by the Security Service of Ukraine (SBU).[466] Around the same time, SpaceX's Starlink terminals, providing supplemental internet to Ukraine, were jammed.[467] In late March, suspected Russian actors disrupted Ukrtelecom, causing significant internet outages.[468] In early April, Russia military intelligence (GRU) cyber actors known as Sandworm tried to deploy Industroyer2 malware against high-voltage electrical substations in Ukraine to cause power outages.[469] They moved from the IT network to the

---

[461] Sam Schechner, 'Ukraine's "IT Army" Has Hundreds of Thousands of Hackers, Kyiv Says' (*The Wall Street Journal*, 2022) <https://www.wsj.com/livecoverage/russia -ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands -of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX> accessed 30 May 2024.
[462] *ibid*.
[463] Thomas Brewster, 'Moscow Exchange, Sberbank Websites Knocked Offline – Was Ukraine's Cyber Army Responsible?' (*Forbes*, 2022) <https://www .forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank -websites-knocked-offline-was-ukraines-cyber-army-responsible/?sh=5dda2477cae3> accessed 30 May 2024.
[464] Canadian Centre for Cyber Security, *Cyber Threat Bulletin: Cyber Threat Activity Related to the Russian Invasion of Ukraine* (2022), 2 [hereinafter: "*Cyber Threat Bulletin*"]; Microsoft Digital Security Unit, *An Overview of Russia's Cyberattack Activity in Ukraine* (Digital Security Unit 2022).
[465] *Cyber Threat Bulletin*, 2.
[466] *ibid*.
[467] *ibid*.
[468] *ibid*.
[469] *ibid*., 2-3.

industrial control system network. CERT-UA, with Slovak internet security company ESET, protected the network.[470]

In May 2022, the Russian hacktivist group XakNet breached the Ukrainian Ministry of Foreign Affairs, leaking documents online and offering rewards for analyses.[471] In the meantime, pro-Ukraine organizations, such as Anonymous, continued to carry out massive attacks against Russia within the coordination of the IT Army, but also independently.[472] Particularly, on 10 March Anonymous declared to have hacked the database of the Roskomnadzor, the Russian federal agency controlling and censoring Russian communications, mass media and information technology, by releasing to the public more than 360.000 documents.[473]

Following numerous cyber-threats between the two entities and, specifically, after the attacks carried out by the pro-Russia group Killnet against European institutions in protest of sanctions imposed on Russia, tensions between Anonymous and Killnet escalated significantly.[474] Consequently, on May 21st 2022, Anonymous declared cyberwar against Killnet by taking their website offline.[475] Although the number of cyber operations related to the Russia-Ukraine conflict has decreased since May 2022, the activity remains substantial.[476] Additionally, the technologies and methods used in these cyber operations have become increasingly sophisticated and potentially more dangerous.[477]

---

[470] *Cyber Threat Bulletin*, 2-3.
[471] *ibid*., 3.
[472] *ibid*., 4; AnonymousTV @YourAnonTV (Twitter, 2022) <https://x.com/YourAnonTV/status/1504556362960879616?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1504556362960879616%7Ctwgr%5E0ba51ef91cea8b071e8a696bb45273b7e2c244ff%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.france24.com%2Fen%2Feurope%2F20220323-ukraine-conflict-presents-a-minefield-for-anonymous-and-hacktivists>
[473] AnonymousTV @YourAnonTV (Twitter, 2022) <https://x.com/YourAnonTV/status/1501942349550653443?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1501942349550653443%7Ctwgr%5Ec34908fd9784a9b5d45aadca8b13e1c6b6b31d0d%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.infosecurity-magazine.com%2Fnews%2Fanonymous-leaked-files-russian%2F>
[474] 'Anonymous "officially in cyber war" with pro-Russia Killnet hacker group' (*CyberDaily.au*, 2022) <https://www.cyberdaily.au/strategy/7861-anonymous-is-officially-in-cyber-war-pro-russian-killnet-hacker-group> accessed 30 May 2024.
[475] *ibid*.
[476] KELA Cyber Intelligence Center, 'Russia-Ukraine war: pro-Russian hacktivist activity two years on' (*KELA*, 2024) <https://www.kelacyber.com/russia-ukraine-war-pro-russian-hacktivist-activity-two-years-on/> accessed 30 May 2024 [hereinafter: "KELA (2024)"].
[477] KELA (2024).

4.2.2. Anonymous: Organized Armed Group or Cyber-Allies?

In light of this framework, several questions arise in respect to the applicability of IHL to similar scenarios. In particular, when focusing on Anonymous involvement in the conflict between Russia and Ukraine, three main alternative scenarios can be identified under IHL. The diverse legal categorization under IHL is strictly connected to how cyber entities are perceived in accordance to the previously introduced general classifications. The three scenarios can be summarized into these three hypotheses:

1. Whether the attacks perpetrated are considered mere acts of hacktivism, the members of the collective conducing attacks against one of the countries involved in the conflict can be identified in the category of civilians taking part to the hostilities.[478] Three requirements must be fulfilled: threshold of harm, direct causation, and belligerent nexus.[479]

2. Whether the group is defined as cyber-terrorist organization and the attacks perpetrated between the cyber entity and the state achieve a certain level of violence for a perpetrated period of time, this can be transferred in IHL under the scenario of an organized armed group involved in a NIAC against the targeted state.[480]

3. Whether the group's actions are recognized as acts of cyber-support, the organization can be identified as co-party of the supported state in the IAC intercurrent between such state and the targeted country, according to a new systematic interpretation of the existing legal framework.[481] Starting from the concept of irregular armed forces, these entities can be recognized as cyber-organized resistance groups.[482] Despite not fulfilling all the requirements to be considered irregular armed forces, due to the inherent characteristics of cyberspace and cyber entities, according to this reexamination of the legal framework, the group can be defined as co-party of the state is supporting, whether it can be

[478] APII, art. 13(3).
[479] Nils Melzer (ICRC 2009).
[480] GCs, art. 3.
[481] GCs, art. 2.
[482] API, art. 4.

demonstrated a direct connection to the hostilities and a relation of cooperation or coordination between the co-parties.

Considering the characteristics of Anonymous, its peculiar relations with the states involved and the cyber-attacks conducted against Russia, in the conflict between the latter and Ukraine – which also represent most of cyber entities' political involvement in the conflicts of today – the study will proceed in investigating only the last two scenarios.

CHAPTER V

5. CYBER-TERRORISM IN ARMED CONFLICTS: CYBER-ORGANIZED ARMED GROUP AS A PARTY TO A NIAC

Having established the necessary premises, to investigate the legal status of the cyber-actors presented the research will proceed by analyzing the first possible scenario between the three presented. As mentioned above, when transferring the categorization of such cyber entities as cyber-terrorist groups into IHL framework, this implies the possible escalation of the cyber hostilities intercurrent between the cyber entity and the targeted state into a proper NIAC.[483] Accordingly, it has been previously highlighted that cyber-terrorist groups commonly target a specific country to coerce its government and population though fear and physical violence, in order to diminish the authority and sovereignty of the state. Such hostile and structured acts are often able to trigger the reaction of the targeted state against the terrorist organization; whether the cyber hostilities occurring between the two parties reach a certain level in both consistency and violence, they have the potential to easily escalate into a proper conflict. Therefore, the study will now examine the possibility of establishing a NIAC between governmental cyber-forces and a cyber non-state actor.

In accordance with the rules established under Common Article 3 GCs and customary law in respect to kinetic confrontations, a conflict of "non-international character" can be described as the situation of protracted armed confrontation occurring between governmental forces and non-state armed group or between two or more non-state armed groups against each other.[484] Two are the main requirements, which must be cumulatively met: a certain level of organization of the parties involved and a minimum level of intensity of the hostilities.[485] In the

---

[483] GCs, art. 3.
[484] GCs, art. 3; ICRC Commentary GCIII; ICTY, *Tadić* Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction (1995) [hereinafter: '*Tadić Decision'*], para. 70.
[485] ICRC, *How is the Term 'Armed Conflict' Defined in International Humanitarian Law?* (Opinion Paper 2008), 5; ICTY, *Tadić Decision*, para. 70; ICTY, *Tadić Judgement*, 562.

absence of specific regulations, there appears to be a consensus within the international community that the same rules and standards should govern the classification of cyber-conflicts as NIACs.[486]

Before proceeding, it is important to note that this research will not analyze the geographical scope of NIACs involving cyber-operations and the broad discussion related to the attribution's issue. Accordingly, these two issues will not be investigated since they are strictly dependent on the establishment of the requirement of intensity of hostilities.[487] With regards to the geographical scope, the study will assume that cyber-hostilities fall within the scope of the Geneva Conventions, when such attacks target objects that are in the territory or cyberspace of a state party to the Geneva Conventions, despite the cyber-attacks originating outside the targeted state's territory.[488] The unique nature of cyberspace and cyber-operations, combined with the technical challenges governments face in preventing the launch of cyber-attacks from their territories, leads to a necessary re-interpretation of the relevant norms on the basis of their context of application.[489] Consequently, the mere transmission of data by armed group members located in a state not party to the conflict does not imply that these states should be considered parties to an IAC involving the state targeted by the cyber-attacks.[490] In addition, considering the limited scope of this research, the attribution's issue will not be analyzed.[491] Particularly, for the investigation of the first scenario, the study will assume that the acts of Anonymous are not attributable to any specific country and therefore it shall be regarded as an independent non-state actor.[492] On the other hand, the study will assume that the control conducted by Russia over some of the above-mentioned pro-Russia cyber-groups could potentially reach the level of control required and be considered as acting on behalf of Russia.[493] Nevertheless,

---

[486] TM2.0, Rule 83.
[487] *Prosecutor v. Haradinaj et al*. (*Trial Judgment*), IT-04-84-T, ICTY, 3 April 2008, para 49.
[488] GCIII, art. 3; TM2.0, Rule 83.
[489] Stéphane Duguin (2023).
[490] TM2.0, Rule 83, paras 3-4.
[491] ICRC Commentary GCIII.
[492] *ibid*., 440-444.
[493] ICRC Commentary GCIII, 440-444.; *Cyber Threat Bulletin;* Microsoft Digital Security Unit, *An Overview of Russia's Cyberattack Activity in Ukraine* (Digital Security Unit, 27 April 2022) [hereinafter: "Microsoft Digital Security Unit (2022)"].

no clear information is available in this regard and therefore it is not possible to clearly establish an attribution link between the cyber-entities allegedly targeting Anonymous and Russia.[494] Some brief considerations on this matter will be presented in the second part of this chapter. In the same manner, the discussion regarding the attribution of the specific acts conducted by the singular members to the collective entities involved will not be addressed, as it will be considered presumed. Consequently, the research will focus solely on the investigation of the two main criteria to identify NIACs, namely organization and intensity of hostilities.[495]

5.1. THE PREREQUISITE OF ORGANIZATION [496]

As previously stated, to constitute a NIAC the involvement in the hostilities of at least one non-state organized armed group is indispensable.[497] Such a group is deemed 'armed' when it possesses the capability to carry out cyber-attacks.[498] While the group will be 'organized' when it operates under a structured command hierarchy and can execute prolonged military operations.[499] This research will not delve into the examination of whether cyber-groups could be considered armed, as it is already assumed that cyber-entities can have the capabilities to carry out cyberattacks, specifically in the case study at stake. Accordingly, the research will focus only on the required level of organization for cyber-armed groups.

Particularly, while state armed forces are presumed organized, it is always needed to demonstrate the existence of a certain level of organization with regards

---

[494] Microsoft Digital Security Unit (2022).
[495] 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 (CUP, 2016) (Commentaries on the 1949 Geneva Conventions) [hereinafter: "ICRC Commentary GCI"], 426.
[496] The content in Section III(a) partially reproduces a blogpost originally authored as an assignment for the Capita Selecta course on 'Armed Groups and International Law'. This course was undertaken as part of the LLM in Public International Law at Utrecht University, which was completed within the framework of the Double Degree program with LUISS University.
[497] ICRC, Opinion Paper (2008), 5; ICTY, *Tadić Decision*, 70; ICTY, *Tadić Judgement*, 562.; ICRC Commentary GCIII.
[498] TM2.0, Rule 83, para 11.
[499] *ibid*.; *Prosecutor v. Limaj et al.* (*Trial Judgment*), IT-03-66-T, ICTY, 30 November 2005, [hereinafter: "*Limaj Judgement*"], 129.

to non-state armed groups.[500] Some additional issues seem to arise when applying the traditional discipline to cyberspace, since the rules have been elaborated on the basis of a physical conception of the conflict and an outdated list of means and methods of warfare.[501] In this respect, it has always been considered necessary to demonstrate that armed groups possess a certain command structure in order to establish whether they have the capacity to physically sustain military operations and therefore engage in protracted armed violence.[502] Possessing such capacity has been described also as a first guarantee for the implementation of the basic IHL provisions.[503] Despite the huge differences between kinetic and cyber-conflicts, the scope of these rules seems to be applicable also in the 'battlespace', within the due considerations.[504]

5.1.1. The Indicative Factors

It is necessary to underline that also with respect to traditional warfare, the international legal framework does not provide a specific notion of organization. In the absence of a definition of "organized armed groups" in the relevant international documents, the International Criminal Tribunal for the Former Yugoslavia (ICTY) in the case *The Prosecutor v Ljube Boskoski and Johan Tarculovski* has elaborated five broad groups of indicative elements.[505] The ICTY's factors are: evidence of a command structure; ability to carry out coordinated operations; logistical capacities; ability to maintain a certain level of discipline and the ability to implement the basic obligations of international humanitarian law; ability of the group to speak with one voice.[506]

---

[500] *Limaj Judgement*, 94-129.
[501] Valentin Jeutner, 'The Digital Geneva Convention' (2019) 10 *JIHLS*, 161-164; Michael N. Schmitt, 'Classification of Cyber Conflict' (2012) 17(2) Journal of Conflict and Security Law 245 [hereinafter: "Michael N. Schmitt (2012)"], 255-260.
[502] ICRC, Opinion Paper (2008), 3.
[503] Cordula Droege, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians' (2012) 94 *International Review of the Red Cross* 533 [hereinafter: "Cordula Droege (2012)"], 550; ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts (2003), 19.
[504] TM2.0, Rule 83; Michael N. Schmitt (2012), 255-260.
[505] *Prosecutor v. Boskoski and Tarculovski (Trial Judgment)*, IT-04-82-T, ICTY, 10 July 2008 [hereinafter: "*Boskoski Judgement*"], 199-203.
[506] Boskoski Judgement, 199-203; Russell Buchan (2016), 747-748.

Subsequently, the International Criminal Court (ICC) Trial Chamber in the case *The Prosecutor v. Jean-Pierre Bemba Gombo* designed a non-exhaustive list of elements useful to assess the criteria.[507] These elements are: the strength of the internal hierarchy; the presence of a command structure and internal regulations; the military equipment available; the ability of the group to plan and carry on military operations; the intensity and seriousness of the military involvement.[508] In this regard, the Pre-Trial Chamber of the same Court generally affirmed that the group must be under responsible command, and therefore possessing the level of organization necessary to enforce discipline and effectively plan and execute military action.[509]

In this respect, the following practical features have been identified as suggestive of a group that is organized: the existence of headquarters; wearing uniforms; the assignment of tasks to individuals within the group; the ability to procure, transport and distribute arms; recruiting new members; affording training to members of the group and taking disciplinary action against them.[510] Nevertheless, it is important to stress that armed groups shall not achieve the same level of organization possessed by state armed forces.[511] In addition, it is crucial to emphasize that all these factors serve as guidelines and, therefore, the group is not required to meet all conditions rigidly in order to be deemed organized. Accordingly, none of these factors is alone able to determine the outcome of the evaluation regarding organization.[512] Contrarily, the evaluation must be done on the basis of a flexible approach. The determination of the degree of organization – specifically in cyberspace – necessitates a case-by-case evaluation, which must be conducted based on the particular circumstances of the given context.[513]

---

[507] *The Prosecutor v. Jean-Pierre Bemba Gombo* (*Trial Judgement*), ICC-01/05-01/08-424, International Criminal Court (ICC), 21 March 2016 [hereinafter: "*Bemba Judgement*"], 134-136.
[508] *Bemba Judgement*, 134-136.
[509] *ibid*.
[510] *Limaj Judgement*, 100-101, 118, 113-117, 123; *Prosecutor v. Slobodan Milošević* (*Decision on Motion for Judgement of Acquittal*), IT-02-54-T, ICTY, 16 June 2004 [*Milošević Decision*], 23; Russell Buchan (2016), 747-748.
[511] *Prosecutor v. Naser Oric* (Trial Judgment), IT-03-68-T, ICTY, 30 June 2006, 254.
[512] *Limaj Judgement*, 94-129.
[513] TM2.0, Rule 83, 11.

5.1.2. Virtual Organization

When analyzing cyber-entities, it is usual to refer to the concept of a "virtual organization", since all activities relevant to the organizational criteria take place online.[514] Within this particular framework, the International Group of Experts has conveyed that the degree of organization to classify a cyber entity as armed group is not met when they "operate not cooperatively, but rather collectively […] without any coordination".[515] Accordingly, the mere fact that multiple hackers are targeting a certain object at the same time does not necessarily mean they are organized.[516] Consequently, when cyber-attacks are carried out simultaneously by different independent actors, the latter will not be considered to be part of an organized group.[517] On the other end, an online group with a certain leadership that coordinates its actions by, for example, assigning specific cyber targets, sharing attack tools, conducting cyber vulnerability assessments, and evaluating cyber damage to determine if further attacks are necessary, shall be considered organized, since the group operates in a cooperative manner.[518] It is relevant to underline that the majority of the International Group of Experts concurred that the absence of physical meetings among group members alone does not disqualify it from possessing the required level of organization.[519]

5.1.3. Anonymous Model: "Operating Cooperatively"

In order to ascertain whether cybergroups such can attain the level of organization, it is imperative to first comprehend the structure and composition of these entities. Accordingly, the research will now proceed by investigating the characteristics of Anonymous in order to determine whether cyber-actors with the same features can reach the threshold. Having a look to the Anonymous Manifesto,

---

[514] TM2.0, Rule 83, 13.
[515] *ibid*., 13-15.
[516] *ibid*.
[517] *ibid*.
[518] *ibid*.
[519] *ibid*., 13.

"Anonymous is not an organization [...] Anonymous has no leaders [...]".[520] Therefore, at first glance, Anonymous appears to function as a collective rather than a structured organization, allowing its members the freedom to join and leave at their discretion by logging in and logging off the discussion board.[521]

Nevertheless, as the Manifesto proclaims itself, "[a]ctions shape who and what we are", not words.[522] In this respect, over the years evidence emerged showing that members of the group have assumed a proactive role in identifying potential targets, assessing their cyber vulnerabilities, and subsequently disseminating this information to other individuals who are prepared to engage in cyber-attacks.[523] These leading members also offer substantial advice and direction to other members regarding the selection of cyber weapons for carrying out the attack and they usually play a crucial role in identifying and creating the necessary malware required to execute the attack.[524]

By taking into consideration the peculiarities and limits of cyberspace, the information available clearly show the existence of a certain degree of responsible command and, therefore, the presence of a command structure, the ability to carry out coordinated operations and a certain level of logistics.[525] Particularly, the lead-members of the cybergroup have shown their ability to give directions, disseminate internal regulations, assign tasks, authorize action, etc., such as traditional commanders would do.[526] Accordingly, Anonymous' intrusive intervention in Egypt, the numerous operations against Israel and the more recent attacks against Russia have demonstrated the capacity of the different operational units placed all over the world to coordinate their action, through an effective dissemination of orders and decisions.[527] In this regard, it must be noted that the diffusion of orders

---

[520] *Anonymous Manifesto.*
[521] Russell Buchan (2016), 748.
[522] *Anonymous Manifesto.*
[523] Russell Buchan (2016), 749; Parmy Olsen (2012); Chapter V, 5.1.
[524] *ibid.*; Stewart K Bertram, *The Tao of Open Source Intelligence* (IT Governance Publishing 2015) [hereinafter: "Stewart K. Bertram (2015)"] 17, 29-31.
[525] *Limaj Judgement*, 199-201; Stewart K. Bertram (2015), 17, 29-31.
[526] *Boskoski Judgement*, 199; Stewart K. Bertram (2015), 17, 29-31.
[527] Boskoski Judgement, 200; Ravi Somaiya, 'Hackers Shut Down Government Sites' (TheNewYorkTimes, 2011) <https://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html> accessed 10 May 2024; Gilbert (2014); Peter Ray Allison (2022).

is more efficiently pursued through the cyber-tools used by these entities, such as encrypted chat rooms, logistics which allow leading members to reach a huge number of cyber-fighters in a very short time.[528] An interesting perspective highlights the possibility to consider the main websites used by the group, e.g. *4chan*, as the headquarter of the group, a domain perceived as the equivalent of the physical location where group members meet to plan and prepare their attacks.[529]

Another indicative factor identified for the "usual" battlefield is the uniform requirement.[530] It must be noted that in order to claim responsibility for cyberattacks, the group usually displays the Guy Fawkes mask on the websites hacked.[531] The same symbol has been used by the group in every communication to the public as a sign of identification, including in the several videos posted on behalf of the cybergroup. Despite this, it must be emphasized that the main aim of the uniform requirement has been development under IHL in respect to the necessity to distinguish combatants and act in compliance with the principle of distinction.[532] Consequently, the traditional scope of the norm seems not able to be fulfilled at all in this context. Nonetheless, the fact that the cybergroup has selected a unique symbol within which it interfaces external communications clearly contributes to attest organization. In accordance with the aforementioned, it demonstrates a form of "membership", serving as a method to "attribute" the conduct to a collective entity rather than being haphazardly executed by individuals. In this respect, the famous videos and declarations released by lead members on behalf of Anonymous in order to claim responsibility over certain attacks or to declare cyberwar against certain states and actors definitely illustrate the ability of the group to "speak with one voice".[533] Relevant evidence of such ability can be found, for example, in the YouTube videos claiming responsibility for the cyber-attacks perpetrated against Israel in November 2012 and July 2014, the videos

---

[528] Stewart K. Bertram (2015), 17, 29-31.
[529] Russell Buchan (2016), 750.
[530] *Limaj Judgement*, 123.
[531] Anonymous Logo (2024).
[532] *Limaj Judgement*, 123; API, art. 48, 51, and 52; *ICRC Study on Customary International Humanitarian Law* (2005), Rules 1 and 7.
[533] *Boskoski Judgement*, 203.

transmitted by Anonymous on Russian medias after being hacked and the post on the social network "X" declaring war against Russia in February 2022.[534]

5.1.4. Flexible Organizational Model?

On the basis of this analysis, despite the decentralized structure typical of cyber-entities, it can be concluded that Anonymous presents a fluid and flexible organizational model. Contrary to the arguments put forth by some authors, the requirement of organization can be indeed met by cyber-entities, when the regulations governing traditional warfare are interpreted within their specific context of application, namely cyberspace.[535] It is essential to acknowledge that in cyberspace, it is impossible to definitively establish a hierarchical structure in which leaders exert material or strict control over members of cybergroups in comparison to traditional means and methods, particularly when the group asserts the absence of hierarchy or leadership. Accordingly, despite the members of online-organizations may never know each other real identity, it has been demonstrated that such groups have the ability to act in a coordinated manner against a common target, by taking orders from a virtual leadership, and therefore they can be highly organized.[536]

Given the rapid advancement of military technologies and the significant risks associated with non-state cyber groups potentially accessing state-controlled lethal technologies, it is imperative to adopt a flexible approach in order to prevent the emergence of ambiguous situations that fall outside legal frameworks, thereby mitigating the potential for exploitation, at least until a specialized set of rules

---

[534] Anonymous #OpIsrael (*Youtube*, 2012) <https://www.youtube.com/watch?v=q760tsz1Z7M>; Anonymous – Message to Israel and Palestine <https://www.youtube.com/watch?v=iyQA3zMg7ZQ&list=UUJ7eFTLJArvkgDBae1hbllw>; Russia-Ukraine Crisis: Anonymous Hacker Takes Down Russian Govt Sites, Unleashes Cyber War <https://www.youtube.com/watch?v=Rdns1BOgC-0>; Anonymous @YourAnonOne (Twitter, 2022)<https://x.com/YourAnonOne/status/1496965766435926039?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496965766435926039%7Ctwgr%5E3e305757b46d489edcdccf5e02acca56c5717b97%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia>.

[535] Russell Buchan (2016), 747-751; Angelo Stirone (2020), 124-129.

[536] Michael N. Schmitt (2012), 256.

governing cyberwarfare will be agreed at the international level.[537] Following this approach, it can be concluded that whether it has been demonstrated that cyber-groups operate cooperatively in conducting cyber-confrontations, such as Anonymous, they shall be regarded as organized armed groups under Common Article 3 GC.[538]

5.2. INTENSITY OF HOSTILITIES

Having proved that cyber-entities with a certain degree of virtual organization can amount to organized armed groups, it is needed to investigate whether the hostilities occurring between the group and the opposing state forces may reach the threshold of intensity required to trigger a NIAC.[539] The term "hostilities" refers to "the (collective) resort by the parties to the conflict to means and methods of injuring the enemy".[540] The requisite of minimum degree of intensity has been formulated in order to distinguish NIACs from mere internal disturbances or in general from "sporadic acts of violence and other acts of a similar nature".[541] The ICTY contributed to developing the threshold by affirming that a NIAC exists when there is "protracted armed violence" between governmental forces and an organized armed group.[542]

5.2.1. The Indicative Factors

In this respect, some indicative factors have been elaborated by the ICTY to assess the threshold, among which: the severity of the conflict, the extent of the attacks and their duration, the increase in government forces, mobilization and

[537] Michael N. Schmitt (2012), 260.
[538] GCIII, art. 3.
[539] ICRC Commentary GCIII, 141-347.
[540] ICRC Interpretive Guidance, 43.
[541] GCIII, art. 3; APII, art. 1(2).
[542] *Tadić Decision*, 70.

weapon distribution, and whether the United Nations Security Council has addressed the issue or passed any resolution.[543]

Additionally, the Trial Chambers have considered the number of civilians forced to flee conflict zones, the types of weapons employed, whether cities and roads have been blocked, the extent of destruction and casualties resulting from the conflicts, the presence of ceasefire orders or agreements, and efforts to enforce them.[544] In light of these criteria, hostilities must reach a certain degree of intensity in terms of both quality and quantity.

5.2.2. Cyber Protracted Armed Violence: Quantitative Perspective

From a quantitative point of view, armed violence must be "protracted" to trigger the existence of a NIAC.[545] Although this term has never been properly defined under IHL, it refers to the duration and frequency of the attacks.[546] While through a literal interpretation the term seems to refer to a situation of constant violence, it has been clarified that the hostilities are not required to be continuous in nature.[547]

In particular, with regard to cyber-attacks, the IGE concurred that multiple cyber-attacks taking place intermittently yet within a specified timeframe may still be classified as "protracted".[548] On the contrary, mere occasional cyber-attacks, even resulting in physical harm or damage, do not meet the criteria to be regarded as NIACs.[549] Similarly, cyber activities that provoke events like sporadic civil disorder or domestic terrorism are not considered as such.[550]

---

[543] *Limaj Judgment*, 135-167; *Prosecutor v. Mrksic et al. (Trial Judgment)*, IT-95-13/1-T, ICTY, 27 September 2007, 39-40, 407-408, 419-421; *Prosecutor v. Hadžihasanović and Kubura (Appeal Judgment)*, IT-01-47-A, ICTY, 22 April 2008, 22; *Milošević Decision*, 28-31.
[544] *Boškoski Judgment*, 177; *Haradinaj Judgment*, 49, 90-99; *Limaj Judgment*, 90, 135-170; *Bemba Judgement*, 137-141.
[545] *Tadić Decision*, 70.
[546] *ibid*.; TM2.0, Rule 83, 9-10.
[547] *Limaj Judgment*, 168, 171–173.
[548] TM2.0, Rule 83, 9.
[549] *ibid*., 9-10.
[550] *ibid*., 10.

5.2.3. Cyber Protracted Armed Violence: Qualitative Perspective

From a qualitative perspective, the attacks must achieve a certain degree of gravity in order to differentiated from internal disturbances. As discussed in the previous Chapter, it is now widely accepted that certain cyber-operations can be considered attacks under Articles 49(1), and thus can constitute armed violence, even in the absence of an ongoing parallel kinetic conflict.[551] Nonetheless, the nature of cyber hostilities differs significantly from traditional warfare and, therefore, huge difficulties arise in applying the traditional legal framework to modern cyber-conflicts.[552]

In particular, most of cyber-attacks registered in modern warfare consist in DDoS attacks aiming to compromise computes by disrupting and halting the services or other types of attacks aiming to halter strategical systems of the targeted actors in order to undermine the latter's military objects and plans.[553] As previously demonstrated, by interpreting Article 49(1) in conjunction with Article 52(2) of Additional Protocol I (API), the term "attack" shall be understood to include not only actions resulting in acts of violence but also any operation aimed at rendering military objectives ineffective to secure a decisive military advantage.[554] However, considering the high threshold elaborated to trigger kinetic NIACs, only attacks amounting to "acts of violence" in the sense of Article 49(1) API shall be taken into account.

Additionally, to meet the threshold attacks must not only escalate to the level of armed violence but also exhibit a certain level of intensity in their consequences. This threshold can only be evaluated by considering the factors mentioned above, all of which entail significant physical repercussions – and therefore are evidently outdated when applied to cyberwarfare.[555] Despite the evolution of State practice, activities such as network intrusions, the deletion or destruction – even on a large

---

[551] API, art. 49(1); TM2.0, Rule 92; *see above* Chapter IV.
[552] Joanna Jarose, 'Reconsidering the Definition of "Attack" and "Damage" in Cyber Operations during Armed Conflict: Emerging Subsequent State Practice' (2023) 44 *Adel L Rev* [hereinafter: "Joanna Jarose (2023)"], 317.
[553] Denys Svyrydenko (2022), 41-42.
[554] API, art. 49(1), 52(2); TM2.0, Rule 92; *see above* Chapter IV.
[555] Joanna Jarose (2023).

scale – of data, computer network exploitation, and data theft are not capable by themselves to establish the existence of a NIAC.[556] For instance, blocking certain Internet functions and services or defacing governmental or other official websites would not meet the criteria to trigger a NIAC.[557] Subsequently, in the absence of a specific set of rules, modern cyber-conflicts will rarely meet the threshold of protracted armed violence traditionally required to establish kinetic NIACs.

5.2.4. Anonymous V. Russia And Its Cyber-Supporters: Protracted Armed Violence?

Having established the relevant framework, it is essential to analyze the applicable law in relation to a specific factual scenario to determine whether the threshold of protracted armed violence can be met by contemporary cyber-confrontations. Accordingly, this research will examine whether the cyber-hostilities involving Anonymous, Russia, and its "cyber-allies" – occurring since the invasion of Ukraine – have reached the minimum level of intensity required.

Quantitative perspective

From a quantitative point of view, in light of the escalation of events presented previously, it can be argued that the cyber-confrontations occurring between Anonymous, Russia and the various pro-Russia cyber-organizations, specifically Killnet, have been conducted frequently within a definite period of time.[558] Accordingly, from February 2022 to May 2022, despite the cyber-attacks being not continuous in nature, hundreds of cyber-operations have been launched between the relevant actors involved.[559] As reported above, on the 24 February 2022 Anonymous has declared cyberwar on Russia by launching several intrusive and large-scale cyber-attacks and operations.[560] While Russian forces were attempting to restore the compromised systems, some pro-Russia cyber-groups began targeting

[556] TM2.0, Rule 83.
[557] *ibid*.
[558] Chapter IV, 4.2.1.
[559] CyberPeace Institute (2023).
[560] Peter Ray Allison (2022); Denys Svyrydenko (2022), 44.

hundreds Ukrainian assets, but also directly Anonymous.[561] In particular, a few days after the declaration of cyberwar, the pro-Russia cyber-organization Killnet claimed to have hacked Anonymous' "headquarter".[562] Denying any shut down, Anonymous replied by continuing attacking Russia's strategical websites, databases and infrastructure.[563] Following Anonymous' cyber-attack in March against Roskomnadzor, pro-Russia cyber entities became increasingly active.[564] In particular, Killnet intensified its operations by launching cyber-attacks against European institutions and several Member States.[565] In response, Anonymous announced on Twitter that it had taken Killnet's website offline.[566]

Based on this overview, it can be argued that the cyber-hostilities conducted during the definite period presented above were "protracted" in time.

Qualitative perspective

More challenges arise in regard to the qualitative point of view. To meet the threshold of intensity, the traditional interpretation of the law, as outlined by international courts and scholars, indicates that attacks must not only fit into the definition enshrined in Article 49(1) API, but also exhibit a certain level of severity.[567] With regards to the threshold imposed by Article 49(1) API, it must be taken into consideration that most of the cyber-attacks registered in modern conflicts do not consist in operations directly causing severe death and destruction of people and physical objects. Nevertheless, as presented above, operations targeting data can be considered "acts of violence" under IHL, even if the targets are non-physical entities, when they cause physical repercussions to the people and objects connected to the targeted data.[568]

---

[561] Microsoft Digital Security Unit (2022).
[562] 'Anonymous "officially in cyber war" with pro-Russia Killnet hacker group' (*CyberDaily.au*, 2022) <https://www.cyberdaily.au/strategy/7861-anonymous-is-officially-in-cyber-war-pro-russian-killnet-hacker-group> accessed 30 May 2024.
[563] *ibid*.
[564] Microsoft Digital Security Unit (2022).
[565] *ibid*.
[566] *ibid*.
[567] API, art. 49(1); *Boškoski Judgment*, 177; *Haradinaj Judgment*, 49, 90-99; *Limaj Judgment*, 90, 135-170.
[568] TM2.0, Rule 92.

When analyzing the cyber-confrontations conducted in the conflict object of this study, it is evident that no cyber-operation has directly caused death or direct harm of people. Nonetheless, it can be argued that different cyber-operations have reached the threshold to be considered attacks under Article 49(1), by provoking damage and destruction of civil and military objects.[569] Accordingly, it has been reported that the actors involved, specifically Anonymous, have repetitively conducted cyber-interferences in order to alter the functionality of the enemy's objects, by causing the need of replacement of physical components for the restoration of the object's functionality or by permanently altering the original functionality of the targeted objects.[570] In this respect, Anonymous not only has launched DDoS attacks in order to block services, deface governmental and other strategic websites or alter/delete data, such as the operation against the Central Bank of Russia, the dissemination of the personal information of 120,000 Russian military personnel, and the attack to the Kremlin's CCTV system and website.[571]

The group has also conducted sophisticated cyber-attacks causing more intense consequences, such as the targeting of Russia's critical infrastructure resulting in the shutdown of gas pipelines, the compromising of Russian state media organizations, and the attack on the Russian agency Roscosmos, which lead to the paralysis of the entity responsible for overseeing satellite operations in space.[572] Accordingly, the attacks on Russian critical infrastructure can clearly amount to damage or destruction since they caused the permanent diminishing of the functions the targeted infrastructures have been designed to, imposing the need of shutting down the gas pipelines. In relation to Russian media agencies, the cyber-attacks carried out by Anonymous in February 2022 and subsequently in March 2022 represent some of the most severe attacks launched by the group against an information system. Specifically, in order to restore the normal operation of Russian media outlets, it can be argued that physical components of the affected

---

[569] Chapter IV, 4.1.2.; API, art. 49(1); Stéphane Duguin (2023).
[570] TM2.0, Rule 92, 5-11; CyberPeace Institute, 'Cyber Dimensions of the Armed Conflict in Ukraine – Q1 2023' (2023) <https://reliefweb.int/report/ukraine/cyber-dimensions-armed-conflict-ukraine-q1-2023> accessed 10 May 2024 [hereinafter: "CyberPeace Institute (2023) II"].
[571] Dan Milmo (2022).
[572] Peter Ray Allison (2022); Denys Svyrydenko (2022), 44.

media transmission systems were replaced. In addition, to prevent further dissemination of messages, photos, and videos contrary to Russian propaganda, Russian agencies had to physically remove the malware used to remotely control the botnets' (infected devices) systems. Similarly, when examining the cyber-attack on Roscosmos, it can be asserted that in order to end the system's state of paralysis, technicians had to replace certain software components. Conversely, reports indicate that pro-Russian cyber organizations have engaged in even more invasive cyber-attacks on data, employing more destructive and intrusive malwares.[573] The nature of malware utilized by Russian cyber-actors consistently necessitates the replacement of physical components within the affected botnets to restore normal system functionality.[574] Should this not be feasible, many of these malware variants are capable of causing a permanent loss of the original functionality of the affected device.[575]

Despite the possibility to consider such attacks as armed violence, when applying the factors elaborated by the ICTY to assess the degree of severity of the hostilities occurring between Anonymous, Russia and pro-Russia cyber-organizations, the cyber-confrontations seems to still not reach the qualitative threshold.[576] It is evident that the abovementioned factors have been elaborated by the ICTY on the basis of kinetic warfare and therefore seem to impose a very high threshold of intensity which implies the presence of imminent physical consequences.[577] With regards to the specific attacks at stake, it must be noted that most of cyber-attacks conducted by Anonymous caused data leaks, by exposing sensitive information and therefore potentially undermining trust in Russian institutions and causing operational security concerns.[578] Furthermore, the attacks have also contributed in diminishing or altering the military capability of the country, causing economic damage in several critical field, with indirect harm to

---

[573] Microsoft Digital Security Unit (2022), 2-17.
[574] *ibid*.; *Cyber Threat Bulletin*, 2.
[575] *ibid*.
[576] *Limaj Judgment*, 135-170; *Mrksic Judgement* 39-40, 407-408, 419-421; *Hadžihasanović Appeal Judgment*, 22; *Milošević Decision*, 28-31; *Boškoski Judgment*, 177; *Haradinaj Judgment*, 49, 90-99.
[577] *ibid*.
[578] Dan Milmo (2022).

civilians, but also a multitude of "cyber-civilian-causalities".[579] Accordingly, it must be noted that most of cyber-operations have provoked the leaking, altering or damaging of data of civilian population, thus targeting civilian objects. However, although a degree of destruction and casualties stemming from conflicts may be evident in cyber confrontations such as the one under consideration, the conventional interpretation of the legal framework necessitates direct effects leading to physical harm to individuals or objects, rather than solely to data.[580]

In addition, it is important to highlight that one of the most important factors in assessing the threshold is the increase in governmental forces and weapon distribution.[581] When examining the conflict under study, while clear evidence demonstrates the involvement of Russian forces in the cyber-attacks against Ukrainian targets, a significant issue is the lack of sufficient information to establish the direct mobilization of Russian governmental forces directly against Anonymous. Reports suggest that pro-Russian cyber groups, such as Killnet and Conti, have threatened and executed cyber-attacks against entities supporting Ukraine, including Anonymous.[582] These actions generally align with Russia's overall cyber warfare tactics rather than being direct reprisals against Ukrainian supporters.[583] Particularly, several factors suggest that the cyber-organization Killnet has conducted cyber-operations at least tacitly supported or condoned by Russia, fitting into the broader context of Russia's cyber warfare strategy.[584]

In light of this, establishing a NIAC between Anonymous and Russia would thus depend on demonstrating that cyber-supporters of Russia, specifically the cyber-organization Killnet, are either controlled by Russia or form part of its cyber irregular armed forces.[585] However, the current lack of evidence prevents

---

[579] Dan Milmo (2022).
[580] *ibid*.
[581] *Limaj Judgment*, 146, 159, 164-165; *Milošević Decision*, 30-31; *Mrksic Judgement* 39-40, 407-408, 419-421.
[582] *Cyber Threat Bulletin*, 5; CyberPeace Institute (2023) II.
[583] *ibid*.
[584] Joe Tidy, 'Meet the hacker armies on Ukraine's cyber front line' (*BBC*, 2023) <https://www.bbc.com/news/technology-65250356> accessed 30 May 2024.
[585] *Case Concerning Application of the Convention on the Prevention and Punishment of the Crime of Genocide* (Bosnia-Herzegovina v. Yugoslavia), International Court of Justice (ICJ), 11 July 1996 [hereinafter: "*Genocide Judgment*"], 404; *Situation in the Democratic Republic of the Congo, in the*

determining the actual relationship between this cyber-entities and Russia. Given the stringent thresholds required, it is not possible to establish that Russian cyber-supporters have acted on behalf of Russia directly against Anonymous. Therefore, despite the intensity of the cyber-attacks at stake could be considered high considering the characteristics of cyberspace, the lack of specific rules leads to the application of an outdated interpretation of the legal framework which does not allow these kinds of cyber-confrontations to reach the threshold to establish a NIAC. Accordingly, while these factors have been delineated as indicative and, therefore, it is necessary to analyze the specific context of application to assess whether the threshold can be met, the lack of specific regulation and guidelines on the matter impedes the potential for a divergent outcome.

Consequently, although there is evidence indicating that certain cyber-operations carried out by Anonymous, Russia and their cyber-allies may meet the criteria for classification as 'attacks' under Article 49(1) API, potentially triggering the threshold for NIACs, the prevailing interpretation of the required standard mandates a significantly high degree of severity of the hostilities, typically achievable only through kinetic attacks.[586] Hence, the attainment of this level of intensity appears unattainable through the cyber-attacks witnessed in modern warfare scenarios.

Chapter Conclusive Remarks

Overall, the Chapter illustrates that cyber entities engaging in cyber-hostilities against state forces may be theoretically categorized as organized armed groups under Common Article 3 GCs.[587] Nevertheless, the unique characteristics of these emerging forms of warfare, combined with the absence of precise information and adequate regulation, other than a prevailing conservative interpretation of the law, does not permit the recognition under IHL of the legal status of the majority of

---

case of the Prosecutor v. Thomas Lubanga Dyilo, ICC-01/04-01/06, International Criminal Court (ICC), 14 March 2012 [hereinafter: "*Lubanga Judgment*"], 541; TM2.0, Rules 82, 87; GCIII, art. 4.
[586] API, art. 49(1); GCIII, art. 3.
[587] GCIII, art. 3; ICRC Commentary GCIII.

cyber entities involved in contemporary digital conflicts and the potential "cyber-NIACs" they might trigger.

One of the main hurdles lies in the nature of cyber entities themselves. Many of these groups operate anonymously and without the centralized command structures typically associated with armed groups in conventional conflicts. This lack of cohesion makes it challenging to attribute specific operations directly to a single group or to demonstrate the level of organization necessary for classification under IHL. Another major challenge is linked to the inherent characteristics of cyber operations. While it has been demonstrated that cyberattacks can have devastating consequences – such as disrupting essential infrastructure, paralyzing government functions, or causing widespread harm to civilian property and civilians – they rarely result in the physical destruction or long-term occupation of territory, that IHL traditionally associates with armed conflict. These distinctions make it difficult to establish the level of sustained and intense violence required to recognize a NIAC. Therefore, the absence of specific legal frameworks, tailored to the cyber domain, creates further obstacles. Even when cyber entities demonstrate levels of organization and intent comparable to those of traditional armed groups, the predominantly non-physical nature of their operations places them outside the clear boundaries of current IHL standards.

In conclusion, while certain cyber activities may share similarities with traditional activities carried out by terrorist organizations or the behavior of other organized armed groups, they do not yet satisfy the criteria needed for NIAC classification. Despite cyber entities conducting protracted and destructive politically motivated cyber-attacks against states, they cannot be considered as proper cyber-terrorist entities operating as organized resistance groups, since at the present day the required physical level of violence provided under IL, and specifically IHL framework, has never been reached. The legal framework of IHL, as it stands, struggles to accommodate the unique characteristics of cyber warfare, leaving these confrontations in a regulatory grey zone. This underscores the pressing need for the international community to develop clearer and more specific legal guidelines to address the realities of modern cyber hostilities.

CHAPTER VI

6. CYBER-SUPPORT IN ARMED CONFLICTS: CYBER-ORGANIZED GROUP AS CO-PARTY TO AN IAC

Having analyzed the first hypothesis, the research will proceed to explore the second sub-question, thus, focusing on how the category of cyber-supporters can be applied within IHL framework. This involves an investigation into whether cyber-entities engaging in cyber-attacks against a specific state in support of another state can be classified as cyber-organized resistance groups acting as co-parties in the ongoing IAC between the states.[588]

As previously stressed, the primary challenge in addressing modern cyber-conflicts lies in the divergence from traditional IHL frameworks. When analyzing the relationships between states and non-state actors acting against the same adversary in a conflict, IHL typically focuses on whether states are controlling or supporting non-state actors.[589] For instance, in traditional scenarios, when a state exercises an high level of control over an organized armed group fighting against another state, the group is considered to be acting on behalf of the controlling state.[590] Consequently, the state providing support is deemed a party to the IAC against the opposing state.[591] However, in the context of cyberwarfare, the situation is often reversed: cyber-organizations frequently intervene in support of one party engaged in an IAC, without being under their control.[592] This opposite scenario complicates the application of IHL, as it requires a re-examination of existing legal paradigms to account for the unique dynamics and actors involved in cyber-conflicts.

Given the urgent need to develop new legal frameworks and interpretations that address the specificities of cyber organizations' involvement in IACs, this study will

---

[588] GCIII, art. 4; Alexander Wentker (2024).
[589] *Genocide Judgment*, 404; *Lubanga Judgment*, 541; ICRC Commentary GCIII, 427-444.
[590] *ibid*.
[591] ICRC Commentary GCIII, 440-444.
[592] Anh V. Vu (2024).

propose a systematic reinterpretation of the relevant provisions and customary rules. Initially, the research will briefly explore the possibility of classifying these cyber-groups as irregular armed forces of the state they support, by investigating whether they can be regarded organized resistance groups according to Article 4 of the Third Geneva Convention (GCIII).[593] By highlighting the challenges cyber-forces face in meeting the conditions established for the traditional battlefield, the study will advocate in favor of the inclusion of the category of cyber-organized resistance group in the rare cases of non-state actors able to participate to an IAC, as cyber-supporters of such state.[594] Having established these actors can take part to IACs, the criteria for being recognized co-party in an armed conflict – namely direct connection to the hostilities and cooperation/coordination between co-parties – will be introduced and thoroughly examined, in order to assess whether these cyber-groups can be identified as co-party of a state in an ongoing IAC.[595]

6.1. CYBER-ORGANIZED RESISTANCE GROUPS: IRREGULAR ARMED FORCES OR CO-PARTIES?

In light of the increasing number of cyber-groups supporting states engaged in IACs, some scholars have investigated the possibility to include such entities into the category of irregular armed forces of a party to an IAC, under Article 4 GCIII.[596] Article 4(A) GCIII is formally designed to establish the conditions for identifying who qualifies as a prisoner of war (POW) under IHL.[597] However, it is widely accepted that this provision also sets the criteria for determining lawful combatancy during IACs.[598] In particular, Article 4(A)(1) specifies that members of a state's regular armed forces are considered combatants.[599] Furthermore, Article 4(A)(2)

---

[593] GCIII, art. 4; TM2.0, Rule 87.
[594] Alexander Wentker (2024), 6-7; UN Security Council, 'Report of the High-level Independent Panel on Peace Operations' (17 June 2015) UN Doc A/70/95 [122] <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2015_446.pdf > accessed 29 May 2024; API, art. 1, 96(3).
[595] Alexander Wentker (2024).
[596] GCIII, art. 4; Russell Buchan (2016), 746-757; Alessandro Stiano (2022), 982-1000.
[597] GCIII, art. 4(A).
[598] ICRC Commentary GCIII, 950; TM2.0, Rule 87, 1; for a definition of "combatants" see API, art. 43(2); see also ICRC, *Customary International Humanitarian Law* (ICRC 2005), Rule 3.
[599] GCIII, art. 4(A)(1).

extends this status to irregular armed forces that belong to a party to the conflict.[600] The underlying rationale for this provision is to grant the privileges associated with lawful combatancy to irregular forces, since these groups are not officially part of a state's armed forces but exhibit characteristics and engage in activities similar to those of regular military forces.[601] Specifically, Article 4(A)(2) defines the category of irregular armed forces as "[m]embers of other militias and members of other volunteer corps, including those of organized resistance movements belonging to a Party to the conflict and operating in or outside their own territory", which must fulfil a list of conditions.[602] The first two requirements that the norm establishes are a certain level of organization of the resistance group and its "belonging to a Party to the conflict".[603] In addition, the group must cumulatively meet four conditions: a responsible command, a fixed distinctive emblem recognizable at a distance, the carrying of arms openly, and conducting operations in accordance with the laws and customs of war.[604]

6.1.1. The Two Prerequisites: Organized Resistance And 'Belonging To'

With regards to organization, it has been previously demonstrated that cyber-groups, such as Anonymous, can achieve a certain level of virtual organization.[605] As a consequence, it can be claimed that cyber-organizations such as the ones involved in the Russia-Ukraine conflict, and specifically Anonymous, can fit into the category of organized resistance groups, as virtual volunteer corps fighting for the sovereignty and freedom of a country and its people.[606] Nevertheless, several issues arise in assessing the other requirements provided to be regarded irregular armed forces. In respect to the condition of "belonging to a party", it is debated whether cyber-entities acting in support of a state party to a conflict could be

[600] GCIII, art. 4(A)(2).
[601] ICRC, *Customary International Humanitarian Law* (ICRC 2005), Rule 4.
[602] GCIII, art. 4(A)(2).
[603] *ibid*.
[604] *ibid*.
[605] Chapter V, 5.1
[606] ICRC Commentary GCIII, 999-1000.

regarded as acting on behalf of such party.[607] The concept of "belonging to" has been elucidated by the International Committee of the Red Cross (ICRC), emphasizing that the crux of the matter lies in the fact that organized armed groups must engage in hostilities on behalf of and with the consent of the party to which they are affiliated.[608] Initially, the ICTY examined the issue by scrutinizing the level of control wielded by the party over the organized armed group and the explicit declarations of the involved actors. Nevertheless, this rationale has faced significant criticism as the Court appeared to conflate the principles of state responsibility with those of international humanitarian law.[609] Accordingly, over time, numerous scholars have underscored that a precise understanding of Article 4 – specifically considering the ICRC Commentary – necessitates setting a less stringent standard grounded in a pragmatic perspective.[610]

Firstly, it has been affirmed that the formal declaration of the relationship between the parties involved is not the sole determinant, as implicit acquiescence or conclusive conduct can serve as indicia of a *de facto* association between the state party and the entity.[611] Secondly, it has been clarified that in the assessment of whether an organized entity is affiliated with a party involved in a conflict, the criterion should not hinge on the extent of state control over said entity, but rather on the underlying motivations or intentions of the armed group and the response of the relevant state, namely whether the armed group is aligned with the state's interests and whether the state overtly or implicitly acknowledges the group's actions on its behalf.[612] Thus, the determination of a group's affiliation with a party necessitates a demonstration of "support" or "loyalty" to the state party by the group, followed by explicit or implicit acceptance of this allegiance by the state.[613] Given this interpretation, it can be argued that cyber-entities openly proclaiming

---

[607] TM2.0, Rule 87, 1-22.
[608] ICRC Commentary GCIII 1960.
[609] Russell Buchan (2016), 756.
[610] ICRC Commentary GCIII 1960, 57; Robert Kolb, *Ius in Bello: Le Droit International Des Conflits Armes; Précis* (Helbing & Lichtenhahn 2003) [hereinafter: "Robert Kolb (2003)"], 160; Katherine Del Mar, 'The Requirement of "Belonging" under International Humanitarian Law', 21 *European Journal of International Law* (2010) [hereinafter: "Katherine Del Mar (2010)"], 111; Russell Buchan (2016), 756.
[611] ICRC Commentary GCIII 1960, 57; Russell Buchan (2016), 756.
[612] Katherine Del Mar (2010), 21.
[613] Robert Kolb (2003), 160.

and showing their involvement in supporting a state in the cyber-conflict against another state are effectively affiliated with the supported state, assuming there exists evidence of at least implicit endorsement by the state.[614]

In this respect, it can be noted that Anonymous has explicitly and repetitively declared its support for Ukraine when conducting cyber-operations against Russia.[615] Anonymous' alignment with Ukrainian interests and cyber tactics becomes apparent solely through an examination of the types of attacks carried out by the group and their repercussions.[616] At the same time, Ukrainian governmental exponents have never publicly affirmed to not support the cyber-organization nor to not be associated with their attacks. Contrarily, two days after the declaration of cyberwar of Anonymous against Russia, the Minister of Ukraine has announced the creation of an IT Army, inviting every volunteer able to help in responding to Russian cyber-attacks and contra-attack Russian targets to join the cyber-confrontations.[617] In this manner, Ukraine has demonstrated its appreciation for the support provided by the cyber-group by actively soliciting further assistance, thereby indicating a tacit acceptance of their allegiance.

6.1.2. The Four Additional Criteria: Are They Applicable To Cyber-Hostilities?

While it could be possible to argue that the cyber-entities object of our study belongs to a party to the conflict, insurmountable challenges arises in the cumulative fulfilment of the other requirements.[618] With regards to responsible command, the analysis on virtual organization provided in the previous Chapter has shown that it could be potentially satisfied.[619] Nonetheless, it seems impossible for cyber-organizations to simultaneously comply with the other three conditions.[620] When analyzing the requirement of a "fixed distinctive emblem recognizable at a

---

[614] TM 2.0, Rule 87, para 7.
[615] Dan Milmo (2022).
[616] Peter Ray Allison (2022).
[617] Mikhailo Fedorov, 'We Are Creating an IT Army' (*Twitter*, 2022) <https://x.com/FedorovMykhailo/status/1497642156076511233> accessed 20 April 2024.
[618] GCIII, art. 4(A)(2) (a-d)
[619] *ibid*., (a); TM2.0, Rule 87, 10.
[620] GCIII, art. 4(A)(2) (b-d).

distance", it is clear that it has been elaborated on the basis of the physical battlefield context, where combatants must visually distinguish themselves from civilians to uphold the principle of distinction.[621] Accordingly, the underlying purpose of this obligation is to prevent combatants from being mistaken for civilians, thereby shielding the latter from attacks.[622] However, cyber operations effectively remove the physical appearance of the operator from the equation, rendering this requirement irrelevant in the virtual domain.[623] In addition, most cyber-entities, such as the actors object of our analysis, are characterized by the fact that they conduct cyber-attacks by covering their real Internet Protocol (IP) addresses, in order to not show their real identity or location.[624] Consequently, the scope of this norm, as delineated under customary law, presents different challenges when applying in the realm of cyberwarfare. Secondly, when referring to the requirement of "carrying arms openly", it is important to underline that this obligation aims to prevent combatants from treacherously concealing their weapons in a manner that risks conflating them with civilians.[625] However, cyber "weapons" like malwares are inherently covert, designed for stealth implantation rather than open carrying.[626] The requirement is reasonably construed to prohibit methods that entangle civilian infrastructure within hostile cyber operations, such as distributed denial-of-service (DDoS) attacks that leverage compromised civilian systems as "zombies".[627] While it has been argued that hypothetically cyber-organizations can fulfil this requirement, when focusing on the case at stake, it is clear that Anonymous' use of such tactics contravenes this provision.[628] Finally, to qualify as lawful combatants, the group's activities must adhere to IHL framework, particularly the rules governing targeting, which prohibit attacks on civilians and

---

[621] GCIII, art. 4(A)(2) (b); API, art. 48, 51(2), 52(2); Russell Buchan (2016), 751; TM2.0, Rule 87, 11-13.
[622] *ibid*.
[623] Sean Watts, 'Combatant Status and Computer Network Attack', 50 *Virginia Journal of International Law* (2010), 440 [hereinafter: "Sean Watts (2010)"], 440; Russell Buchan (2016), 752.
[624] *ibid*.
[625] GCIII, art. 4(A)(2)(c); Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (CUP, 2016) [hereinafter: "Yoram Dinstein (2016)"], 53; Russell Buchan (2016), 751-752; TM2.0, Rule 87.
[626] Russell Buchan (2016), 751-75; TM2.0, Rule 87, 14 and Rule 103, 1-5.
[627] *ibid*.
[628] Russell Buchan (2016), 751-752.

civilian objects.[629] Ensuring and assessing compliance with IHL in the context of cyber warfare is notably complex due to the typically anonymous and borderless nature of cyber-operations.[630] Focusing on the case study, while Anonymous' operations against Russian governmental websites resulted in non-kinetic harm such as defacement and data loss, it can be argued that they have been targeting civilian objects when affecting civilian devices through malwares – for instance during the attacks on Russian information systems – thereby violating the principle of distinction.[631]

6.1.3. A New Systematic Interpretation: Filling The Gap

Taking into consideration the structural differences between cyberwarfare and traditional means and methods of war, it seems quite impossible for cyber-organizations to fit into the traditional notion of irregular armed forces, even though a systematic and progressive interpretation. Nevertheless, it seems evident that these types of cyber-groups could, in the abstract, be considered volunteer corps having similar characteristics to regular armed forces of a party to a conflict.[632] In particular, when referring to the conflict at stake, it must be taken into consideration that Ukraine has instituted a proper IT Army and therefore it could be argued that Anonymous, despite not being officially part of the Ukrainian army, exhibits characteristics and engages in activities similar to the "cyber regular armed forces" of Ukraine, through a relationship of cooperation.[633] In light of the lack of specific regulation, an alternative approach is needed to address the legislative void and prevent potential ambiguities that could be exploited for misuse in future conflicts.[634] A novel and intriguing perspective involves initiating the analysis from the framework of organized resistance groups, as outlined in Article 4 GCIII, to

---

[629] GCIII, art. 4(A)(2)(d); TM2.0, Rule 87, 15.
[630] Kubo Mačák (2021), 411-423.
[631] API, art. 48, 51(2), 52(2); Buchan (2016), 751.
[632] ICRC, *Customary International Humanitarian Law* (ICRC 2005), Rule 4; Henckaerts(2005).
[633] Stefan Soesanto, 'The IT Army of Ukraine. Structure, Tasking, and Ecosystem' (2022) Cyberdefence Report [hereinafter: "Stefan Soesanto (2022)"], 4-5, 8-22.
[634] Kubo Mačák, 'Will the centre hold? Countering the erosion of the principle of distinction on the digital battlefield' (2023) International Review of the Red Cross 105(923) [hereinafter: "Kubo Mačák (2023)"], 965-991.

consequently contemplate the potential inclusion of this category within the exceptional scenarios of non-state actors engaging in IACs.[635] Consequently, from a combined reading of the criteria delineated for irregular armed forces and the principles governing co-belligerency, it could be posited that cyber organized resistance groups may assume the role of co-parties to the state they are backing in an ongoing IAC, contingent upon the satisfaction of two pivotal conditions: a demonstrable nexus of directness between the group's actions and the hostilities, and a certain level of collaboration or coordination between the co-parties.[636] This interpretation implies the fulfilment – to some extent – of the requirements elaborated in regard to irregular armed forces, but offers a more adaptable framework, better suited to the dynamics of modern warfare. Specifically, it is important to emphasize that a minimum level of organization remains essential to ensure that the group can effectively engage in and sustain hostilities.[637] Thus, organization must be established as a prerequisite before determining whether these groups can be identified as co-parties.[638] Additionally, the requirements of connection to the hostilities and coordination/cooperation are intended to demonstrate the direct impact of the cyber-entity's actions on the hostilities and a certain level of agreement between the parties fighting a common enemy.[639] Consequently, this ground-breaking interpretation of the traditional legal framework seems able to embody the underlying principles of the rules developed to discipline irregular armed forces, thereby accommodating a broader spectrum of cases of cyber-groups recognized as lawful combatants when they conduct cyber-attacks in support of a state in an ongoing IAC.[640] Unlike the traditional discipline elaborated for irregular armed forces in respect of Article 4 GCIII, this approach puts emphasis on functional capabilities and organizational coherence rather than

---

[635] GCIII, art. 4(A)(2); Alexander Wentker (2024), 6-7; Anthea Roberts, Sandesh Sivakumaran, 'Lawmaking by Nonstate Actors: Engaging Armed Groups in the Creation of International Humanitarian Law' (2012) 37 *Yale J Int'l L* 107 [hereinafter: "Anthea Roberts (2012)"], 108-115.
636 Russell Buchan (2016), 746-757; Alexander Wentker (2024), 4-24; Morris Greenspan, The Modern Law of Land Warfare, (University of California Press 1959) [hereinafter: "Morris Greenspan (1959)"], 531.
[637] ICRC, Opinion Paper (2008), 3.
[638] Alexander Wentker (2024), 17.
[639] *ibid.*; 17-22.
[640] GCIII, art. 4; TM2.0, Rule 87.

physical markers and conventional combat methods.[641] The evolving nature of warfare necessitates a re-evaluation of existing legal frameworks to adequately address the role of cyber-organized groups in IACs.[642] Therefore, a more adaptable approach, recognizing organized resistance groups based on organizational and operational criteria, offers a viable solution. This approach aligns better with the characteristics of modern warfare and ensures that legal norms evolve to encompass the complexities of cyber conflict. The study will now delve into a more detailed analysis of the concept of co-party and the criteria elaborated for being considered a co-party in an ongoing armed conflict (direct connection to the hostilities and coordination/cooperation), to subsequently investigate whether this approach can be applied to Anonymous and its involvement in the Russia-Ukraine conflict.[643]

6.2. CYBER-SUPPORTERS AS CO-PARTIES TO A CONFLICT: A NEW "EXCEPTION" TO STATEHOOD EXCLUSIVITY IN IACS

To clarify, the term "co-party" denotes being a party in an armed conflict - whether international or non-international - alongside other participants on the same side.[644] It does not constitute a distinct status separate from that of party to an armed conflict.[645] All legal consequences associated with party status are equally applicable to co-parties.[646] The term co-party has been chosen for the purposes of this study in order to underline the shift from the era of "co-belligerency", relating to original idea that only states could be party of IACs and therefore fight on the same side, to the era of "co-participation", notion able to include also the increasing complex relationships of support and coordination occurring between states, international organizations and non-state actors registered in modern conflicts.[647] Traditionally, only states could be considered party to an IAC under IHL.[648] However, over years conflicts have seen a huge rise in the involvement of different

[641] GCIII, art. 4; TM2.0, Rule 87.
[642] François Delerue (2019), 313-314
[643] Alexander Wentker (2024), 4-24.
[644] *ibid*., 8
[645] *ibid*.
[646] *ibid*.
[647] *ibid*., 9; Morris Greenspan (1959), 531.
[648] *ibid*.

non-state actors and organizations.[649] Consequently, exceptions have emerged over time, allowing for the inclusion of entities other than states in IACs, such as international organizations and national liberation movements engaged in self-determination conflicts.[650] In the current landscape, also considering the unstoppable evolution of technology and the continuous development of cyber lethal systems, the growing urgency in accommodating contemporary realities leads to the need of broadening these exceptions.[651] Through a systematic analysis of the law, it can be argued that cyber-groups amounting to organized resistance groups, may become co-party in a conflict, even if the conflict has an international dimension, provided that the specific threshold for the establishment of the armed conflict has been previously met.[652] This interpretation seems effective in aligning IHL with the changing nature of modern warfare, where non-state actors and cyber capabilities are assuming increasingly prominent roles.[653] By recognizing the potential for these groups to engage in IACs, the legal framework can better capture and regulate the dynamics of modern conflict.[654] As outlined earlier, having acknowledged the potential for cyber organized actors to participate in IACs, it is imperative to consequently delve deeper into whether, within the particular context under examination, these actors may be deemed as co-parties.[655] To ascertain this, two conditions must be satisfied: a direct link to the hostilities and a level of cooperation or coordination.[656]

Before analyzing these two main requirements, it is necessary to address some preliminary considerations. Prior to determining the fulfillment of the above-mentioned conditions, it is essential to ensure that the party-related criteria are met. Additionally, it is crucial to establish the attribution of individual members' actions to the collective entity. Concerning the first aspect, it has been clarified that the

---

[649] Alexander Wentker (2024), 9; Morris Greenspan (1959), 531.
[650] Alexander Wentker (2024), 6-9; UN Security Council Report (2015); API, art. 1, 96(3).
[651] Gia Fernicola, 'Once Upon a Time in Cyberspace: A Grim Reality about the Dangers of Cyberwarfare' (2020) 20(2) International and Comparative Law Review 77, DOI: 10.2478/iclr-2020-0004 [hereinafter: "Gia Fernicola (2020)"], 94.
[652] Alexander Wentker (2024), 6-9, 17.
[653] François Delerue (2019), 295-298; Gia Fernicola (2020), 94.
[654] *ibid*.
[655] Alexander Wentker (2024), 4-24.
[656] *ibid*., 18-22.

party-related criteria regard the nature and structure of the entities involved, as well as the requisite level of hostilities. Consequently, in respect of the object of our study, party-related criteria consist in demonstrating the organization of the cyber resistance group and the recourse to armed force between states, thereby triggering the existence of an IAC. Upon examination of the case study, it is evident that both prerequisites have been satisfied. As previously demonstrated, Anonymous can be regarded as an organized armed group [*see above*, Chapter V] At the same time, the existence of an IAC occurring between Russia and Ukraine has been undisputable established since the invasion of Ukraine.[657] With regard to the second aspect, this study will presume that the requirement of attribution has been fulfilled.

6.2.1. Connection To The Hostilities

The first condition to become co-party of an armed conflict has been identified in the connection between the actions of the presumed co-party and the hostilities.[658] As introduced at the beginning, the term "hostilities" has a broader scope of application compared to the "attacks" recognized under Article 49 API.[659] Hostilities generally denote the techniques and tactics used to inflict damage on the adversary.[660] Accordingly, it is evident that investigating how hostilities are conducted by the actors involved is indispensable to identify which is the nature of the conflict and which are the relationships between the parties.[661] In particular, the connection to the hostilities must be "direct" to fulfil the threshold.[662] In evaluating the presence of a sufficiently direct association with hostilities, a variety of factors may be taken into account, although they are not conclusive in establishing co-party status.[663] These factors encompass the nature and extent of the actions undertaken,

---

[657] E. S. Puspoayu, H. Widodo, I. Ronaboyd, I. Lovisonny, 'Legal Classification on the Armed Conflict Between Ukraine and Russia in Light of International Humanitarian Law' in SHS Web of Conferences (149 EDP Sciences, 2022) 03020, 4.
[658] Alexander Wentker (2024), 18-19.
[659] *ibid*.; Yoram Dinstein (2016), 2; API, art. 44(3).
[660] ICRC Interpretive Guidance, 43.
[661] *ibid*.
[662] Alexander Wentker (2024), 18-19; Tristan Ferraro (2013), 585.
[663] Alexander Wentker (2024), 19.

as well as their spatial and temporal proximity to the harm inflicted upon the opposing party.[664]

With regards to the factual scenario object of the study, it is necessary first to clarify that the hostilities occurring between Russia and Ukraine have been formally recognized as IAC in concomitance with the declaration of invasion of Russia.[665] Accordingly, the research will investigate the connection of the Anonymous groups' acts to the hostilities conducted between Russia and Ukraine since the 24th of February 2024. Moreover, it is important to highlight that the term 'hostilities' encompasses both kinetic and cyber confrontations.[666] Notably, while various cyber-attacks occurred between the parties prior to the invasion, the onset of the invasion has clearly marked the beginning of a significant and chaotic cyberwar between Russia, Ukraine, and their respective cyber-supporters.[667] Therefore, when examining the nexus to hostilities, it is pertinent to also consider the cyber-operations conducted between these states.

Focusing on the activities of Anonymous, the group has consistently demonstrated a direct connection to the hostilities since the initial days of the conflict.[668] This connection is firstly evidenced by the multitude of cyber-attacks the organization launched against Russian governmental websites, databases, and strategic infrastructures from the day Russia formally invaded Ukraine.[669] These attacks aimed to weaken Russia's military and political power in favor of Ukraine.[670] Notably, within hours of Russia's invasion announcement, Anonymous initiated cyber-attacks to gather information on Russian military strategies and troop locations, subsequently releasing this information online, including details about troops' frequency.[671] These actions significantly aided Ukraine in

---

[664] Michael N. Schmitt, 'Ukraine Symposium – Are We at War?' (*Articles of War*, 2022) <https://lieber.westpoint.edu/are-we-at-war>; Kleffner(2019), 161, 177.
[665] Puspoayu, Elisabeth, Widodo, Hananto, Ronaboyd, Irfa, Lovisonnya, Intan, and Amiq, 'Legal Classification on the Armed Conflict Between Ukraine and Russia in Light of International Humanitarian Law' (2022) 149 *SHS Web of Conferences* 03020 <https://doi.org/10.1051/shsconf/202214903020>, 4.
[666] TM2.0, Rule 82, 11; ICRC Commentary GCI, 255.
[667] Anh V. Vu (2024), 1596.
[668] CyberPeace Institute (2023) II.
[669] Dan Milmo (2022); Peter Ray Allison (2022).
[670] *ibid*.
[671] Denys Svyrydenko (2022), 44.

formulating its military strategy and facilitating the evacuation of civilians from certain areas. With regards to the cyber battlespace, as previously discussed, the period following the invasion saw the launch of hundreds of cyber-operations and attacks targeting critical military, political, and economic institutions and infrastructures in both Russia and Ukraine.[672]

It is important to note that Russia has long been acknowledged as one of the foremost cyber-powers globally.[673] Prior to the invasion, Russian forces and their cyber allies had already been conducting significant cyber-operations against Ukraine. However, the dynamics of the cyber-conflict shifted markedly with the entry of Anonymous on behalf of Ukraine.[674] The involvement of Anonymous provided Ukraine with a distinct advantage in cyber-confrontations or, at the very least, elevated the level of cyberwarfare sophistication. Between February 2022 and May 2022, Anonymous consistently executed cyber-operations that supported Ukraine's military and cyber strategy, thereby directly contributing to the disruption and harm of the adversary [*see above,* Chapter V]. Although direct evidence is scarce, it has been asserted that Anonymous cooperated closely with Ukraine's IT Army, conducting joint cyber-attacks.[675] This assumption is reinforced by the Ukrainian Minister's call for experts to join the IT Army, which resulted in the rapid enlistment of over 400,000 cyber-fighters.[676] Among these recruits, several have reported collaborating with members of Anonymous.[677] On the basis of this analysis, it can be argued that the requirement of direct connection to the hostilities has been satisfied by Anonymous.

---

[672] *Cyber Threat Bulletin*, 2-5.
[673] Peter Ray Allison (2022).
[674] *ibid*.
[675] Joe Tidy, 'Meet the hacker armies on Ukraine's cyber front line' (*BBC*, 2023) <https://www.bbc.com/news/technology-65250356> accessed 30 May 2024 [hereinafter: "Joe Tidy (2023)"].
[676] Sam Schechner, 'Ukraine's "IT Army" Has Hundreds of Thousands of Hackers, Kyiv Says' (*The Wall Street Journal*, 2022) <https://www.wsj.com/livecoverage/russia -ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-of-hackers-kyiv-says-RfpGa5zmLtavrot27OWX> accessed 30 May 2024 [hereinafter: "Sam Schechner (2022)"].
[677] Joe Tidy (2023).

6.2.2. Cooperation/Coordination

The second criteria focus on the relationship between the co-parties.[678] In order to establish that a collective entity and a state are co-parties in an armed conflict, there must be a level of cooperation or coordination among them against a shared adversary during specific hostilities, allowing their actions to synergize within a single armed conflict.[679] The precise extent of cooperation or coordination required cannot be definitively outlined in a general sense.[680] Factors such as the proximity in time and space of one's activities to those of their partners, as well as the presence of structured mechanisms for coordinating activities, can be utilized to evaluate the level of cooperation in practice.[681] The determination of whether a state or collective entity is a co-party in an armed conflict is not contingent on their desire to hold such a status.[682] It is crucial to note that states or potential co-parties are not obligated to actively seek co-party status or the associated legal implications.[683] The fundamental objective of the current international legal framework governing armed conflict is for these regulations to apply when the circumstances on the ground necessitate it.[684] Therefore, the identification of parties must be grounded in an objective assessment of pertinent facts.[685] Nevertheless, engaging in cooperation or coordination concerning specific hostilities presupposes that the state or armed group possesses an understanding of the factual context in which their activities are situated, indicating a level of awareness regarding their partners' actions.[686] Substantially, the required knowledge typically relies on the surrounding circumstances of the potential co-party's actions, unless explicitly stated in official documents.[687] In the realm of cyber support, similar conclusions can be achieved.[688]

---

[678] Alexander Wentker (2024), 19.
[679] Alexander Wentker (2024), 19-22.
[680] *ibid*., 19-20.
[681] *ibid*.
[682] *ibid*.
[683] *ibid*.
[684] *ibid*., GCI, art. 2.
[685] Alexander Wentker (2024), 20; ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts (ICRC 2015), 8.
[686] *ibid*.
[687] *ibid*.
[688] *ibid*.

Simply bolstering the cyber capabilities of another entity would not automatically confer co-party status.[689] However, cyber operations can either be integrated into specific kinetic military actions of the recipient or independently constitute operations that impact the adversary, thereby becoming part of hostilities.[690] In the latter scenario, the classification of the entity conducting cyber operations as a co-party hinges on their cooperation or coordination with the recipient of such support.[691] Cyber operations conducted against a common adversary without collaboration would only constitute a distinct armed conflict, if the criteria for establishing an IAC or NIAC with that adversary are met.[692]

When analyzing the level of cooperation or coordination between Anonymous and Ukraine, different observations must be done. In respect to time and space, the actions carried out by the cyber-organization and Ukraine are characterized by strict proximity [*see above* Chapter V]. Firstly, it has been already highlighted that Anonymous has declared its cyberwar on Russia, by launching several cyber-attacks against Russian targets, as a response to Russia's invasion and therefore to the need of mobilization of Ukrainian forces.[693] In particular, the group not only conducted cyber-operations aiming to diminish the capabilities of Russia in favor of Ukraine, but also cyber-attacks that per se would be useless, but with a coordinated action within the military of Ukraine can be of indispensable importance. For instance, on the day of the beginning of the invasion, 24 February 2022, the cyber-organization has intercepted Russian military communications and has consequently given warning to Ukraine through their common mean of "public" communication – Twitter – of the time of the invasion and the city.[694] Anonymous specifically posted on Twitter: "The Russian armed forces are preparing a large-scale bombing operation in the capital of #Ukraine"[695] and "Russian authorities plan to invade Kiev within 96 hours. #Ukraine". On the 26th February 2022, Russian

---

[689] Alexander Wentker (2024), 22.
[690] *ibid*.; TM2.0, Rules 80-83.
[691] *ibid*.
[692] *ibid*.
[693] Dan Milmo (2022).
[694] *ibid*.
[695] Anonymous @YourAnonOne (Twitter, 2022) <https://x.com/YourAnonOne/status/1496981560406339600> accessed 20 May 2024.

military communications have been intercepted again.[696] This time, the frequency of some troops and some short recordings of the soldiers have been released online, in order to give information to Ukrainian military.[697] Moreover, when Anonymous brutally attacked Russian information systems, it did so in response of the parallel Russian kinetics attacks ongoing, in order to show the brutalities of Russian military actions and to create awareness between the population against the Russian propaganda, therefore stimulating political dissent and instability leading to loss of military power.[698] It must be observed that during the attacks on media, Anonymous has not used its own logo. On the contrary, the group has clearly demonstrated its cooperation with Ukraine by displaying symbols of Ukraine, such as the flag, and broadcasting the Ukrainian national anthem.[699] In this regard, the intention of Anonymous to cooperate with Ukraine in the fight against the brutal violation of human rights perpetrated by Russia is clear also from some other statements posted on Twitter. For example, the official account wrote: "We read your messages, thank you for supporting Ukraine. Let's be united!"[700] On the other side, Ukrainian governmental exponents have never publicly affirmed to not support the cyber-organization nor to not be associated with their attacks. Contrarily, two days after the declaration of cyberwar of Anonymous against Russia, the Minister of Ukraine announced the creation of an IT Army, by emphasizing the need of cooperation of cyber-organization and inviting every volunteer to join the cyber-army.[701] In this manner, Ukraine demonstrated its appreciation for the support provided by the cyber-group by actively soliciting further collaboration, thereby indicating a tacit acceptance of their allegiance. Accordingly, an interesting view can be to consider the creation of the IT Army as a way to coordinate the operations between Ukrainian official forces and cyber volunteer corps, including Anonymous.[702] As

---

[696] Denys Svyrydenko (2022), 44.
[697] *ibid*.
[698] *Cyber Threat Bulletin*, 2-5.
[699] Anonymous @YourAnonOne (*Twitter*, 2022) <https://x.com/YourAnonOne/status/1534628011592634373> accessed 20 May 2024.
[700] Anonymous @YourAnonOne (*Twitter*, 2022) <https://x.com/YourAnonOne/status/1496970367709360129> accessed 20 May 2024.
[701] Mikhailo Fedorov, 'We Are Creating an IT Army' (*Twitter*, 2022) <https://x.com/FedorovMykhailo/status/1497642156076511233> accessed 20 April 2024.
[702] Stefan Soesanto (2022).

noted above, some internal sources of the Army have argued that Anonymous has directly collaborated with the Ukrainian IT Army in the launch of different cyber-attacks against Russia, by clearly demonstrating a relationship of coordination or, at least, cooperation.[703] In light of this framework, considering the peculiarities of cyberspace and its actors, it can be established that the requirement of cooperation or coordination between Anonymous and Ukraine has been met.

Chapter Conclusive Remarks

The analysis provided in this Chapter has shown that, by employing a contextual and systematic approach to legal interpretation, the cyber entities object of our study may be considered cyber supporters acting as co-parties of a state already participating in an IAC. Upon identifying the cyber-entities object to this study as co-parties in an IAC, the research will finally provide a concise overview of the implications of assuming such a status. It is crucial to emphasize that the primary duty of upholding compliance with IL during armed conflicts lies with the involved parties.[704] Parties engaged in both international and non-international armed conflicts are obligated to adhere to various regulations under IHL, which cover rules governing the conduct of hostilities and the protection of individuals.[705] As previously mentioned, determining the legal status of conflict parties and the nature of the conflict necessitates the application of distinct sets of rules.[706] When referring to cyber-actors, the IGE has clarified under Rule 86 TM 2.0 that: "[t]he law of armed conflict does not bar any category of person from participating in cyber operations. However, the legal consequences of participation differ, based on the nature of the armed conflict and the category to which an individual belongs."[707]

Consequently, when it can be established that a cyber-entity is co-party of an IAC, such entity will be also bound by the set of rules applying to the parties of the conflict. Specifically, when the conflict is international in nature, the members of

---

[703] Stefan Soesanto (2022); Joe Tidy (2023).
[704] Alexander Wentker (2024), 27.
[705] *ibid*.
[706] *ibid.*
[707] TM2.0, Rule 86.

such entity will be granted the status of lawful combatants.[708] The attribution of combatant status within the framework of IHL holds significant legal implications.[709] Being recognized as a combatant entails specific rights and duties under IHL, including the duty of respecting the principles of distinction, proportionality and military necessity, the eligibility for prisoner of war (POW) designation and the immunity from prosecution for lawful acts of warfare.[710] The application of these traditional rules to cyber warfare poses distinct challenges, given that the nature of cyber-operations blurs the distinction between combatants and non-combatants and prevents the possibility to apply certain laws which seems suitable only in relation to kinetic conflicts.[711] Hence, the effectiveness of provisions like Article 4 GC III, which confers POW status, or Article 44 AP I, which mandates the differentiation of combatants from civilians, appears to be limited in the context of cyber-combatants.[712]

In contrast, it is evident that certain crucial rules remain applicable.[713] By designating individuals affiliated with cyber-organizations as lawful combatants, they become obligated to uphold the principle of distinction between civilian and military targets, including non-physical targets like data.[714] Furthermore, cyber-combatants will be granted immunity for cyber-attacks that, in peacetime, would constitute criminal offenses but can be deemed lawful under the laws governing armed conflicts.[715] When focusing on the principle of distinction, some authors have correctly criticized the consequences of the increasing trend of civilization of the digital battlefield.[716] While the increasing involvement of civilians in digital battlefield activities during armed conflicts poses grave risks and seems to undermine this principle, the scenario partially changes when dealing with proper

---

[708] TM2.0, Rule 86; GCIII, art. 4.
[709] *ibid*.
[710] GCIII, art. 4; API, art. 43(2), 48, 51, 52; ICRC, *Customary International Humanitarian Law* (ICRC 2005), Rule 1, Rule 14, Rule 22, Rule 98, Rule 158.
[711] Kubo Mačák (2023), 965-991; Jake B. Sher (2016), 239.
[712] GCIII, art. 4; API, art. 44; Ann Väljataga (2022), 2.
[713] Ann Väljataga (2022), 2; TM2.0, Rule 87;
[714] Tilman Rodenhäuser, Mauro Vignati, '8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them' (EJIL:Talk! 2023) <https://www.ejiltalk.org/8-rules-for-civilian-hackers-during-war-and-4-obligations-for-states-to-restrain-them/> accessed 28 April 2024.
[715] Ann Väljataga (2022), 2.
[716] Kubo Mačák (2023), 966.

cyber-organizations, such as the one under consideration.[717] In the latter, obtaining legal status and the subsequent responsibility to uphold fundamental principles of IHL, like distinction and proportionality, can lead to a more conscientious use of cyber warfare methods and may enable the prosecution of cyber-combatants who violate these regulations. While the urgent need to redefine the concept of combatant and its legal implications in cyber-hostilities, has been highlighted by different scholars, a temporary solution is essential. [718] In light of the existing lacuna in legislation and the associated ambiguous territory vulnerable to exploitation, the precise classification of contemporary cyber-actors as combatants stands out as the optimal strategy to uphold a foundational level of adherence to IHL amidst the complexities of modern warfare scenarios. Addressing the substantial threats posed by cyberwarfare necessitates urgent action to establish a framework of minimal safeguards by bridging the legislative void.[719]

[717] Kubo Mačák (2023), 966.
[718] Jake B. Sher (2016), 239; Cordula Droege (2012), 533-534.
[719] *ibid*.

CONCLUSION

7. SUMMARY OF THE FINDINGS

This thesis has explored the profound and growing influence of digital technologies and cyber actors on national and international security, shedding light on the legal challenges they pose. As demonstrated through the analysis, existing legal frameworks struggle to adapt to the rapid evolution of cyber operations, creating significant gaps in protection, accountability, and enforcement. Traditional international legal principles – particularly sovereignty and state responsibility – prove difficult to apply in cyberspace, where the involvement of non-state actors blurs the lines between state and private conduct. In this regard, the study has specifically focused on how the ambiguous relationships intercurrent between cyber actors and states exacerbates these legal uncertainties, particularly when cyber means are deployed to challenge governmental authority, disrupt civilian infrastructure, or escalate into full-scale cyberwarfare.

To better define the nature of cyber threats, the study has identified three broad categories: cybercrime, politically motivated cyber operations, and cyber warfare. Given the distinct nature and broad scope of cybercrime, this thesis has focused on the latter two, emphasizing the increasing involvement of non-state actors. Taking into consideration the first class of actions, the study has primarily highlighted that under general International Law the legal status of cyber non-state actors remains uncertain, as traditional classifications – such as the notions of cyber-terrorists and hacktivists – fail to fully capture their evolving role. Subsequently, the thesis has demonstrated that many contemporary cyber entities do not fit neatly into these pre-existing categories, as their actions often transcend ideological activism without fully amounting to terrorism. To address this conceptual gap, the thesis has introduced the category of cyber-support groups, a classification that better reflects the realities of modern cyber operations. The case of Anonymous was examined as a key example, particularly regarding its cyber activities targeting state entities in the name of human rights, democracy, and self-determination.

The case study of Anonymous serves as a crucial illustration of the evolving role of cyber non-state actors and of their impact to national and international stability. It highlights the fluidity of cyber operations, where ideological motivations, political activism, and state-aligned actions often intersect, blurring the traditional legal distinctions between hacktivism, cyberterrorism, and proper cyberwarfare. In particular, Anonymous' involvement in the Russia-Ukraine conflict demonstrates how cyber groups can exert significant influence on international security dynamics without formal state affiliation, raising critical questions about attribution, responsibility, and the applicability of International Humanitarian Law. This case properly underscores the inadequacy of existing legal categories in capturing the operational realities of modern cyber entities, emphasizing the necessity of the cyber-support classification introduced in this thesis, especially when cyber operations escalate in digital conflicts. By analyzing Anonymous' actions, the study also reveals a growing trend in which cyber actors' function as informal allies in state conflicts, potentially qualifying as co-belligerents under certain legal interpretations. This example is particularly useful in demonstrating how contemporary cyber engagements challenge the conventional frameworks of war and peace, underscoring the urgent need for legal adaptations that recognize the strategic and operational impact of cyber-support groups in modern conflicts.

Building upon this factual framework, the thesis has demonstrated that when ideologically motivated cyber-attacks escalate, they often evolve into cyberwarfare, underscoring the need for a more nuanced legal framework to govern such situations. Moving beyond general International Law, the study has examined cyberwarfare within the International Humanitarian Law's framework, where the legal classification of cyber non-state actors has direct implications for the characterization of conflicts and the applicable legal regimes. The research has identified two possible legal scenarios under International Humanitarian Law (the law applying to armed conflicts):

1. Entities which are typically recognized as cyber terrorist organizations could qualify as organized armed groups engaged in a non-international armed conflict against a state.

2. Entities which are commonly recognized as strong hacktivist groups could be identified as cyber-support organizations acting as co-belligerents in an international armed conflict between states.

To assess which scenario is more reflective of contemporary realities, the thesis has analyzed Anonymous' involvement in the Russia-Ukraine conflict. While ultimately concluding that the existence of a non-international armed conflict between cyber groups and states remains highly unlikely, the study has demonstrated a growing trend in which cyber entities align themselves with states, often acting as informal allies in inter-state conflicts. Although modern cyber groups do not fully meet the traditional criteria for irregular armed forces under International Humanitarian Law, this thesis argues that they exhibit key characteristics that could justify their recognition as co-belligerents when supporting a state engaged in an international armed conflict. This argument challenges the prevailing tendency – both in media and academic discourse – to categorize all cyber non-state actors as terrorist organizations. Instead, this thesis has shown that many functions as cyber-support groups, aligning their activities with state interests rather than pursuing independent extremist agendas.

By advocating for a clearer legal recognition of cyber-support groups under International Law and International Humanitarian Law, this study proposes an alternative interpretation of existing legal frameworks – one that better reflects the realities of modern security threats and warfare. Recognizing organized cyber groups as potential co-parties to an international armed conflict in exceptional circumstances would provide more legal clarity and offer a foundation for their regulation within armed conflicts. Such an approach could ensure that non-state cyber actors engaged in warfare are subject to the obligations and principles of International Humanitarian Law, rather than operating in a legal gray zone.

Ultimately, this thesis contributes to the broader academic debate on the legal status of cyber non-state actors and their impact on global security. It underscores the urgent need for an adaptable and cohesive legal framework capable of addressing evolving cyber threats while upholding the core principles of International Law and International Humanitarian Law. As cyber operations continue to shape modern warfare, it is imperative for the legal community to

develop forward-looking solutions that balance security concerns with fundamental legal protections, specifically ensuring that cyberwarfare does not remain an unregulated battlefield. Despite the foundational role of states in shaping International Law and global governance, in the realm of cybersecurity and cyberwarfare, states appear to deliberately avoid reaching a legal consensus. Rather than establishing clear regulations, they seem to exploit the legal uncertainty to maintain strategic flexibility, allowing them to leverage cyber capabilities without binding constraints. In this context, a formalized legal framework may remain elusive. However, as this thesis suggests, the international community must seek alternative pathways towards regulation, either through soft law instruments or by adopting creative, even unconventional, legal interpretations that better align with contemporary cyber realities. Without such efforts, cyberspace will continue to be a domain where law lags behind practice, leaving accountability gaps that benefit those willing to operate in the shadows of legal ambiguity.

BIBLIOGRAPHY

Case Law

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro) (Merits) [2007] ICJ Rep 43.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia-Herzegovina v. Yugoslavia), (Preliminary Objections) [1996] ICJ Rep 595.

Application of the International Convention on the Elimination of All Forms of Racial Discrimination (Georgia v Russia) (Preliminary Objections) [2011] ICJ Rep 70.

Corfu Channel Case (United Kingdom v Albania) (Merits) [1949] ICJ Rep 4.

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America) (Merits) [1986] ICJ Rep 14.

Oil Platforms (Islamic Republic of Iran v United States of America) (Separate Opinion of Judge Higgins) [2003] ICJ Rep 161.

Opuz v. Turkey App no 33401/02 (ECtHR, 9 June 2009).

Prosecutor v Tadić (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1-AR72 (2 October 1995).

Prosecutor v Tadić (Opinion and Judgment) ICTY-94-1-T (7 May 1997).

Prosecutor v Tadić (Judgment) ICTY-94-1-A (15 July 1999).

Prosecutor v Boškoski and Tarčulovski (Trial Judgment) IT-04-82-T (10 July 2008).

Prosecutor v Hadžihasanović and Kubura (Appeal Judgment) IT-01-47-A (22 April 2008).

Prosecutor v Haradinaj et al. (Trial Judgment) IT-04-84-T (3 April 2008)

Prosecutor v Limaj et al. (Trial Judgment) IT-03-66-T (30 November 2005)

Prosecutor v Mrkšić et al. (Trial Judgment) IT-95-13/1-T (27 September 2007)

Prosecutor v Orić (Trial Judgment) IT-03-68-T (30 June 2006)

Prosecutor v Milošević (Decision on Motion for Judgment of Acquittal) IT-02-54-T (16 June 2004)

Pulp Mills on the River Uruguay (Argentina v Uruguay) [2010] ICJ Rep 14.

The Prosecutor v. Jean-Pierre Bemba Gombo (Trial Judgement), ICC-01/05-01/08-424, International Criminal Court (ICC), 21 March 2016.

Legislation

African Union Convention on Cyber Security and Personal Data Protection [signed 27 June 2014] AU Doc EX.CL/846(XXV).

Agreement between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information

Security [signed 16 June 2009, entered into force 5 January 2012] ('Yekaterinburg Agreement').

Constitution of the International Telecommunication Union (concluded 22 December 1992, entered into force 1 July 1994) 1825 UNTS 143.

Council of Europe, Additional Protocol concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems [opened for signature 28 January 2003, entered into force 1 March 2006] ETS 189.

Council of Europe, Convention on Cybercrime (adopted 23 November 2001, entered into force 1 July 2004) ETS No 185.

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148.

European Parliament and Council, Directive 2013/40/EU on attacks against information systems, adopted 12 August 2013 [2013] OJ L 218/8.

European Union, Regulation (EU) 2025/38 of the European Parliament and of the Council of 19 December 2024 laying down measures to strengthen solidarity and capacities in the Union to detect, prepare for and respond to cyber threats and incidents and amending Regulation (EU) 2021/694 (Cyber Solidarity Act) [2025] OJ L 5/1.

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 the 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 31.

Geneva Convention relative to the Treatment of Prisoners of War (adopted 12 August 1949, entered into force 21 October 1950) 75 UNTS 135

Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 PE/86/2018/REV/1.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Adoption of an Additional Distinctive Emblem (Protocol III) (adopted 8 December 2005, entered into force 14 January 2007) 2404 UNTS 261.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 3 31.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (adopted 8 June 1977, entered into force 7 December 1978) 1125 UNTS 609.

International Convention for the Suppression of Terrorist Bombings (adopted 15 December 1997, entered into force 23 May 2001) 2149 UNTS 256.

International Convention for the Suppression of the Financing of Terrorism (adopted 9 December 1999, entered into force 10 April 2002) 2178 UNTS 229.

International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts (2001) [ARSIWA] UNGA Res 56/83 (12 December 2001), annex, UN Doc A/RES/56/83.

Italy, Codice di Procedura Penale (Italian Code of Criminal Procedure), Decreto del Presidente della Repubblica 22 settembre 1988, n. 447, revised 2024.

Italy, Codice Penale (Italian Penal Code), Regio Decreto 19 ottobre 1930, n. 1398, revised 2024.

United Nations, Charter of the United Nations, adopted 26 June 1945, entered into force 24 October 1945, 1 UNTS XVI.

United Nations, Draft United Nations Convention against Cybercrime, finalized by the Ad Hoc Committee on 9 August 2024, pending adoption by the General Assembly.

United Nations General Assembly Resolutions on Cybersecurity, UNGA Res 73/27 (5 December 2018) UN Doc A/RES/73/27, UNGA Res 74/28 (12 December 2019) UN Doc A/RES/74/28.

United *N*ations General Assembly*, Report of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security,* (2021) UN Doc A/76/135.

United Nations, Security Council Resolution, UNSC Res 1373 (28 September 2001) UN Doc S/RES/1373.

United Nations, Security Council Resolution, UNSC Res 1566 (8 October 2004) UN Doc S/RES/1566.

Vienna Convention on the Law of Treaties, opened for signature 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980).

Secondary Sources

Allison, Peter Ray, 'The cyber security impact of Operation Russia by Anonymous' (ComputerWeekly.com, 2022) <https://www.computerweekly.com/feature/The-cyber-security-impact-of-Operation-Russia-by-Anonymous> accessed 1 May 2024

Anonymous Logo (1000Logos, 2024) <https://1000logos.net/anonymous-logo/#:~:text=Meaning%20and%20history,symbol%20of%20anonymity%20and%20decentralization> accessed 10 May 2024.

Anonymous – Message to Israel and Palestine <https://www.youtube.com/watch?v=iyQA3zMg7ZQ&list=UUJ7eFTLJArvkgDBae1hbllw> accessed 10 May 2024.

Anonymous "officially in cyber war" with pro-Russia Killnet hacker group' (CyberDaily.au, 2022) <https://www.cyberdaily.au/strategy/7861-anonymous-is-officially-in-cyber-war-pro-russian-killnet-hacker-group> accessed 30 May 2024.

'Anonymous: 10 Things We Have Learned In 2013' (DarkReading, 2013) <https://www.darkreading.com/cyberattacks-data-breaches/operation-payback-feds-charge-13-on-anonymous-attacks> accessed 10 May 2024.

Anonymous @YourAnonOne (Twitter, 2022) <https://x.com/YourAnonOne/status/1496965766435926039?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496965766435926039%7Ctwgr%5E3e305757b46d489edcdccf5e02acca56c5717b97%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia> accessed 10 May 2024.

Anonymous @YourAnonOne, (Twitter, 2022) <https://x.com/YourAnonNews/status/1510494900713840641> and <https://x.com/YourAnonNews/status/1497574730282541060> accessed 10 May 2024.

Anonymous @YourAnonOne, (Twitter, 2022) <https://x.com/YourAnonOne/status/1496965766435926039?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1496965766435926039%7Ctwgr%5E2b2839cb70395f2111429a52331a3adc1f0ce352%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.theguardian.com%2Fworld%2F2022%2Ffeb%2F27%2Fanonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia> accessed 20 April 2024.

Anonymous #OpIsrael (Youtube, 2012) <https://www.youtube.com/watch?v=q760tsz1Z7M>.

AnonymousTV @YourAnonTV (Twitter, 2022) <https://x.com/YourAnonTV/status/1504556362960879616?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1504556362960879616%7Ctwgr%5E0ba51ef91cea8b071e8a696bb45273b7e2c244ff%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.france24.com%2Fen%2Feurope%2F20220323-ukraine-conflict-presents-a-minefield-for-anonymous-and-hacktivists> accessed 10 May 2024.

AnonymousTV @YourAnonTV (Twitter, 2022) <https://x.com/YourAnonTV/status/1501942349550653443?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1501942349550653443%7Ctwgr%5Ec34908fd9784a9b5d45aadca8b13e1c6b6b31d0d%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.infosecurity-magazine.com%2Fnews%2Fanonymous-leaked-files-russian%2F> accessed 10 May 2024

Afzal, Jamil, *Implementation of Digital Law as a Legal Tool in the Current Digital Era* (Springer 2024).

Australia, 'Australia's Cyber Security Strategy: Enabling Innovation, Growth & Prosperity' (Department of Home Affairs 2016) <https://cybersecuritystrategy.pmc.gov.au/assets/img/PMC-Cyber-Strategy.pdf>.

Baldi, Stefano, Gelbstein, Eduardo, and Kurbalija, Jovan, *Hacktivism, Cyber-Terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace* (*DiploFoundation* 2003) 23 https://books.google.it/books?id=oKS2RtaKDm8C accessed 14 January 2025.

Biggio, Giovanni, *Humanizing the Law of Cyber Targeting: Human Dignity, Cyber-Attacks and the Protection of the Civilian Population* (PhD thesis, University of Sheffield 2019).

'BRICS Leaders Xiamen Declaration' (2017 BRICS Summit, 5 September 2017) <https://www.bricschn.org/English/2017-09/05/c_136583711_2.htm> accessed 14 December 2024.

Buchan, Russell, 'Cyber Warfare and the Status of Anonymous under International Humanitarian Law' (2016) 15(4) *Chinese Journal of International Law*.

Bygrave, Lee A, *International Law and the Internet* (OUP 2016).

Cambridge Dictionary, 'Hacking' (CUP) accessed 13 January 2025 <https://dictionary.cambridge.org/dictionary/english/hacking>.

Cambridge Dictionary, 'Activism' (CUP) accessed 13 January 2025 <https://dictionary.cambridge.org/dictionary/english/activism>.

Canadian Centre for Cyber Security - An Introduction to the Cyber Threat Environment (Communications Security Establishment 2022).

Chałubińska-Jentkiewicz, Katarzyna, 'Cyberspace as an Area of Legal Regulation' In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) *Cybersecurity in Poland* (Springer, Cham 2022) <https://doi.org/10.1007/978-3-030-78551-2_2>.

CheckPoint Research Team, 'Fake News of Cyber Attacks Fast-Spreads, as Conflict between Russia and Ukraine Escalates' (CheckPoint 2022) <https://blog.checkpoint.com/security/hacktivism-in-the-russia-ukraine-war-questionable-claims-and-credits-war/> accessed 29 May 2024.

Cherney, Mike, 'U.S, allies issue rare warning on Chinese hacking group' (The Wall Street Journal 2024) <https://www.wsj.com/politics/national-security/u-s-allies-issue-rare-warning-on-chinese-hacking-group-9eebb0ce> accessed 28 September 2024.

Clark, David D, Landau, Susan, 'Untangling Attribution' (2011) 2 *Harvard National Security Journal*.

Coleman, G, Our Weirdness Is Free, <https://canopycanopycanopy.com/contents/our_weirdness_is_free> accessed 10 May 2024.

Collin, Barry, 'The Future of Cyberterrorism' (1997) *Crime and Justice International* <http://www.cjimagazine.com/archives/cji4c18.html> accessed 11 January 2025.

Conway, Maura, 'Terrorism and IT: Cyberterrorism and Terrorist Organisations Online' (Paper presented at the International Studies Association Annual International Convention, Portland, Oregon, 2003).

Couzigou, Irène, 'Securing cyber space: the obligation of States to prevent harmful international cyber operations' (2018) 32 *Int'l Rev Law Computers & Technology*.

Council of the European Union, *A Strategic Compass for a stronger EU security and defence in the next decade* (Press Release 2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/> accessed 1 May 2024.

Crowther, Alexander G., 'National Defense and the Cyber Domain' (2017) *The Heritage Foundation*.

'Cyber Attacks in Time of Conflict, Platform #Ukraine' (CyberPeace Institute 2023) <https://cyberconflicts.cyberpeaceinstitute.org/ > accessed 29 May 2024.

'Cyber Dimention of the Armed Conflict in Ukraine', (CyberPeace Institute 2023) <https://reliefweb.int/report/ukraine/cyber-dimensions-armed-conflict-ukraine-q1-2023> accessed on 10 May 2024.

Del Mar, Katherine, 'The Requirement of "Belonging" under International Humanitarian Law' (2010) 21 *European Journal of International Law*.

Delerue, François, *Cyber Operations and International Law* (CUP 2020).

Denagamage, PL, and Thalpathawadana, TRMYSB, 'International humanitarian law and cyber warfare: sufficiency of international humanitarian law in combating cyber warfare as a new phenomenon' (2015) *South Eastern University Arts Research Session.*

Denning, Dorothy E, 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy' (1999) *Global Problem-Solving Information Technology and Tools* <https://nautilus.org/global-problem-solving/activism-

hacktivism-and-cyberterrorism-the-internet-as-a-tool-for-influencing-foreign-policy-2/.> accessed 3 January 2025.

Denning, Dorothy E, 'Cyberterrorism' (Testimony before the Special Oversight Panel on Terrorism, Committee on Armed Services, US House of Representatives, 23 May 2000) <http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html> accessed 11 January 2025.

Dinstein, Yoram, 'Computer Network Attacks and Self-Defense', in Michael Schmitt and Brian O'Donnell (eds), *Computer Network Attack and International Law* (Naval War College 2002).

Dinstein, Yoram, *The Conduct of Hostilities under the Law of International Armed Conflict* (CUP 2016).

Döge, Jenny, 'Cyber Warfare. Challenges for the Applicability of the Traditional Laws of War Regime' 48(4) (2010) *Archiv des Völkerrechts*.

Dörmann, Knut, "The Applicability of the Additional Protocols to Computer Network Attacks: An ICRC Viewpoint", in Karin Byström (ed.), *International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, 17–19 November 2004, Stockholm Sweden, (Swedish National Defence College 2004).

Droege, Cordula, 'Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians' (2012) 94 *International Review of the Red Cross*.

Duguin, Stéphane, and Pavlova, Pavlina, 'The Role of Cyber in the Russian War against Ukraine: Its Impact and the Consequences for the Future of Armed Conflict' (2023) EP/EXPO/A/COMMITTEE/FWC/2019-01/Lot4/1/C/20.

Duić, Igor, Cvrtila, Vlatko, Ivanjko, Tomislav, (eds), 'International Cyber Security Challenges', 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO 2017).

European Commission, 'Cybercrime' (Migration and Home Affairs, 31 October 2024) <https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en> accessed 20 October 2024.

European Parliament and Council, 'Proposal for a Regulation on Horizontal Cybersecurity Requirements for Products with Digital Elements and Amending Regulation (EU) 2019/1020 COM (2020) 823 final.

Feigenbaum, Joan, Johnson, Aaron, Syverson, Paul, 'A Model of Onion Routing with Provable Anonymity' in *Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007* (Springer 2007).

Fernicola, Gia, 'Once Upon a Time in Cyberspace: A Grim Reality about the Dangers of Cyberwarfare' (2020) 20(2) *International and Comparative Law Review*, DOI: 10.2478/iclr-2020-0004.

Ferraro, Tristan, 'The applicability and application of international humanitarian law to multinational forces' (2013) 95 *International Review of the Red Cross.*

Fidler, David P, *Cybersecurity and International Law* (OUP 2015).

Fonte, Giuseppe, and Amante, Angelo, 'Italy Plans Crackdown on Database Hacks' Reuters (21 November 2024) <https://www.reuters.com/technology/cybersecurity/italy-plans-crackdown-database-hacks-2024-11-21/> accessed 10 September 2024.

France (SGDSN), ‘Stratégie nationale de la Cyberdéfense [*Revue stratégique de cyberdéfense*]’ (Secrétariat général de la défense et de la sécurité nationale (SGDSN) and Economica 2018) <www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/>.

France, ‘International Law Applied to Operations in Cyberspace [*Droit international appliqué aux opérations dans le cyberespace*]’ (Ministère des Armées 2019)<https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations +in+cyberspace.pdf>.

Franke Kleist, Virginia, ‘Global Multinational Organizations: Unintended Threats from Nation-State Cyberwarfare’ (2021) 24(4) *Journal of Global Information Technology Management.*

Franzese, Patrick W, ‘Sovereignty in Cyberspace: Can It Exist?’ (2009) 64 *Air Force L Rev 1.*

Gamble, John King, and Ku, Charlotte, ‘International Law - New Actors and New Technologies: Center Stage for NGOs’ (2000) 31 *Law & Pol'y Int'l Bus*.

Gilani, Iftikhar, ‘Deadly cyber-attacks in Lebanon reveals the new face of warfare’ (Frontline 2024) <https://frontline.thehindu.com/news/lebanon-hezbollah-cyber-attack-pager-explosions-warfare-israel-gaza/article68654302.ece> accessed 28 September 2024.

Gilbert, David, ‘#OpSaveGaza: Anonymous Continues Cyber-Campaign Knocking Israeli Ministry of Defence Website Offline’ (International Business Times 2014) <www.ibtimes.co.uk/opsavegaza-anonymous-continues-cyber-campaign-knocking-israeli-ministry-defence-website-offline-1457580> accessed 10 May 2024.

Global Commission on the Stability of Cyberspace, Advancing Cyber Stability: Final Report (November 2019) <https://cyberstability.org/report/> accessed 30 November 2024.

Gordon, Sarah, Ford, Richard, 'On the definition and classification of cybercrime' (2006) 2 *Journal in Computer Virology* 13-20.

Green, Joshua, 'The Myth of Cyberterrorism' (Washington Monthly 2002) <http://www.washingtonmonthly.com/features/2001/0211.green.html> accessed 10 January 2025.

Green, Joshua, 'The Myth of Cyberterrorism' (*Washington Monthly* 2002) http://www.washingtonmonthly.com/features/2001/0211.green.html accessed 10 January 2025.

Greenberg, Andy, 'The Untold Story of NotPetya, the Most Devastating Cyber Attack in History' (Wired 2018) <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> accessed 29 May 2024.

Greenspan, Morris, *The Modern Law of Land Warfare*, (CUP 1959).

Griffin, Andrew, 'Anonymous War on ISIS: Online Activists Claim to have Foiled Terror Attack on Italy as Part of "Operations ISIS"' (The Independent 2015) https://www.independent.co.uk/tech/anonymous-war-on-isis-online-activists-claim-to-have-foiled-terror-attack-on-italy-as-part-of-operation-isis-a6788001.html accessed 10 May 2024.

Henckaerts, Jean-Marie, and Doswald-Beck, Louise, *Customary International Humanitarian Law, Volume I: Rules* (ICRC 2005).

Holt, Thomas J., Freilich, Joshua D., Chermak, Steven M., 'Exploring the subculture of ideologically motivated cyber-attackers' (2017) 33(3) *Journal of Contemporary Criminal Justice*.

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 (CUP 2016) (Commentaries on the 1949 Geneva Conventions).

ICRC, Commentary on the Third Geneva Convention Relative to the Treatment of Prisoners of War (1960) (Commentaries on the 1949 Geneva Conventions).

ICRC, Commentary on the Third Geneva Convention: Convention (III) relative to the Treatment of Prisoners of War (CUP 2021) (Commentaries on the 1949 Geneva Conventions).

ICRC, 'How is the Term 'Armed Conflict' Defined in International Humanitarian Law?' (Opinion Paper 2008).

ICRC, *International humanitarian law and the challenges of contemporary armed conflicts* (2016) 32IC/15/11.

ICRC, 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts: Excerpt of the Report Prepared by the International Committee of the Red Cross for the 28th International Conference of the Red Cross and Red Crescent Geneva, December 2003' (2004) *Revue Internationale de la Croix-Rouge/International Review of the Red Cross* 86(853).

Islam, Mohammad Saidul, 'Cyber Warfare and International Humanitarian Law: A Study' (2017) 5 *International Journal of Ethics in Social Sciences*.

Italy, 'Italian Position Paper on International Law and Cyberspace' (Ministry of Foreign Affairs and International Cooperation 2021) <https://www.esteri.it/mae/resource/doc/2021/11/italian_position_paper_on_international_law_and_cyberscybe.pdf>.

Jarose, Joanna, ‘Reconsidering the Definition of “Attack” and “Damage” in Cyber Operations during Armed Conflict: Emerging Subsequent State Practice’ (2023) 44 *Adel L Rev*.

Jeutner, Valentin, ‘The Digital Geneva Convention: A Critical Appraisal of Microsoft’s Proposal’ (2019) 10(1) *Journal of International Humanitarian Legal Studies*.

KELA Cyber Intelligence Center, ‘Russia-Ukraine war: pro-Russian hacktivist activity two years on’ (KELA 2024) <https://www.kelacyber.com/russia-ukraine-war-pro-russian-hacktivist-activity-two-years-on/> accessed 30 May 2024.

Kenney, Michael, *Cyber-Terrorism in a Post-Stuxnet World* (Foreign Policy Research Institute 2015).

Kenney, Michael, *Hacktivism, Cyber-Terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace* (DiploFoundation 2003) 23 <https://books.google.it/books?id=oKS2RtaKDm8C> accessed 14 January 2025.

Kerttunen, Mika, Kiisel, Saskia, (eds), ‘Norms for International Peace and Security: The Normative Frameworks of International Cyber Cooperation’ (ICT4Peace Foundation 2015) <https://ict4peace.org/wp-content/uploads/2020/05/16496284.pdf accessed on 10 November 2024>.

Kleffner, Jann., ‘The Legal Fog of an Illusion: Three Reflections on “Organization” and “Intensity” as Criteria for the Temporal Scope of the Law of Non-International Armed Conflict’ (2019) 95 *International Law Studies*.

Kleist, Virginia Franke, ‘Global Multinational Organizations: Unintended Threats from Nation-State Cyberwarfare’ (2021) 24(4) *Journal of Global Information Technology Management*.

Kolb, Robert, *Ius in Bello: Le Droit International Des Conflits Armes; Précis* (Helbing & Lichtenhahn; Bruylant 2003).

Kutub, Thakur, 'An Investigation on Cyber Security Threats and Security Models.', Institute of Electrical and Electronic Engineers (IEEE) 2nd International Conference on Cyber Security and Cloud Computing (IEEE 2015).

Langbroek, Philip, 'Methodology of Legal Research: Challenges and Opportunities' (2017) 13(3) <https://utrechtuniversity.on.worldcat.org:443/atoztitles/link?sid=google> accessed 10 May 2024

Lin, Herbert S., 'Offensive Cyber Operations and the Use of Force' (2010) 4 *JNat'l Sec L & Pol'y*.

Mačák, Kubo, 'Is the International Law of Cyber Security in Crisis?' (2016) 8th International Conference on Cyber Conflict (CyCon 2016) https://doi.org/10.1109/CYCON.2016.7529431 accessed 10 November 2024.

Mačák, Kubo, 'Unblurring the lines: military cyber operations and international law' (2021) 6(3) *Journal of Cyber Policy* https://doi.org/10.1080/23738871.2021.2014919 accessed 10 May 2024.

Margulies, Peter, 'Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility' (2013) 14 *Melbourne Journal of International Law*.

Marx, Christy, *Battlefield Command Systems of the Future* (The Rosen Publishing Group 2005).

McAdam, Doug, Tarrow, Sidney, and Tilly, Charles, *Dynamics of Contention* (CUP 2001)

Melzer, Nils, *Cyberwarfare and International Law* (UNIDIR Resources 2011).

Melzer, Nils, *Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law* (ICRC 2009).

Microsoft Digital Security Unit, *An Overview of Russia's Cyberattack Activity in Ukraine* (Digital Security Unit, 27 April 2022).

Milmo, Dan, 'Anonymous: The Hacker Collective That Has Declared Cyberwar on Russia' (The Guardian 2022) <https://link-gale-com.proxy.library.uu.nl/apps/doc/A695152994/ITOF?u=utrecht&sid=bookmark-ITOF&xid=ab63ae49 > accessed 10 May 2024

Mitchell, Ariana J. B, *Cybersecurity and International Law: Policy Options for a Global Regime* (*Routledge* 2017).

Mikhailo Fedorov, 'We Are Creating an IT Army' (Twitter 2022) <https://x.com/FedorovMykhailo/status/1497642156076511233> accessed 20 April 2024.

Molloy, David, Tid, Joe, 'George Floyd: Anonymous hackers re-emerge amid US unrest' (BBC 2020) <https://www.bbc.com/news/technology-52879000> accessed 10 May 2024.

National Research Council, *Computers at Risk: Safe Computing in the Information Age* (National Academy Press 1991).

North Atlantic Treaty Organization (NATO), *Comprehensive Cyber Defence Policy* (2021) https://www.nato.int/cps/en/natolive/topics_82798.htm accessed 4 November 2024.

North Atlantic Treaty Organization (NATO) Glossary of Terms and Definitions AAP-06 (2019) <https://www.coemed.org/files/stanags/05_AAP/AAP-06_2019_EF.pdf> accessed on 30 October 2024.

Noortmann, Math, Ryngaert, Cedric, 'Introduction: Non-state Actors: International Law's Problematic Case' in Math Noortmann and Cedric Ryngaert (eds), *Non-state Actor Dynamics in International Law: From Law-Takers to Law-Makers* (Ashgate 2010).

O'Connell, Mary Ellen, Arimatsu, Louise, Wilmshurst, Elizabeth, 'Cyber Security and International Law' *International Law Meeting Summary* (Chatham House 2012).

Olsen, Parmy, 'We are Anonymous: Inside the Hacker World of LulzSec', *Anonymous and the Global Cyber Insurgency* (2012).

'Operation Payback', Radware <https://www.radware.com/security/ddos-knowledge-center/ddospedia/operation-payback/> accessed 10 May 2024.

Ottis, R., Lorents, P., *Cyberspace: Definition and Implications* (2010) In: 'Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April', Reading: Academic Publishing Limited 267-270 <https://ccdcoe.org/library/publications/cyberspace-definition-and-implications/> accessed on 4 November 2024.

Paganini, Pierluigi, *Cybersecurity and Critical Infrastructures: The Role of the EU in Tackling Cyber Threats* (CSSII 2022) https://www.cssii.unifi.it/upload/sub/Pubblicazioni/2022_Paganini_Pierluigi.pdf accessed 14 December 2024.

Paris Call for Trust and Security in Cyberspace (adopted 12 November 2018) https://pariscall.international/en/ accessed 4 November 2024.

Pawan, R. S., '21st century warfare: from "battlefield" to "battlespace"' (Future Wars 2017) <https://futurewars.rspanwar.net/21st-century-warfare-from-battlefield-to-battlespace/> accessed 10 May 2024.

Picker, Colin B., ‘A View from 40,000 Feet: International Law and the Invisible Hand of Technology’ (2001) 23 *Cardozo L Rev*.

Polityuk, Pavel, Vukmanovic, Oleg, and Jewkes, Steven, ‘Ukraine’s Power Outage Was a Cyber Attack: Ukrenergo’ (Reuters 2017) <https://www.reuters.com/article/world/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BB/> accessed 10 May 2024.

Privacy International and CILD, ‘Call to Amend DDL Orlando on Hacking’ (Liberties 2024) <https://www.liberties.eu accessed> accessed 25 September 2024.

Puspoayu, E. S., Widodo, H., Ronaboyd, I., and Lovisonnya, I., ‘Legal Classification on the Armed Conflict Between Ukraine and Russia in Light of International Humanitarian Law’ in SHS Web of Conferences (149 EDP Sciences, 2022) 03020.

Radoniewicz, Filip, ‘Cyberspace, Cybercrime, Cyberterrorism’ In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) *Cybersecurity in Poland* (Springer, Cham 2022) <https://doi.org/10.1007/978-3-030-78551-2_2>.

Radziwill, Yaroslav, *Cyber-Attacks and the Exploitable Imperfection of International Law* (Brill & Martinus Nijhoff Publishers 2015).

Reuter, Christian (ed), Information Technology for Peace and Security: IT Applications and Infrastructures in *Conflicts, Crises, War, and Peace* (Springer Fachmedien Wiesbaden 2019) <http://link.springer.com/10.1007/978-3-658-25652-4> accessed 10 May 2024.

Roberts, Anthea, and Sivakumaran, Sandesh, ‘Lawmaking by Nonstate Actors: Engaging Armed Groups in the Creation of International Humanitarian Law’ (2012) 37 *Yale J Int'l L*.

Rodenhäuser, Tilman, and Vignati, Mauro, '8 rules for "civilian hackers" during war, and 4 obligations for states to restrain them' (EJIL:Talk! 2023) <https://www.ejiltalk.org/8-rules-for-civilian-hackers-during-war-and-4-obligations-for-states-to-restrain-them/> accessed 28 April 2024.

Russian Federation, 'Doctrine of Information Security of the Russian Federation' (2016) 34 <http://www.scrf.gov.ru/security/information/DIB_engl/>.

Russia-Ukraine Crisis: Anonymous Hacker Takes Down Russian Govt Sites, Unleashes Cyber War <https://www.youtube.com/watch?v=Rdns1BOgC-0> accessed 10 May 2024.

Ryngaert, Cedric, 'Non-State Actors: Carving out a Space in a State-Centred International Legal System' (2016) The Netherlands International Law Review.

Sands, G, *What to Know About the Worldwide Hacker Group 'Anonymous'* (ABCNews, 2016) <https://abcnews.go.com/US/worldwide-hacker-group-anonymous/story?id=37761302> accessed 10 May 2024.

Schechner, Sam, 'Ukraine's 'It Army' Has Hundreds of Thousands of Hackers, Kyiv Says' (The Wall Street Journal, 4 March 2022) <https://www.wsj.com/livecoverage/russia-ukraine-latest-news-2022-03-04/card/ukraine-s-it-army-has-hundreds-of-thousands-hackers-kyiv-says-RfpGa5zmLtavrot27OWX> accessed 30 May 2024>.

Schmitt, Michael N., 'Classification of Cyber Conflict' (2012) 17(2) *Journal of Conflict and Security Law*.

Schmitt, Michael N., 'Cyber Operations and the Jud Ad Bellum Revisited' (2011) 56 *Vill L Rev* 569.

Schmitt, Michael N., ‘Ukraine Symposium – Are We at War?’ (Articles of War 2022) <https://lieber.westpoint.edu/are-we-at-war>.

Schmitt, Michael N., (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

Schmitt, Michael N., and Watts, Sean, ‘Beyond State-Centrism: International Law and Non-State Actors in Cyberspace’ (2016) 21 *Journal of Conflict and Security Law*.

Schmitt, Michael N., and Watts, Sean, ‘The Decline of International Humanitarian Law Opinio Juris and the Law of Cyber Warfare’ (2015) 50 *Tex Int'l L J*.

Schwart, Mathew J, ‘Anonymous: 10 Things We Have Learned In 2013’ (DarkReading, 2013) <https://www.darkreading.com/cyberattacks-data-breaches/operation-payback-feds-charge-13-on-anonymous-attacks> accessed 10 May 2024.

Shackelford, Scott J., Russell, Scott, and Kuehn, Andreas, ‘Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors’ (2016) 17(1) *Chicago Journal of International Law*.

Sher, Jake B., ‘Anonymous Armies: Modern Cyber-Combatants and Their Prospective Rights under International Humanitarian Law’ (2016) 28 *Pace Int'l L Rev.*

Soesanto, Stefan, ‘The IT Army of Ukraine. Structure, Tasking, and Ecosystem’ (Cyberdefence Report 2022).

Somaiya, Ravi, ‘Hackers Shut Down Government Sites’ (TheNewYorkTimes 2011) <https://www.nytimes.com/2011/02/03/world/middleeast/03hackers.html> accessed 10 May 2024.

Stewart K. Bertram, ‘Authority and Hierarchy within Anonymous Internet Relay Chat Networks’ (2015) 6 *Journal of Terrorism Research*.

Stewart K. Bertram, *The Tao of Open Source Intelligence* (IT Governance Publishing 2015).

Stiano, Alessandro, ‘L’intervento di Anonymous nel conflitto tra Russia e Ucraina: Alcune riflessioni sullo status giuridico degli hacker attraverso il prisma del diritto internazionale umanitario’ (2022) *Ordine Internazionale e Diritti Umani*.

Stirone, Angelo, ‘Hacking and International Humanitarian Law’ (2020) 3(1/2) *Humanitäres Völkerrecht: Journal of International Law of Peace and Armed Conflict*.

Svyrydenko, Denys, and Możgin, Wiktor, ‘Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia’s War against Ukraine’ (2022) 17 *Future Human Image* <https://doi.org/10.29202/fhi/17/6> accessed 10 May 2024.

Tech Accord, TM 2.0: Principles for Tackling Cyber Threats (2021) <https://cybertechaccord.org/tm2-0/> accessed 30 November 2024.

Text Anon, ‘We are Anonymous. We do not forgive. We do not forget’ (Dazed, 2013) [Anonymous Manifesto], accessed 10 May 2024, <https://www.dazeddigital.com/artsandculture/article/16308/1/we-are-anonymous-we-do-not-forgive-we-do-not-forget>.

The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, OJ EU C 2014.32.19., <http://www.europarl.europa.eu/meetdocs/2009_2014/documents/join/com_join(2013)0001_/com_join(2013)0001_pl.pdf>.

The Netherlands, ‘Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in

cyberspace' and 'Appendix: International Law in Cyberspace' (Ministry of Foreign Affairs 2019) < https://www.government.nl/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace>.

Thomas Brewster, 'Moscow Exchange, Sberbank Websites Knocked Offline – Was Ukraine's Cyber Army Responsible?' (Forbes 28 February 2022) <https://www.forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank-websites-knocked-offline-was-ukraines-cyber-army-responsible/?sh=5dda2477cae3 accessed 30 May 2024>.

Tidy, Joe, 'Meet the hacker armies on Ukraine's cyber front line' (BBC 2023) <https://www.bbc.com/news/technology-65250356> accessed 30 May 2024.

United Nations General Assembly, Measures to Eliminate International Terrorism, UNGA Res 49/60 (adopted 9 December 1994) UN Doc A/RES/49/60.

United Nations General Assembly, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (9 September 2013) UN Doc A/68/156/Add.1.

United Nations General Assembly, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security' (30 June 2014) UN Doc A/69/112.

United Nations General Assembly, 'Report of the Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security (Addendum)' (18 September 2014) UN Doc A/69/112/Add1.

United Nations General Assembly, Resolutions on Cybersecurity, UNGA Res 73/27 (adopted 5 December 2018) UN Doc A/RES/73/27.

United Nations General Assembly, Resolutions on Cybersecurity, UNGA Res 74/28 (adopted 12 December 2019) UN Doc A/RES/74/28.

United Nations Group of Governmental Experts, *Final Report of the 2019-2021 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (2021) UN Doc A/76/135.

United Nations Group of Governmental Experts, *Norms, Rules, and Principles for Responsible State Behaviour in Cyberspace,* Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace (2015).

United Nations Office on Drugs and Crime, 'Hacktivism' (E4J University Module Series: Cybercrime) https://www.unodc.org/e4j/zh/cybercrime/module-14/key-issues/hacktivism.html accessed 15 January 2025.

United Nations, *Open-Ended Working Group on the Use of Information and Communications Technologies in the Context of International Security (OEWG), 'Final Report'* (2021) UN Doc A/75/818.

United Nations Security Council, 'Report of the High-level Independent Panel on Peace Operations' (adopted 17 June 2015) UN Doc A/70/95 [122] <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2015_446.pdf > accessed 29 May 2024

United Kingdom, 'National Cyber Security Strategy' (2016) 63 <www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021>.

Väljataga, Ann, 'Cyber Vigilantism in Support of Ukraine: A Legal Analysis' (2022) *NATO Cooperative Cyber Defence Centre of Excellence*.

Ventre, Daniel, *Cyberespace et acteurs du cyberconflit* (Lavoisier & Hermes 2011).

Vibhute, Khushal, and Aynalem, Filipos, 'Legal Research Methods' (2009) 17 *Ethiopian Legal Bief*.

Vu, Anh V., and others, 'Getting Bored of Cyberwar: Exploring the Role of Low-Level Cybercrime Actors in the Russia-Ukraine Conflict' (Proceedings of the ACM on Web Conference, 2024).

Watts, Sean, 'Combatant Status and Computer Network Attack' (2010) 50 *Virginia Journal of International Law*.

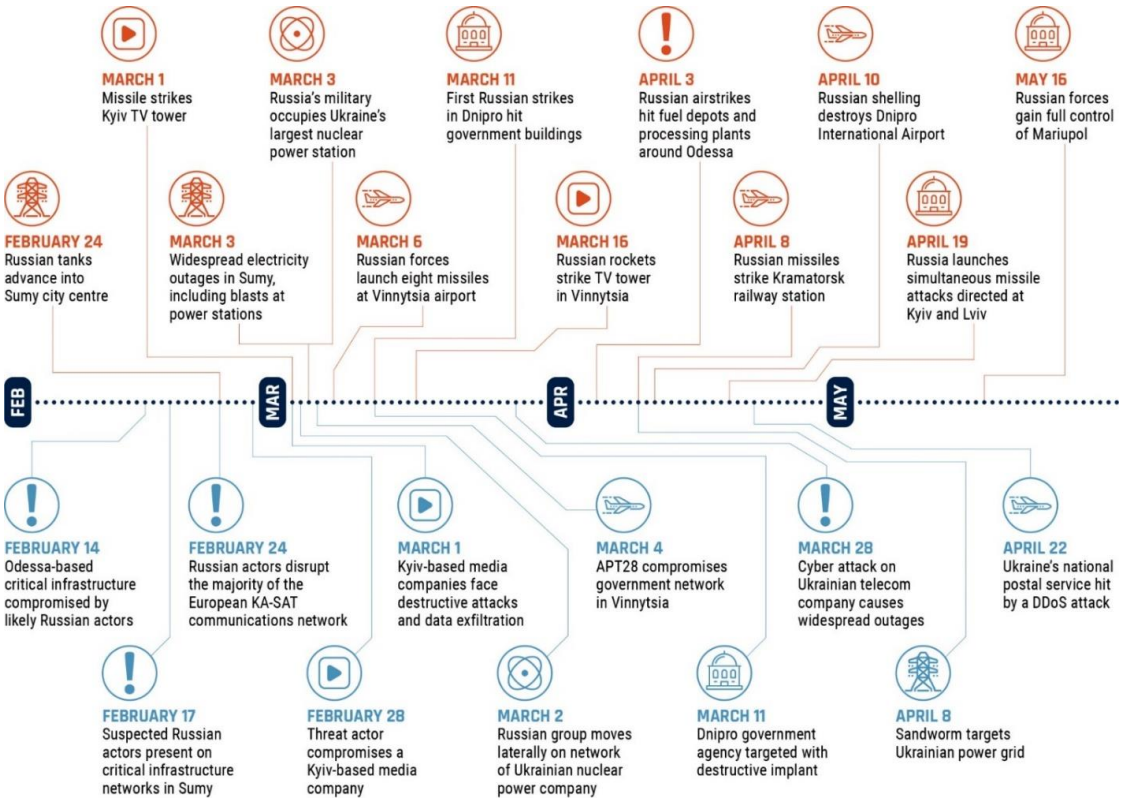
Weimann, Gabriel, 'Cyberterrorism: The Sum of All Fears?' (2005) 28(2) *Studies in Conflict and Terrorism*.

Wentker, Alexander, Miles, Jackson, and Hill-Cawthorne, Lawrence, 'Identifying Co-Parties to Armed Conflict in International Law: How States, International Organizations and Armed Groups Become Parties to War' (2024) Research Paper, Royal Institute of International Affairs <https://doi.org/10.55317/9781784136017>

Zdzikot, Tomasz, 'Cyberspace and Cybersecurity' In: Chałubińska-Jentkiewicz, K., Radoniewicz, F., Zieliński, T. (eds) *Cybersecurity in Poland* (Springer, Cham 2022) <https://doi.org/10.1007/978-3-030-78551-2_2>.

ANNEXES

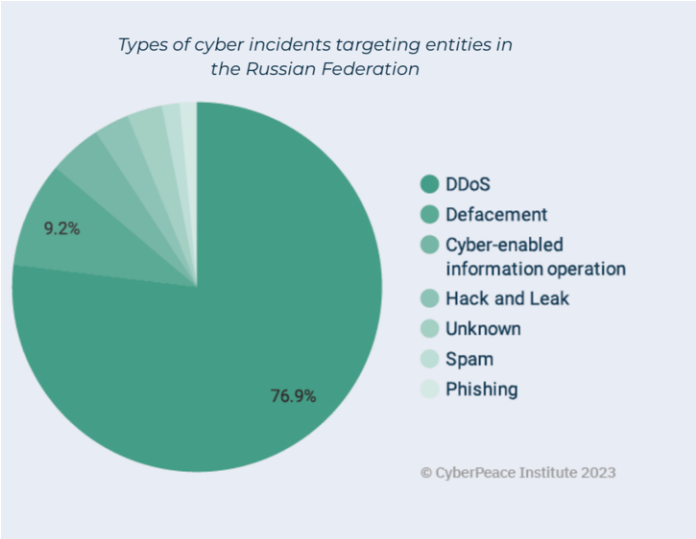
A. Illustration: Timeline of Kinetic Attacks and Cyber-Operations in Ukraine from 14 February to 16 May

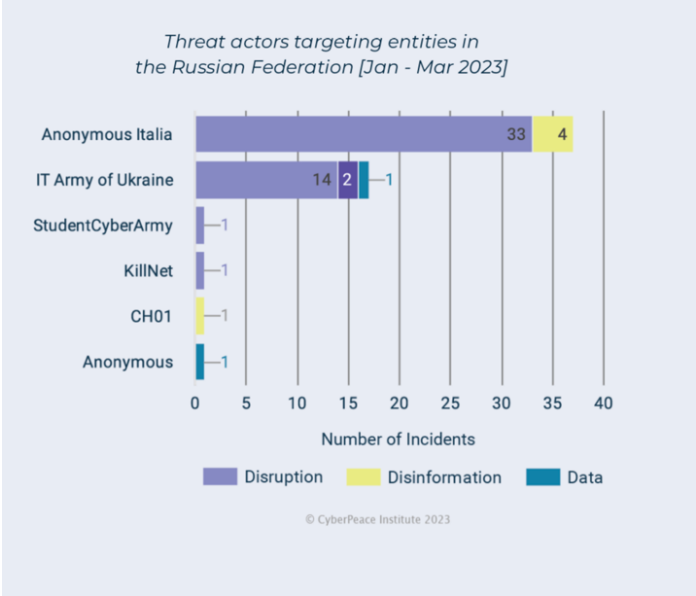


"This graph shows examples of significant Russian cyber activity (blue, below the timeline) and kinetic activity (orange, above the timeline)."[720]

[720] *Cyber Threat Bulletin*, 3.

B. Illustrations: Trends and emerging issues regarding Russian Federation from January to March 2023 [721]





[721] Cyber Dimention of the Armed Conflict in Ukraine', (CyberPeace Institute, 2023) <https://reliefweb.int/report/ukraine/cyber-dimensions-armed-conflict-ukraine-q1-2023> accessed on 10 May 2024.

Top 5 sectors impacted in the Russian Federation [Jan - Mar 2023]

	Sector	Incidents ▾	% Δ
1.	Financial	15	275.0% ↑
2.	Transportation	9	800.0% ↑
3.	Media	6	500.0% ↑
4.	Administrative / Support	5	∞
5.	ICT	5	-16.7% ↓