UNIVERSIDADE CATÓLICA PORTUGUESA

Application of the Principle of Distinction to the cyber domain

Iasnaya Rodrigues Abel

Master's degree in law

Porto Faculty of Law

2025

UNIVERSIDADE CATÓLICA PORTUGUESA

Application of the Principle of Distinction to the cyber domain

Iasnaya Rodrigues Abel

Supervisor: Prof. Dra. Maria Isabel Tavares

Master's degree in law

Porto Faculty of Law

2025

“Aos meus pais, que, sob muito sol,

me fizeram chegar até aqui à sombra”.

RESUMO

Os avanços tecnológicos e a crescente digitalização dos conflitos armados trouxeram novos desafios para a aplicação do Direito Internacional Humanitário. Neste sentido, a presente dissertação aborda a interpretação e aplicação do princípio da distinção no domínio cibernético, analisando a sua aplicação à luz das particularidades deste contexto, bem como as questões daí emergentes. Especificamente, analisa a sua aplicação no que respeita à diferenciação entre civis e combatentes, bem como entre objetos e alvos militares. Para além disso, explora também o exemplo contemporâneo do Exército tecnológico ucraniano e discute a atribuição da responsabilidade aos Estados no contexto dos conflitos cibernéticos. Por fim, conclui que apesar das regras existentes serem aplicáveis ao contexto cibernético, um maior desenvolvimento se faz necessário para garantir a efetividade do Direito Internacional Humanitário, nomeadamente do princípio da distinção – considerando a dificuldade de transpor e aplicar as regras de um ambiente cinético para o cibernético.

Palavras-chave: domínio cibernético, combatentes, civis, direito internacional humanitário, princípio da distinção.

ABSTRACT

Technological advances and the increasing digitalization of armed conflicts have brought new challenges for the application of International Humanitarian Law. In this sense, this dissertation addresses the interpretation and application of the principle of distinction in the cyber domain, analyzing its application in light of the particularities of this context, as well as the issues arising from it. Specifically, it examines its application regarding the differentiation between civilians and combatants, as well as between objects and military targets. Furthermore, it also explores the contemporary example of the Ukrainian IT Army and discuss the attribution of responsibility to States in the context of cyberconflicts. Finally, it concludes that, even though the existing rules are applicable to the cyber context, further development is needed to guarantee the effectiveness of International Humanitarian Law, namely the principle of distinction – considering the difficulty of transposing and applying the rules from a kinetic to a cyber environment.

Keywords: cyber domain, combatants, civilians, international humanitarian law, principle of distinction.

TABLE OF CONTENTS

LIST OF ABREVIATIONS

AP – Additional Protocol

ATM – Automated Teller Machine

DDos – Distributed Denial-of-Service

EU – European Union

ICJ – International Court of Justice

ICRC – International Committee of the Red Cross

ICTY – International Criminal Tribunal for the former Yugoslavia

IGE – International Group of Experts

IHL – International Humanitarian Law

IIL – Institute of International Law

ILC – International Law Commission

IP – Internet Protocol

IT – Information Technology

NATO – North Atlantic Treaty Organization

OAG – Organized Armed Group

OCHA – United Nations Office for the Coordination of Humanitarian Affairs

RSIWA – Responsibility of States for Internationally Wrongful Acts

UN – United Nations

US – United States

USCYBERCOM – United States Cyber Command

USSR – Union of the Soviet Socialist Republics

WWI – World War I

1. INTRODUCTION

The use of cyber operations during armed conflicts is a reality. In the past 20 years the use of cyber operations and the question of how IHL applies to those have developed significantly[1]. Moreover, lately, cyber operations have shown that they can seriously affect civilian infrastructure and might result in human harm[2] – and is likely to be more prominent in the future. In addition, the current society is increasingly cyber-reliant, raising several concerns regarding the development of new cyber weapons[3]. Given this, questions have emerged about whether and how IHL should be interpreted and applied in cyber domain[4].

In this context, ideally, the IHL rules would simply apply to cyberwarfare, since it consists in a mere new mean and method of warfare[5]. However, considering the difference between a traditional and a cyber battlefield, the applicability of many rules is posed into question – especially concerning the principle of distinction[6]. Therefore, multilateral debates on this matter have been ongoing for many years[7], and although some States had agreed on some aspects of the legal and normative framework that regulates cyber warfare[8], no consensus has been reached. Thus, IHL's applicability to cyber operations during armed conflict continues to be highly debated[9].

Given this, discussing and comprehending how the principle of distinction is interpreted and applied on the cyber domain is crucial - not only to the individuals and objects protected by IHL, but also for the States that are acquiring cyber capabilities and developing tactics for their use. Following this reasoning, this thesis intends to analyze the application of this principle considering the particularities of the cyber domain. Initially by briefing exposing its origin and reasoning of its applicability in the cyber context, and then addressing the differentiation between civilians, combatants and objects and military targets. Furthermore, examining the example of the IT Army of Ukraine, and discussing the attributability of responsibility to States in cyberconflicts - aiming to comprehend the current state of the interpretation and application of the principle in issue.

---

[1] Gisel et al., 2020.
[2] ICRC, 2020.
[3] Schmitt, 2013.
[4] *Ibid*. 3.
[5] Huang & Ying, 2020.
[6] *Ibid.* 5.
[7] *Ibid.* 5.
[8] *Ibid.* 1.
[9] *Ibid.* 1.

2. THE PRINCIPLE OF DISTINCTION: ORIGIN AND APPLICATION TO THE CYBER DOMAIN

The idea of distinction has always been in tension with armed conflicts[10]. Since the US Civil War, the idea that civilians should enjoy special protection has been supported by governments[11]. At the time, President Lincoln adopted the Lieber Code, which recognized the principle of distinction referring to a differentiation between "the private individual belonging to a hostile country and the hostile country itself, with its men in arms"[12]. Immediately after this conflict the principle was formalized in international law as part of the Saint Petersburg Declaration of 1868 – which stated, in the preamble, that "the only legitimate object which states should endeavor to accomplish during war is to weaken the military forces of the enemy"[13], summarizing the idea that "would later grow into a full-fledged doctrine"[14].

Thereafter, and over the years, there were many other attempts to codify the war laws, including this idea of distinguishing participants and non-participants in a conflict. The Convention on Land Warfare and the Convention on Naval Forces, for example, demonstrated a "growing belief in the difference between civilian and military targets"[15]. Later, on WWI, some states committed to this idea by adhering to the letter of the Principle of Distinction, although the combatants did not follow it[16]. After this, because of the changes of warfare, the rules proposed by The Hague Rules of Air Warfare of 1923 were a "ringing endorsement of the Principle of Distinction (…) But not a single country adopted"[17]. Instead, the "countries issued non-binding policy statements during the interwar period"[18] and in 1938 the League of the Nations adopted a non-binding resolution with principles proposed by the British Prime Minister, which were: it is illegal to bomb or deliberately attack civilians; targets attacked from the air must be identified military objectives; and military objectives must be attacked with reasonable care so civilians are not hurt[19]. A year later, when Germany invaded Poland, European Governments and President Roosevelt agreed that civilian populations and unfortified

[10] Sweney, 2005.
[11] *Ibid.* 10.
[12] Lieber, 1898, p. 9.
[13] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight, 1868.
[14] *Ibid*. 10, p. 738.
[15] *Ibid*. 10, p. 738.
[16] *Ibid*. 10.
[17] *Ibid*. 10, p. 738.
[18] *Ibid*. 10, p. 739.
[19] *Ibid*. 10.

cities would not be bombed[20]. However, "perhaps never in the history of armed conflict has a promise been more thoroughly broken"[21].

In this scenario, the principle of distinction was weakened and abandoned in 1943. Since even though "attacking civilian targets was not originally the goal of American and British commanders (…) The targeting of enemy civilians was something that the Allies gradually decided to do"[22] – therefore "distinction (…) seemed dead"[23]. In this context, there were no more attempts to codify it until 1950, when the ICRC proposed to expand the Geneva Conventions of 1949 to include distinction[24]. At the time, the IIL and the UN also drafted proposals, but none of them was adopted and "the issue was eventually dropped"[25].

Although the ICRC, since the beginning of its work, considered necessary to explicitly confirm the concept of the distinction in a treaty, the idea was that "in the conduct of military operations, a distinction should be made at all times between (…) persons who directly participate in military operations and (…) persons who belong to the civilian population"[26]. However, only in 1974, at the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts, the idea really re-emerged[27]. In this context, the ICRC introduced a draft to the Conference which stated that:

> To ensure respect for the civilian population, the Parties to the conflict shall confine their operations to the destruction or weakening of the military resources of the adversary and shall make a distinction between the civilian population and combatants, and between civilian objects and military objectives[28].

After several amendments, the Committee III decided on the present text of the article, and later, the Conference "drafted and submitted Additional Protocols I and 1I to

[20] *Ibid*. 10.
[21] *Ibid*. 10, p. 740.
[22] *Ibid*. 10, p. 740.
[23] *Ibid*. 10, p. 740.
[24] Meyer, 2001.
[25] *Ibid*. 10, p. 741.
[26]ICRC*,* article 48, 1987.
[27] *Ibid*. 10.
[28] *Ibid.* 26

the 1949 Geneva Conventions"[29]. As a result, the principle of distinction was officially laid down - in proper sense - as part of IHL, in the 1977 AP to the Geneva Conventions[30]. As the Official Records of the Conference show, this measure was adopted by consensus[31]. France, in its vote, refers that its elaboration was made with humanitarian purposes, and USSR, in its statement, acknowledges the approval of the article as a "major step forward in the development of IHL"[32]: Moreover, affirms that the article "develops a basic principle of international humanitarian law (…) one of the main (…) of the present-day international law"[33], giving a "wider protection to the civilian population"[34].

Currently, although not all states have ratified the AP, "most governments and commentators have wholeheartedly accepted the principle"[35], agreeing that the Protocol's statements about the principle express international customary law - with the US government expressly recognizing this principle as part of it[36]. In addition, as results from the ICJ case law, this principle has a customary character, thus representing a basic value of the international community and must be applied to any type of armed conflict[37]. However, although these fundamental questions about the principle have been consolidated in IHL, contemporaneity has brought new challenges to its application - given the increasing use of cybertechnology for military purposes and the consequent digitalization of conflicts, which raises questions about the identification of legitimate targets, combatants, and protection of civilians.

In this sense, since IHL does not contain a definition of cyber operation, the determination of whether it applies to it has to be made on its nature, effects, and circumstances[38]. In this context, there is an increasing recognition among states that IHL applies in cyberspace and to cyber operations during armed conflicts. The 2013 and 2015 reports of UN Group of Governmental Experts pointed that international law, and particularly the UN Charter, is applicable to the information and communication technologies environment – which was further confirmed by the UN General Assembly[39].

---

[29] *Ibid*. 10, p. 741.
[30] *Ibid*. 10.
[31] ICRC, 1978.
[32] *Ibid*. 31, p 201.
[33] *Ibid*. 31, p 200.
[34] *Ibid*. 31, p 201.
[35] *Ibid*. 10, p. 735.
[36] *Ibid*. 10.
[37] *Ibid*. 10.
[38] *Ibid.* 1.
[39] *Ibid.* 1.

Aligned with this, an increasing number of states and international organizations, such as EU and NATO, asserted that IHL applies to cyber operations during armed conflict. In the ICRC view, there is no doubt that cyber operations during armed conflicts are regulated by IHL "just as it regulates the use of any other weapon, mean or method of warfare in armed conflict, new or old"[40]. For them, the fact that these operations rely "on new and continuously developing technology does not prevent the application of IHL to the use of such technology"[41] as a warfare method. This position can be supported by the ICJ on *Legality of the Threat or Use of Nuclear Weapons*, in which the court held that the established principles and rules of IHL apply both to all forms of warfare and kinds of weapons, including the ones of the future[42].

Moreover, considering that the objective and purpose of IHL is to regulate future conflicts, when adopting IHL treaties, States include rules that anticipate the development of new means and methods of warfare and presume that IHL will be applied. In this regard, the Saint Petersburg Declaration, for example, intended that its principles should be maintained with respect to "future improvements which science may effect in the armament of troops"[43]. Also, the obligation provided by article 36 of AP I assumes that IHL applies to new weapons, means and methods – including those which rely on cyber technology[44].

Ultimately, according to the Tallinn Manual, the law of armed conflict "applies to cyber operations as it would to any other operations undertaken in the context of an armed conflict"[45]. The IGE was unanimous in this conclusion, because the condition to IHL's application is the existence of an armed conflict. Therefore, in the cyber context, there must simply exist a nexus between the cyber activity and the armed conflict to IHL be applied[46]. However, there is some disagreement related to the nature of this nexus. One view affirms that IHL governs any cyber activity conducted by a party to an armed conflict against its opponent[47]. While others state that the cyber activity "must have been undertaken in furtherance of the hostilities (…) to contribute to the originator's military effort"[48].

---

[40] *Ibid. 2*, p. 484
[41] *Ibid.* 1, p 298.
[42] ICJ, 1996.
[43] *Ibid.* 13
[44] *Ibid.* 1.
[45] *Ibid. 3*, p. 68.
[46] *Ibid.* 3.
[47] *Ibid* 3.
[48] *Ibid*. 3, p.69.

Finally, given that IHL applies to cyber operations during armed conflicts, the question is whether all or only some of its rules are applicable in this context. Concerning this, we have rules that are applied to all weapons, means and methods of warfare wherever they are used, and others specific to certain weapons or domains. The main customary principles which regulate the conduct of hostilities, including the principle of distinction, belong to the first type and, therefore, apply to cyber operations during armed conflicts[49]. Given this, chapters three and four will discuss the application of this principle, on the cyber domain, concerning the distinction between civilians and combatants, as well as between civilian objects and military targets - and the challenges arising from it.

3. MILITARY OBJECTIVES AND CIVILIAN OBJECTS

According to AP I to article 52 (2) military objects are "those which by their nature, location, purpose or use make an effective contribution to the military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage"[50]. According to the ICRC Commentary, nature corresponds to the inherent character of the object, while purpose concerns its intended use[51]. And two elements must be met to an object be considered as military: make an effective contribution to military action and its attack offers a definitive military advantage[52].

In this context, an 'effective contribution' is the one "closely and obviously linked to military operations"[53]. And regarding the gain of 'definite military advantage', it must be definite and concrete, not being considered the potential, indeterminate or political ones. As provides the Tallin Manual, this advantage is the one "accruing from an attack"[54] and "must be assessed by reference to the attack considered as a whole and not only from isolated or particular parts"[55]. Lastly, there is also the 'situational relevance' which by mentioning "under the circumstances ruling at the time"[56] means that it must be assessed

[49] *Ibid*. 1.
[50] ICRC, article 52, 1987
[51] ICRC*,* 1987.
[52] Mavropoulou, 2015.
[53] *Ibid. 52, p. 40.*
[54] *Ibid.* 3, p. 111.
[55] *Ibid.* 3, p. 111.
[56] *Ibid. 3*, p. 112.

"under a temporal framework that consists of the initial planning of the attack until the final execution"[57].

Given this, although both requirements are equivalent, in the cyber context, where the military uses the same infrastructure as the civilians for its military action, the second requirement becomes more autonomous[58]. Because, considering that the "cyberspace is relatively resilient"[59], a partial destruction of a network, for example, "might effectively contribute to military action but will hardly offer a definite advantage in the end"[60]. Thus, in the cyber domain, the determination of an object's nature is made *a fortiori*[61], since the definition of military objective is relative[62] and "there is no fixed borderline between civilian objects and military objectives"[63]. Lastly, concerning the definite military advantage, its early identification is difficult, since its measurement in this context can be specially challenging[64].

As referred, in the cyber domain the military uses the same cyber infrastructure as the civilian population. And, because of the *sui generis* nature of the cyberspace, where there is a "inherent interconnectedness of civilian and military system"[65], "the definition of military objective applied to cyber operations can render many components of the civilian cyber infrastructure military objectives by use"[66]. In this regard, the dual use targets are those "used for civilian and military purposes"[67], such as satellites, cables, servers and computers[68]. Thus, in theory, "the systemic interconnectivity renders the whole cyber domain a potential dual-use target"[69], and "every bit of memory capacity (…) has a military potential at all times"[70]. However, the understanding that the whole cyber domain is a potential military objective is farfetched, since even if the entire cyber infrastructure of a belligerent state can be qualified as a military objective by use, "it is still difficult to prove that the object's contribution"[71] is both effective to the military action and closely

[57] *Ibid. 52,* p. 44
[58] *Ibid.* 52.
[59] *Ibid.* 52, p. 44.
[60] *Ibid.* 52, p. 44.
[61] *Ibid.* 52.
[62] Dinstein, 2002.
[63] *Ibid.* 62, p. 144 *apud* Albrecht Randelzhofer, Civilian Objects, *Encyclopedia of public international law*, 1992.
[64] *Ibid.* 52.
[65] Geib & Lahmann, 2012, p. 383.
[66] *Ibid.* 52, p.45.
[67] Hathaway *et al.*, 2024, p. 6.
[68] *Ibid. 52.*
[69] *Ibid. 52, p. 46.*
[70] *Ibid. 68, p. 389.*
[71] *Ibid. 52, p. 46.*

- as the definition requires. In addition, it is "highly unlikely that the cyber domain as a whole could effectively contribute to the war effort offering at the same time a definite military advantage"[72].

In this context, since "an object cannot simultaneously have civilian and military status"[73], if a dual use object is acknowledged as military under the definition, its civilian use "would have to be assessed under the proportionality assessment"[74]. For these objects, AP I article 52 (3) provides that in case of doubt, it shall be presumed as civilian. However, since this paragraph is not part of the customary IHL, the Tallinn Experts could not achieve unanimous consensus on its customary nature and application on cyber domain[75]. Instead, its rule 102 provides that if there is any doubt if "an object and associated cyber infrastructure (…) normally dedicated to civilian purposes is being used to make an effective contribution to military action"[76], the determination of the object's use must be done by the attacker "following a careful assessment"[77].

Additionally, as the document 'International Humanitarian Law and the Challenges of Contemporary Armed Conflicts' provides, there is an increasing concern about safeguarding essential civilian data[78]. According to the organization, the protective rules are comprehensive for some categories of objects that enjoy protection under IHL, such as the medical data belonging to medical facilities[79], given protection to the data of protected facilities. However, it is necessary to understand to which extent the not protected civilian data is covered by the existing rules.

To clarify this, it is important to comprehend if data itself is considered as an object under IHL. According to the ICRC Commentary on the AP, object means "something placed before the eyes, or presented to the sight or other sense, an individual thing seen, or perceived, or that may be seen or perceived; a material thing"[80]. That is, "something (…) visible and tangible"[81]. Considering this, the IGE was divided concerning the characterization of data as an object. The majority stated that, considering the intangibility of data; its inconsistence with the ordinary meaning of the term object; and its non-

[72] *Ibid.* 52, p. 46..
[73] *Ibid.* 52, p. 47.
[74] *Ibid.* 52, p. 47.
[75] *Ibid. 52.*
[76] Schmitt, 2017, p. 448.
[77] Schmitt, 2017, p. 448.
[78] McCormack, 2018.
[79] *Ibid.* 78.
[80] ICRC, article 52, 1987.
[81] *Ibid.* 80.

correspondence with the ICRC 1987 Commentary, an attack against it does not qualify as an attack unless it affects "the functionality of cyber infrastructure or results in other consequences that would qualify the cyber operation in question as an attack"[82] - such as against targets subjected to special protection under law, like hospitals[83]. That is, "the targeting of any such data resulting in death or serious harm, or causing physical damage extending to loss of functionality of computers or other physical cyber infrastructure would constitute an attack to which the rules of targeting apply"[84]. However, when it comes to operations against civilian data that does not cause physical consequences, there is disagreement regarding its subjection to the laws of targeting[85]. Lastly, for some scholars, interpreting data as an object would "greatly expand the class of permissible targets in warfare, and is counter to the object and purpose of enhancing the protection of civilians during (…) armed conflict"[86]. Thus, for them, data itself does not benefit from IHL protection, consequently being targetable[87].

On the other hand, a minority affirmed that this position is underinclusive, failing to include the cases of attack against data *per se*. Thus, "the deletion of essential civilian datasets (…) would potentially escape the regulatory reach of the law of armed conflict, thereby running counter to the principle (…) that the civilian population enjoys (…) protection from the effects of hostilities"[88]. For them, the key factor lies in the severity and consequences of the operation, not in the harm's nature. Consequently, "at a minimum, civilian data that is 'essential' to the well-being of the civilian population is encompassed in the notion of civilian objects"[89] and should be protected as such[90]. Following this reasoning, considering that "the issue of striking economic targets is becoming more and more appealing to cyber targeteers"[91] and that deleting certain data "could quickly bring government services and private businesses to a complete standstill, and (…) cause more harm to civilians than the destruction of physical objects"[92], the understanding that this kind of attack would not be forbidden under IHL it is "difficult to

[82] Schmitt 2017, p. 437.
[83] *Ibid.* 78.
[84] *Ibid.* 78 p. 238.
[85] *Ibid*. 78.
[86] *Ibid.* 5, p. 361.
[87] *Ibid.* 78.
[88] Schmitt 2017, p. 437.
[89] Schmitt 2017, p. 437.
[90] *Ibid. 78.*
[91] *Ibid. 52, p. 41.*
[92] *Ibid. 78. p. 237.*

reconcile with the object and purpose of this body of norms"[93]. Also, exclude data from the IHL protection "would result in an important protection gap"[94].

Moreover, according to the principle of contemporaneity, "the terms of a treaty must be interpreted according to the meaning which they possessed, or which would have been attributed to them, and in the light of current linguistic usage, at the time when the treaty was originally concluded"[95]. In this sense, at the time of the creation of the Commentary, the debate of military objectives was "grounded in the reality of 'analog' warfare"[96], and it is not "difficult to believe that the idea of cyber warfare did not cross the minds of the authors"[97]. Additionally, the authors described objects and objectives as tangible to distinguish them from the abstract notion of goals and aims of the parties, thus, it does not seem that they intended to exclude data when they wrote the document[98]. This can be demonstrated by the fact that, in the 1982 Commentary by Bothe and his co-authors, it was observed that "'in the dynamic circumstances of armed conflict, objects which may have been military objectives yesterday may no longer be such today and vice versa'"[99]. Given this, and the fact that "both civilian life and military operations depend to a growing degree on information and activities confined to cyber-space"[100], it is illogical, and inconsistent with its objectives and purpose, exclude data's protection under IHL.

4. CIVILIANS AND COMBATANTS

Article 50 (1) AP defines civilian as "person who does not belong to one of the categories of persons referred to in Article 4 A (1), (2), (3) and (6) of the Third Geneva Convention and in Article 43 of Additional Protocol I"[101]. Moreover, to the ICRC Guidance civilians are "all persons who are neither members of the armed forces of a party to the conflict nor participants in a *levee en masse* and who do not take a direct part

[93] *Ibid*. 78. p. 237.
[94] *Ibid.* 2, p. 490
[95] Macak, 2015 p. 69 *apud* Sir Gerald Fitzmaurice, The Law and Procedure of the International Court of Justice 1951-4: Treaty Interpretation and Other Treaty Points', *British Year Book of International Law*, 1957.
[96] *Ma*cak, 2015 p. 67.
[97] *Ma*cak, 2015 p. 67.
[98] *Ma*cak, 2015
[99] *Ibid.* 98, p. 80 *apud* Bothe *et al*., New rules for victims of armed conflicts: commentary on the two 1977 protocols additional to the Geneva Conventions of 1949, 1982.
[100] *Ibid.* 98, p. 80.
[101] ICRC, 1977, p. 37.

in hostilities"[102]. Considering this, the AP provides that this group shall not be the object of an attack, being generally immune – unless they take direct part in the hostilities[103].

On the other hand, combatants are all members of the armed forces of a Party to a conflict - other than medical personnel and chaplains covered by Article 33 of the Third Convention[104]. The ICRC on Customary IHL, on its turn, states that the armed forced in an international armed conflict are "all organised armed forces, groups and units which are under command responsible to that party for the conduct of its subordinates"[105]. In sum, combatants "are all members of the armed forces of a belligerent party, both regular and irregular forces de facto incorporated, including members of militias and volunteer corps belonging to a party to the conflict as well as *levée en masse*"[106].

The Geneva Conventions have enumerated five conditions which must be satisfied to a person be considered a combatant, and, consequently, a lawful target: (1) being under the command of a person responsible for his or her subordinates; (2) having a fixed distinctive sign recognizable at a distance; (3) carrying arms openly; (4) conducting operations in accordance with the laws and customs of war; and (5) belonging to a party to the conflict. In this sense, the people that conduct operations in cyber units – which some States have incorporated in their armed forces divisions – are, undoubtedly, combatants within the AP[107] once they are part of the regular armed forces of a state. In this regard, some scholars have suggested that incorporating specialized people to the conduction of cyber attacks is a "potential solution to the problem of distinguishing combatants and civilians"[108]. Since, once incorporated, such personnel would be considered as part of the military and, consequently, combatants[109].

Concerning the volunteer corps or militias they would have to meet the criteria of organization to qualify as armed forces - which may be difficult considering the cyber scenario[110]. Regarding the 'belonging to a party to the conflict', this means that it must exist "a *de facto* relationship between an organized armed group and a party to the conflict"[111] or at least a tacit agreement or a conclusive behavior[112]. Especially in the

[102] Melzer, 2009 p. 20-21.
[103] *Ibid. 52.*
[104] ICRC, 1977, p. 32.
[105] Heckaerts & Doswald-beck, p. 14, 2005.
[106] *Ibid. 52, p. 59*
[107] Ibid. 52.
[108] *Ibid. 52, p. 60.*
[109] Doswald-Beck, 2002.
[110] Melzer, 2009.
[111] *Ibid.* 110, p 23.
[112] *Ibid.* 110.

cyber context, the belonging requirement can be challenging to apply, mainly the 'complete dependence'.

Concerning this, the 'complete dependence test' – established by the ICJ in *Genocide* - requires the existence of a "great degree of state control over the persons, groups or entities"[113]. It must be proven, that the people belonging to a party to the conflict are on "'complete dependence' on the state of which they are ultimately merely the instrument"[114]. This sets a "relatively high threshold of control and effectively of combatant status"[115] and its adoption "could risk establishing eventually a very high threshold on combatant status under the law of targeting"[116]. Because only if the attackers are completely dependent on the government, they would qualify as combatants and lawful targets. Thus, it is necessary to "fill the interpretation gap on the necessary degree of control so as to establish a nexus between militias and volunteer groups conducting cyber operations and belligerent parties"[117]. In this regard, Article 4 A (2) enshrines:

> Members of militias and volunteer corps i.e. partisans, organized resistance movements, shall belong to a party to the conflict in order to qualify as a combatant (…) and fulfill the (…) four additional conditions: (a) being under the person's responsible command for his subordinates; (b) have a distinctive sign recognizable at a distance; (c) carry arms openly; and (d) conduct their operations in accordance with the law and customs of war[118].

Concerning the first condition, it reflects the presence of a responsible command and hierarchical relationship. Therefore, if a cyber group does not have sufficient organization, with a typically superior–subordinate structure "its members cannot be lawful combatants"[119]. Thus, independent hackers who wish to engage in the conflict without the belligerent party's authorization are out of this definition. Moving to the second and third requirements, its application is challenging, considering that the attacks performed on computer network are characterized by anonymity, and that it is highly

[113] *Ibid. 52, p. 65.*
[114] *Ibid. 52, p. 65.*
[115] Ibid. 52, p. 65.
[116] *Ibid.* 52, p. 66.
[117] *Ibid.* 52, p. 66.
[118] *Ibid.* 52, p.66.
[119] *Ibid.* 5, p. 347.

unlikely to identify the user of a computer and decide his status[120]. Therefore, it can be argued that these elements "would not be delete outright, but there would be little need for much discussion about them"[121], and some would say that these could even be considered obsolete in this domain.

However, considering the essentiality of the principle of distinction, it has been suggested the establishment of a "class of designated military (…) IP addresses only from which computer networks attacks can be launched"[122]. Thus, "the computer with which a cyber operation is launched will be marked as a designated military IP address"[123]. As an alternative, a computer could also be marked by the "creation of 'universally recognized electronic identifiers' that will recognize the status of persons in compliance with the Geneva Conventions"[124]. Following this reasoning, the ICRC have published a study which proposes solutions to signalize, digitally, the protection of medical infrastructure during armed conflicts[125], and this resource could be used to identify combatants. But some have argued that this proposal is untenable since "marking a military computer is tantamount to making a lawful target of any system to which it is connected"[126]. Others say that armed forces could still wear uniforms to comply with the obligation of having a fixed distinctive sign recognizable at a distance. But this requirement would probably be irrelevant since the parties remain anonymous, once when cyber combatants are in front of their computers, wearing uniforms does not make difference[127]. Also, although technically feasible, this scenario does not seem to be the reality, since the states would probably be against it for tactical reasons. Moreover, "even if states approve such a measure, the belligerent parties will perhaps abuse the identifiers in times of conflicts"[128].

Ultimately, reading the compliance with the laws and customs of war, "it is *a fortiori* the case with respect to cyber warfare, as cyber operations might tempt combatants to violate more often the principle of distinction because of cyber means non-lethal potential"[129]. Notwithstanding, some scholars defend that, on the digital battlefield, this distinction is not necessary, because independent of who committed the attack – either a

---

[120] *Ibid.* 52.
[121] *Ibid.* 5, p. 347.
[122] *Ibid.* 52, p. 69.
[123] *Ibid.* 52, p. 69.
[124] *Ibid*. 52. p.69, *apud* Davis Brown, A Proposal of an International Convention to Regulate the Use of Information Systems in Armed Conflict, 2006.
[125] Iaria, 2023.
[126] *Ibid.* 5, p. 348.
[127] *Ibid 5.*
[128] *Ibid.* 52, p. 69.
[129] *Ibid.* 52, p. 70.

combatant or a civilian directly participating in the hostilities – the person has lost the protected status[130].

4.1. CYBER LEVÉE EN MASSE

This concept arises exclusively in the context of international armed conflicts, comprising inhabitants of a non-occupied territory, who on the approach of the enemy, and without having had time to form into regular armed units, spontaneously take and carry arms openly to resist, respecting the laws and customs of war[131]. Therefore, being considered combatants. Applying to the cyber domain, this concept of spontaneously conducting cyber operations upon the approach of invading forces seems problematic and impractical[132].

In this sense, scholars have found this provision outdated, calling for reconceptualization. Because, if "*levée en masse* is (…) an emergency uprising, a temporary mobilization of the inhabitants of a territory that comes together to defend the nation"[133], a cyber *levée en masse* "is only feasible upon response to a traditional territory invasion by conventional force"[134]. In this scenario this notion seems unworkable, since the 'unoccupied territory' and 'spontaneously take up arms openly' does not conform with the reality of a cyber warfare – given that cyber-attacks are, by nature covert, and geographical limitation is not a factor in the "borderless cyber domain"[135].

The Tallin Manual, recognizing this, chose to keep the concept in its strict sense, requiring the physical invasion of a territory where most of the territory's population, on its own initiative, starts a cyber operation against the invaders. But this position has been criticized by some scholars, who said that this concept is an "unworkable anachronism"[136], recommending its elimination in cyber conflicts and requiring, instead, all assemblages of cyber participants to comply "with the criteria that define militias, volunteer corps or organized resistance movements"[137].

---

[130] *Ibid.* 5.
[131] ICRC, article 4 (6), 1949.
[132] *Ibid.* 52.
[133] *Ibid.* 52, p 72.
[134] *Ibid.* 52, p 72.
[135] *Ibid.* 52, p 72.
[136] Wallace & Reeves, 2013, p. 664.
[137] Wallace & Reeves, 2013, p. 664.

4.2. CIVILIANS TAKING DIRECT PARTICIPATION IN THE HOSTILITIES

As provided in article 51 AP I, civilians are immune from attacks unless they take direct part in hostilities. That is, civilians, when taking direct part in the hostilities, constitute legitimate targets as long as their participation lasts[138]. Meaning that "the loss of protection against direct attack is temporal and lasts from the beginning until the end of participation"[139], which includes the "preparatory acts to the execution of a specific act as well as the timeframe between the deployment to and return from the execution"[140]. In the cyber domain, this participation has been increasing and assuming a relevant position, since cyber operations require specialized knowledge and work, as well as technical expertise - not possessed by the typical military personnel - which leads to the outsourcing of this job to civilian experts[141].

Considering this, except for some cyber units incorporated into the armed forces, most cyber attacks are conducted by civilians[142]. However, since IHL does not provide a definition of the precise meaning of 'direct participation in the hostilities', the ICRC - on its Interpretive Guidance on the Notion of Direct Participation in Hostilities - identified three elements that constitutes 'direct participation', there are: (1) threshold of harm; (2) direct causation; and (3) belligerent nexus.

4.2.1. THRESHOLD OF HARM

Harm is a "a specific act that is likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack"[143]. In this regard, the Guidance recognizes that if harm is reasonably expected to occur its materialization is not necessary, and its objective likelihood is enough[144]. Therefore, the conduction of computer network attacks or transmission of tactical targeting intelligence, for example, if it affects the enemy's military operations or capacity, satisfies the requirement [145].

---

[138] *Ibid.* 52.
[139] *Ibid.* 52, p. 88.
[140] *Ibid.* 52, p. 88.
[141] *Ibid.* 5.
[142] *Ibid.* 52.
[143] *Ibid.* 110, p. 47.
[144] *Ibid.* 52.
[145] *Ibid.* 52.

On the other hand, if there are no physical consequences such as "interruption of electricity, water, food supplies, or the manipulation of computer networks from the required degree of harm"[146], it is disqualified by the Guidance. However, it must be highlighted that this position, in the cyber context, seems contradictory with the one adopted by the ICRC concerning the threshold of attack as defined in Article 49[147]. Because a cyber-attack against vital civilian cyber infrastructure "aimed at their neutralization that resulted in serious malfunction of the computer networks, risking thus the civilian population's public health, would satisfy the required degree of harm"[148] as materialization is not necessary. In addition, considering that the elements of 'direct causation' and 'belligerent nexus' are also satisfied, the civilian that conducted such operation would lose his protection[149]. This approach is more aligned with the inherent interconnectivity of military and civilian infrastructure, once it considers the current "cyber-centric character"[150] of society, in which a considerable degree of harm can be caused even if there are no physical to the civilian infrastructure incapacitation[151].

4.2.2. DIRECT CAUSATION

This element is fulfilled when a direct casual link between the act and resultant harm exists. That is, the harm must result from "that specific act or from a coordinated military operation of which that act constitutes an integral part"[152]. However, the causal link does not have to be an uninterrupted chain of events, and even if the sequence is interrupted, the direct connection between the action and consequences might still be enough[153]. But, according to the Guidance, the result of the harm must be objectively likely, thus only primary consequences are relevant, and indirect effects are not included. In this context, considering that it is doubtful that cyber-attacks could meet this requirement, since its "both intended and unintended consequences (…) are likely to occur over several causal steps"[154], accept this approach leads to the conclusion that civilian engaging in cyber attacks with

[146] *Ibid.* 52.
[147] *Ibid.* 52, p. 81.
[148] *Ibid.* 52, p. 81.
[149] *Ibid.* 52.
[150] *Ibid.* 52, p. 81.
[151] Melzer, 2011.
[152] *Ibid.* 110, p. 51.
[153] *Ibid.* 52.
[154] Turns, 2012, p. 288.

secondary or tertiary harmful effects maintain their civilian status immunity[155]. Also, even if an act, that does not reach required threshold of harm, "constitutes an integral part of a concrete and coordinated tactical operation that directly causes such harm"[156] this requirement is filled.

In general, there are three main categories of civilians engaging in cyber operations: designers or writers of malicious programs; operators (operating the computer programs in the cyber warfare); and webmasters (acting as service administrators, assistants and maintainers)[157]. In this regard, if a civilian provides maintenance to the information system used to conduct attacks, there is no direct link between its work and the eventual harm caused by the attacks. So, the person could qualify as "accompanying the armed forces, being thus immune from attack"[158]. But, if a person is specifically recruited and trained to carry out certain acts, then these activities constitute an integral part of this act and is equivalent to direct participation[159].

Moreover, regarding designers and developers, the Guidance considers experts and scientists generally protected, except in extreme situations where the expertise of a particular civilian is very exceptional and of "decisive value for the outcome of an armed conflict"[160]. Therefore, in the cyber conflicts, where IT experts "provide the exceptional expertise needed for the harm to occur, being thus the *condicio sine qua non* of the outcome"[161], their contribution corresponds to direct participation, and they lose their protection. In sum, writing a malicious program can qualify a person as a direct harmer, "despite the separation in time between the act and the harm caused"[162]. Furthermore, concerning the operators, if an operation consists in the execution of the attack, there is clearly a direct causation.

4.2.3. BELLIGERENT NEXUS

It refers to the objective purpose for which a specific act is designed. Thus, an act should be closely linked to the hostilities and aim to "directly cause the required

[155] *Ibid.* 52.
[156] *Ibid.* 52, p. 85-86.
[157] *Ibid.* 52.
[158] *Ibid.* 52, p. 84.
[159] *Ibid.* 52.
[160] *Ibid.* 110, p. 53, footnote 122.
[161] *Ibid.* 52, p. 83.
[162] *Ibid.* 52, p. 84-85.

threshold of harm in support of a party to the conflict and to the detriment of another"[163]. It is important to note that it is necessary to distinguish the objective purpose from the subjective intent, considering that the former is an element of the act's objective created directly to inflict harm. Thus, the civilians who are forced to participate in hostilities still lose their protected status - except those who are not aware of their involvement because they were instrumentalized by a part[164]. In the cyber domain, when a robot network is specifically elaborated to distribute DDoS attacks by a "civilian computers that might result in violent physical consequences and cause harm"[165], and the equipment owners is unaware of its existence and purpose, we consider that the person is a civilian and any attack against it must take into account the proportionality assessment[166].

In sum, although the cumulative application of these requirements constitutes a relatively high threshold for reaching the notion of direct participation[167], "there is no exhaustive list of examples of direct participation"[168]. Therefore, considering the absence of international jurisprudence on this, it is left to scholars, and States practice its clarification[169]. Finally, relative to the temporal loss of the protection of the civilian taking direct participation in the hostilities, although it is accepted that the period of time between the deployment to and return from the execution are integral part of that act - thus being included in the time period of the loss of the protected status - questions arise when it comes to the "'execution' of cyber attacks with long-delayed effects"[170]. To the Tallinn Experts, the duration period starts with emplacement of the bomb and lasts until its activation by an individual's command, "regardless the time of the effects or damage occurrence"[171].

However, some scholars believe that a more restrictive approach should be preferred, focusing on the act and not on its effects. Because "a civilian who is responsible for the installation of a malware that is due to activate in the next couple of months is no longer

[163] *Ibid.* 110, p. 58.
[164] *Ibid.* 52.
[165] *Ibid.* 52, p. 87.
[166] *Ibid.* 52.
[167] Turns, 2012.
[168] *Ibid*. 52, p. 87.
[169] *Ibid.* 52.
[170] *Ibid.* 52, p. 89.
[171] *Ibid.* 52, p. 89.

posing any military threat by the time of the malware's activation"[172] and the opposite of this does not comply with the law. Since "it treats the civilian as a military objective targetable at all times, even when he completely detaches or disengages himself from the hostilities"[173]. On the other hand, this gaps between 'non-protection' moments, allows the engagement in many attacks while benefits with a certain immunity, since once he returns home, "he regains the full immunity from attack that civilians enjoy (...) until such time as he deploys again to directly participate in hostilities"[174], creating "an imbalance between the direct participant and the member of the regular armed forces, since the latter is open to attack at any time"[175]. Specially in the cyber domain, the restrictive interpretation would mean that the participant only can be attacked when launching the operation[176] – which is problematic, since cyber operations can last just for some minutes or seconds, and this requirement would "effectively extinguish the right to strike at direct participants"[177].

In this regard, Michal N. Schmitt proposed the understanding that "the only reasonable interpretation of 'for such time as' is that it encompasses the entire period during the cyber participant engaging in repeated cyber operations"[178]. But this opposes to the ICRC Guidance's comprehension that treats each act separately. A definitive answer to this requirement does not seem to exist and depends on multiple constantly changing situational factors, that shall be treated with great care[179]. Because, although "target acquisition cyber operations are accepted as forming an integral part of specific cyber attacks"[180], if the participation is limited to the preparation of the target acquisition, he is no longer targetable once the act has been completed. Therefore, it is possible that individuals will only participate in the preparation, whose targeting will be impossible, unless they get attacked while preparing[181]. Thus, a case-by-case analysis and answer is needed "for whether a specific preparatory measure forms an integral part of a specific act or not"[182].

---

[172] *Ibid.* 52, p. 89.
[173] *Ibid.* 52, p. 89
[174] Schmitt, 2011, p 102.
[175] Schmitt, 2011, p 102.
[176] Schmitt, 2011.
[177] *Ibid.* 176, p. 102.
[178] *Ibid.* 176, p. 102.
[179] *Ibid.* 52
[180] *Ibid.* 52, p. 90.
[181] *Ibid.* 52
[182] *Ibid.* 52, p. 90.

Within this context, although the theory regarding the application of the principle of distinction is relatively settled, several questions arise concerning its practical application. Therefore, the fifth chapter will expose the example of the IT Army of Ukraine, intending to explore the challenges emerging from the application of this principle in cyber warfare.

5. IT ARMY OF UKRAINE

Since the beginning of the Ukraine-Russia conflict, the cyber warfare has played a significant and increasingly role. Before February 2022, Russian governmental actors "have allegedly been involved in several hostile cyber operations against Ukrainian governmental, military, and civilian infrastructures"[183]. Moreover, cyber-sabotage' against civilian infrastructure has also occurred. In 2015 and 2016 "parts of the Ukrainian power grid were shut down by (…) malwares"[184], affecting thousands of citizens. And, after the invasion in February 2022, Russia's alleged involvement with cyber operations has remained constant[185].

To counter, in a certain way, these attacks, a growing number of cyber operations have been launched, since February 2022, by non-state actors to support Ukraine[186]. In this context, the IT Army of Ukraine (IT Army) emerged from a meeting between a Ukrainian entrepreneur and the Ukrainian Minister of Digital Transformation, in which was discussed the creation of a volunteer IT Corp to defend Ukraine's digital infrastructure. As a result, on 26 February 2022, by a Tweet of Minister calling "for IT specialists to help Ukraine"[187], thousands of volunteers joined. The IT Army, that uses social media to communicate, coordinate and report actions, it is considered the first in the world to be created by an official open announcement from a state calling "on hackers (…) to join a nation's military defensive efforts"[188].

In the beginning, "there was no system for prioritizing targets or attack vectors"[189], and the main structure consisted in a social media channel in which were disseminated IP addresses, domain names and port numbers. Over time, a "dynamically updated list of targets was released"[190], but "the coordination between members has been

[183] Biggio, 2024, p. 145.
[184] Biggio, 2024, p. 145
[185] Biggio, 2024.
[186] *Ibid.* 185.
[187] *Ibid,* 185, p. 47.
[188] *Ukraine's IT army is a world first: here's why it is an important part of the war*, University of Portsmouth, 2023.
[189] Done, 2023, p. 17.
[190] Done, 2023, p. 17.

questionable"[191]. Despite this, the group has claimed responsibility for many cyber operations, and it is estimated that around 2,000 attacks were launched between February and June 2022[192]. One of the most significant targeted Russia's authentication system, causing a "widespread disruption with serious economic costs"[193]. Moreover, the group also targeted Russian radio and TV stations, adding "snippets of videos about the war in Ukraine to programmes, and to broadcast fake air raid alerts"[194]. Besides that, the IT Army directed operations against the Moscow Stock Exchange and a Russian bank [195]. However, their "potent force is controversial"[196], since there are critics accusing the group to target civilian entities such as food delivery services[197].

Considering this, important discussions about the role of cyberwarfare in real-life military operations have emerged, mainly whether "the IT army could be considered combatants, rather than civilians"[198] - since it affects the protection conferred by international law and, consequently, their status as legal targets, or not. In this regard, the ICRC has expressed concern to the recruitment of civilian volunteers, once "even though not every form of civilian involvement on the digital battlefield qualifies as direct participation, the danger is that it may be seen as such (…) thus exposing numerous civilians to a grave risk of harm"[199].

In this sense, and as suggested by one the participants in September 2022, the hybrid structure of the Army was composed by "around 25-30 'Generals' from the Ukrainian Secret Service and other ministries (…) and high level hackers"[200]. In sum, the group is a "state-sponsored, volunteer offensive operations force comprised of civilians using personal computer equipment"[201], subordinated to the "Ukraine's Ministry of Digital Transformation and not to the armed forces"[202], but it is not clear the operational command legally possessed by this organ. In this context, although called by the government, the members took part of it voluntarily and autonomously, and whilst they

[191] Done, 2023, p. 17.
[192] Kirichenko, 2023.
[193] *Ibid.* 188.
[194] *Ibid.* 188.
[195] *Ibid.* 185.
[196] *Ibid.* 192.
[197] *Ibid.* 192
[198] *Ibid.* 188.
[199] Biggerstaff, 2023.
[200] Render-Katolik, 2023.
[201] Done, 2023, p. 16.
[202] Done, 2023, p. 18.

do make a strategic contribution to the defense, they "are not combatants in the traditional sense"[203].

Following this reasoning, a legal gray area is created by their independence from the Ukrainian government, especially regarding the foreign volunteers[204]. This situation led the Ukrainian government, in April 2023, to draft a law to formally recognize the status of the IT Army and its participants - intending to officially integrate them in the Armed Forces[205]. However, it has not passed so far. Moreover, besides them, other hacktivist groups have been formed, raising questions regarding their status[206]. Therefore, it is crucial to understand the status of these individuals and groups within IHL.

5.1. IT ARMY LEGAL STATUS

Currently, it is a little difficult to find that IT Army members are civilians[207]. However, considering the definition of combatant laid in article 43 AP I, members must be part of the armed forces or other militias or volunteer corps belonging to a party in the conflict to be considered as combatants. That is, they must be incorporated into the armed forces by being enlisted or through a similar procedure - which the volunteers of the IT Army are lacking. Additionally, the group that the person belongs must fulfill certain conditions. In this regard, as a decentralized internet-based group, the IT Army appears to lack an organized hierarchical structure, and a commander capable of enforcing a disciplinary system. Thus their members are, at least for now, civilians[208]. However, this does not mean that they benefit from the protection conferred by IHL, once civilians only lose their protection for such time as they directly participate[209]. So, it is crucial to differentiate the civilians acting individually, or on an unorganized basis, from the ones that are part of OAG.

In this context, according to the Tallinn Manual's rule 83, a group is considered armed if it capable of undertaking cyber-attacks, it is under an established command structure and can conduct sustained military operations[210]. Additionally, the organization "does not have to reach the level of a typical military disciplined unit, but "small groups of hackers

[203] *Ibid.* 192.
[204] *Ibid.* 192.
[205] *Ibid.* 192.
[206] *Ibid.* 192.
[207] *Ibid.* 199.
[208] *Ibid.* 199.
[209] ICRC, 1977.
[210] Schmitt, 2017.

are unlikely to meet this requirement[211]. Considering this, and the descriptions that define the group as "'decentralized', 'loosely corralled' amalgam of 'vigilantes,' many of whom only associate over the Internet"[212], there is less certainty of its sufficient organization and, without more information regarding its structure and organization, it is difficult to conclude that they are an OAG[213]. Nevertheless, according to the ICRC Interpretive Guidance on the Notion of Direct Participation in Hostilities, persons not in continuous combat function are only targetable when directly participating. Therefore, based on its constitutive elements, and the scale and range of their activities, only IT Army's specific conducts that satisfy all the three elements can be considered as direct participation[214].

Regarding the threshold of harm, even if the cyber operation engaged by a member of the IT Army does not qualify as a cyber-attack, but adversely "affect the military operations or military capacity of a party to an armed conflict or (…) inflict death, injury, or destruction on persons or objects protected against direct attack"[215], crosses the threshold of harm. Concerning direct causation, generally in the cyber context actions that adversely affect the war effort are not sufficient, but "operations that result in or directly enable the impairment of military networks, equipment, functions, or capabilities likely qualify"[216]. However, considering that "many of the operations publicly attributed to the IT Army (…) have temporarily disabled or defaced Russian websites that have little, if any, connection to the Russian war effort"[217], they do not seem acts of direct participation. In addition, some acts, which are likely to affect negatively the military operations conducted by Russian, are greatly attenuated, being more accurately related with Russian's overall war effort. Since they are 'indirect' and focused on provoking economic damaged intending to weaken Russia's ability to "wage war against Ukraine"[218].

Finally, concerning the last element, considering the group's "impetus and stated purpose, and the fact that its targets are provided by Ukrainian officials, there is little question that many, if not all, of its cyber operations satisfy this element"[219]. According to the ICTY on Dario Kordic and Mario Cerkez judgments, direct participation means "to engage in acts of war that by their nature or purpose are intended to cause harm to the

[211] *Ibid.* 210.
[212] *Ibid.* 199.
[213] *Ibid.* 199.
[214] *Ibid.* 199.
[215] *Ibid.* 199.
[216] *Ibid.* 199.
[217] *Ibid.* 199.
[218] *Ibid.* 199.
[219] *Ibid.* 199.

personnel or equipment of the adverse party"[220]. In this context, "the Ukrainian government's call to arms has highlighted the uncertainty that exists regarding the status of civilian hackers who engage in international armed conflicts"[221], and the direct participation standard is "somewhat unclear as applied to these hacktivists"[222]. Because, considering the concept presented by Guidance, the three criteria will doubtfully be met for the IT Army - at least for the majority of the group's acts. Since their form of making websites inaccessible or accessing private information are not, by itself, strongly likely to affect the adversary's military operations or capacity, nor bring 'death, injury, or destruction' on civilians. Even if the websites or data are military, the temporary nature of the attacks do not constitute an independent threat"[223].

Therefore, once "the threshold of harm will likely not be met, the belligerent nexus requirement also cannot be sustained"[224]. Under this, the IT Army members are likely to keep their civilian status, unless they are found to be directly participating in hostilities at some point. But, considering the volume and range of the operations conducted by the group, "it is likely that at least some of the IT Army's activities satisfy"[225] all of them. In this regard, "there is widespread agreement that Russian forces may target an IT Army member engaged in a cyber operation at his or her computer or while 'travelling to and from the location where a computer used to mount an operation is based'"[226]. However, once direct participation ceases, those cannot be lawfully targeted.

On the other hand, The US Commander's Handbook on the Law of Land Warfare provides a 'factor-based interpretation', in which direct participation "extends beyond merely engaging in combat, including certain acts that are an integral part of combat operations or that effectively and substantially contribute to an adversary's ability to conduct or sustain combat operations"[227]. In this comprehension, when determining if a civilian is a direct participant, it is considered the degree to which the act causes harm to the opposing party[228], such as "whether the act is the proximate or 'but for' cause of death, injury, or damage to persons or objects belonging to the opposing party"[229]; "the degree

[220] Stubblefield, 2024, p. 232.
[221] Stubblefield, 2024, p. 232.
[222] Stubblefield, 2024, p. 233.
[223] Stubblefield, 2024, p. 233.
[224] Stubblefield, 2024, p. 233.
[225] *Ibid.* 199.
[226] *Ibid.* 199.
[227] US Department of the Army, p. 2-2.
[228] US Department of the Army.
[229] *Ibid.* 228, p. 2-3.

to which the act is temporally or geographically near the fighting; or the degree to which the act is connected to military operations"[230]; "whether the activity is intended to advance the interests of one party to the conflict to the detriment of the opposing party"[231]; and "the degree to which the act contributes to a party's military action against the opposing party"[232]. Therefore, DDoS attacks by the IT Army "that primarily target websites or leak data are generally not a but-for cause of injury or damage to an adversary's property"[233]. Because these attacks, when directed to websites, reach the 'threshold of harm' to cause a sufficient impact on military capacity or operations as required by the Handbook. Factors such as geographic proximity - of the place where the cyber activity originates - and the intent to advance one party's military interests to the detriment of the other, can indicate 'direct participation'. But most of the facts "weigh against the (…) DDoS attacks by hackers being considered direct participation"[234]. In sum, within the different comprehensions of direct participation, nothing seems to indicate that "IT Army members carrying out basic DDoS attacks are directly participating"[235].

Nevertheless, this classification could change if the goals of the hackers alter, since the Handbook enshrines that the act of providing or relaying information of immediate use in combat operations constitutes direct participation. Therefore, if the hackers engage in "acts of intelligence gathering (…) during a concrete and coordinated military operation"[236], such as accessing "personal devices or accounts of top military commanders to learn sensitive information such as location of weapons or troops"[237], their direct participation becomes clear. Because "becomes more likely that the hacking is a but-for cause of injury or damage to the adversary"[238], once "intelligence gathering is traditionally done alongside military operations and thus is more likely to adversely affect (...) the opposing party"[239].

In addition, if the hackers engaged in a more damaging way, interfering in the military operations, they would be undoubtedly close to direct participation, as for example, the case of hacking the Russian highway system installing trains that carried Russian soldiers

[230] *Ibid.* 228, p. 2-3.
[231] *Ibid.* 228, p. 2-3.
[232] *Ibid.* 228, p. 2-3.
[233] Stubblefield, 2024, p. 235.
[234] Stubblefield, 2024, p. 235-236.
[235] Stubblefield, 2024, p. 236.
[236] Fleck, 2007, p, 689.
[237] Stubblefield, 2024, p. 236.
[238] Stubblefield, 2024, p. 236.
[239] Stubblefield, 2024, p. 236.

– which the IT army allegedly has done[240]. This kind of act "is more likely to reach a sufficient threshold of harm than website interference"[241]. In this sense "when paired with a more direct causal link between the hackers action and an act that is intended to cause actual harm to the adverse party, an act by the IT army could reach a belligerent Nexus which creates direct participation"[242]. Therefore, when engaging in activities with the threshold of harm, the hackers would, during their direct participation, be lawful targets.

Following this reasoning, finding when exactly they are directly participants "requires a unique analysis for cyberattacks, and the outcome will impact the length of time a military may permissibly target them"[243]. Moreover, if direct participation is only considered when the hackers are at their devices actively provoking negative consequences, there is an "advantage over lawful combatants"[244]. Since, while these can be attacked at any moment, those gain protection when they cease their direct participation[245]. This being the case, although targeting them individually "may be impractical from a military perspective, it presents opportunities for belligerent countries to target hackers (…) under a pretense of legitimacy"[246]. Ultimately, if the hackers repeatedly engage in attacks that reach the threshold of harm, it is likely that they will lose their status and protection as civilians under the 'revolving door' theory[247].

Furthermore, "if direct participation is defined as any time the ripple effect of the hacker's actions is being felt, even when the hackers are no longer actively taking steps to cause the attack, this opens the doors for more counterattack and (…) civilian casualties"[248]. In this scenario, although it could be argued that is unlikely that a hacktivist would launch a cyberattack large enough to allow their targeting, in a crowded area, under the principle of proportionality, it application, in practice, "is a difficult and imprecise science, and states may take advantage of any possible diversification during war to attack, even if they are applying principles improperly"[249]. Additionally, despite the existence of the limiting principles, when hackers participate in hostilities "civilian casualties increase concurrently"[250] due to the lack of accurate military intelligence.

---

[240] Stubblefield, 2024.
[241] *Ibid.* 240, p. 237.
[242] *Ibid.* 240, p. 237.
[243] *Ibid.* 240, p. 237.
[244] Reeves & Powell, 2021, p 181.
[245] Reeves & Powell, 2021.
[246] *Ibid.* 240, p. 239.
[247] *Ibid.* 240.
[248] *Ibid.* 240, p. 239.
[249] *Ibid.* 240, p. 239.
[250] *Ibid.* 240, p. 239.

5.1.1. IT ARMY AS NON-STATE ACTOR

While the IT army might not be classified as direct participants, they are different from independent hacktivists[251]. Since, although the Ukrainian government argues that "it does not 'formally employ' these hacktivists, the role of a member of the IT army is more akin to that of a volunteer militia soldier then an independent hacktivist"[252]. Moreover, the "IT Army members voluntarily joined an organization that, while clarity is still needed on its exact characteristics, has assignments, training, and the sole goal of interfering in another state's affairs"[253]. Therefore, it has more similarities to the structure and purpose of a volunteer militia, while it is different from a single hacktivist or a collective - considering that "non-state armed group members are open to attack at any point, regardless of the nature of the activities they are engaged"[254].

In this context, even if the IT Army members do not fit in the conventional comprehension of 'combatants' and does not fulfill the requirements of being a volunteer corps with a clear leader and distinctive sign, it shares similarities with other non-state armed groups[255]. Considering that, despite the absence of a formal definition in international law, ICTY in *Prosecutor v. Haradinaj* and Article 1 (1) AP II characterize non-stated armed groups by the existence of a responsible command, which exercise control over a territory, and it is "enable to carry out sustained and concerted military operations and to implement this protocol"[256]. It should be noted that, even if there is not a clear hierarchical command structure, a group can still satisfy this element, as in *Haradinaj*, where the existence of checkpoints leading to territorial control were considered as a form of 'hierarchical command structure'. In addition, this case added two additional elements that characterize a non-state armed group: "the ability to gain access to weapons, training or recruits; and the ability to engage in agreements with a unified voice"[257].

Furthermore, the Manual on Humanitarian Negotiations with Armed Groups by OCHA defines non-state armed groups as groups that:

---

[251] *Ibid.* 240.
[252] *Ibid.* 240, p. 240.
[253] *Ibid.* 240, p. 240.
[254] *Ibid.* 240, p. 240.
[255] *Ibid*. 240.
[256] ICRC, art. 1(1), 1977.
[257] *Ibid.* 240, p. 241.

> Have the potential to employ arms in the use of force to achieve political, ideological or economic objectives; are not within the formal military structures of states, state-alliances or intergovernmental organizations; and are not under the control of the state(s) in which they operate[258].

In *Tadic*, the ICTY Appeals Chamber recognized additional characteristics, clarifying that such groups "will be under the control of a state if the state to which the group's acts will be attributed has a role in training, financing, organizing, or coordinating the military actions of the group"[259]. In this context, some could argue that, since the IT Army is not literally armed, the classification of non-stated armed group could not be applied. However, "this nomenclature is likely because the law of war was codified at a time when its primary tools were physical weapons"[260]. Moreover, international community has already confirmed that, even if the language is outdated, the laws of war are applied to cyberwarfare, and the ICTY made clear that it is possible to expand the application of its criteria[261]. In addition, this may be "difficult to apply if IT Army members are based in Ukraine, given that there is a clear link between the Ukrainian government and the formation of the IT Army"[262]. Therefore, although additional information on the Ukrainian's government degree of involvement is needed, only providing the list of targets - without coordinating, offering operational support, training, or equipping – it unlikely to meet the standard "to formally attribute an armed group's actions to a state"[263].

Nevertheless, the other characteristics of the IT Army, such as the fact that it is not part of the Ukrainian formal military structure; it has a unified voice to promote and work toward their common political goal; its organization with both public and private parts; and the sufficient command structure to plan new recruits train besides and provide targets, leads them to a classification as a non-stated armed group[264]. Additionally, although they do not have a "publicized command structure, the *Haradinaj* judgment found that the absence of a rigid hierarchical structure was not

[258] Mc Hugh, & Bessler, 2005, p. 6.
[259] *Ibid.* 240, p. 241.
[260] *Ibid.* 240, p. 241.
[261] *Ibid.* 240.
[262] *Ibid.* 240, p. 242.
[263] *Ibid.* 240, p. 242.
[264] *Ibid.* 240.

fatal"[265]. Lastly, the group is clearly capable of participating in agreements and apply IHL - as demonstrated by their compliance with the ICRC Rules of Engagement for civilian hackers[266]. And "the carrying out of military-like operations by even a few members of the group, as seen in actions like derailing trains used to carry soldiers, is sufficient to cloak all members with such actions"[267]. Therefore, and considering that "that the attacks are parallel to a broader war effort, they are also more likely to be considered military-like, particularly given their frequency and responsiveness to attacks"[268].

In sum, although this categorization may not be perfect, "takes into account the expectation of being on notice of retaliation that comes with joining an organized group with the goal of interfering with another state's sovereignty"[269]. In this sense "there is enough overlap to find it possible that members of the IT Army could be considered members of a non-state armed group, thus making them combatants and legitimate targets at any point"[270]. Finally, it must be referred that considering the IT Army as a non-state armed group and as lawful targets can be dangerous - since it can harm neutral countries, as with its members operating in neutral states around the world, Russia could argue that states are permitting acts of war to be committed by combatants in their territory[271]. Therefore, it could "use this as a justification for the use of force against neutral states under the exception of self-defense"[272].

Moreover, as a non-state armed group, the IT Army does not have a legal connection with Ukraine, which enables the latter to distance itself and avoid the responsibility that may arise from the members unlawful acts under international law[273]. This can create a "precedent" to other states outsource their operations intending to escape from the responsibility that being a party to the conflict implies. Given this, it is crucial to comprehend how responsibility is attributable to States in the cyber domain, mainly when actions of non-state actors are at stake, to prevent states refraining from the obligations for breaches of international law.

---

[265] *Ibid.* 240, p. 242.
[266] *Ibid.* 240.
[267] *Ibid.* 240, p. 242.
[268] *Ibid.* 240, p. 243..
[269] *Ibid.* 240, p. 243.
[270] *Ibid.* 240, p. 243.
[271] *Ibid.* 240.
[272] *Ibid.* 240, p. 246.
[273] *Ibid.* 240.

6. STATE RESPONSABILITY AND NON-STATE ACTORS IN THE CYBER DOMAIN

Originally, state responsibility was conceived as a set "rules governing States' international obligations in their relations with other States"[274], constituting, "a classic way of dealing with violations of customary international law"[275]. Thus, it can be said that the responsibility of states is a corollary of the international juridical order, contributing to its affirmation[276]. The idea was that "a State's primary obligation is to pay compensation or make reparation for injuries suffered by nationals of other States"[277]. As was held in *Factory at Chorzów*, state responsibility "is a principle of international law, and (…) any breach of an engagement involves an obligation to make reparation"[278].

In this context, the RSIWA "was built on the basic that every internationally wrongful act of a state entails the international responsibility of that state"[279], and requires three elements to be met: (1) a conduct attributable to a state under international law; (2) which constitutes a breach of an international obligation incumbent to the latter; and (3) which the wrongfulness cannot be excluded by the circumstances[280]. Concerning this, international responsibility originates from the commitment of an international illicit fact, which is composed by two elements: the conduct (act or omission attributable to a state) and the illicitness – behavior that constitutes a violation of an international law rule[281]. In this regard, considering that attribution means "the operation of attaching a given act or omission to a state"[282], and that to this purpose the articles rely on the relation between an individual or group with a state, "the issue of attribution is reduced to identifying the persons, groups or entities that should be considered to act on behalf of the state"[283].

In this regard, as article 4 provides that, for the purpose of international responsibility, the conduct of any State organ is considered as acts of the State[284]. However, as enshrines article 8, when a person or group – which is not state agent or organs, or an entity authorized to exercise prerogatives of public authority by the State - act under the instructions, direction or control of a certain State, their actions will be imputable to the

[274] Sucharitkul, 1996, p. 823.
[275] Sucharitkul, 1996, p. 823.
[276] Lopes *et al*., 2020.
[277] Sucharitkul, 1996, p. 823.
[278] Antonopoulos, 2021, p. 115.
[279] Pacholska, 2023, p. 160.
[280] Pacholska, 2023.
[281] Sucharitkul, 1996, p. 823.
[282] Antonopoulos, 2021, p. 116.
[283] Antonopoulos, 2021, p. 116.
[284] ILC, 2001.

it[285]. Therefore, a State is held accountable for acts or omissions committed by: *de jure* State organs; and *de facto* state organs - "non-state actors or entities that have been 'elevated' to *de facto* state agents or organs because they are under absolute dependence or control of a state"[286]. To this purpose, in *Nicaragua v. US*, the ICJ ruled that to a State to be considered as accountable for the acts of a non-state actor, their relation should be characterized by the control, on one side, and dependence on the other[287]. That is, the State should be controlling the group, providing specific instructions to it, and the latter should depend on the State[288].

However, international jurisprudence has not been linear when interpreting these concepts[289]. The ICTY, in *Tadic*, considered that the existence of specific instructions or directives are not necessary to a 'total control' be verified[290]. Instead, held that the proof of financial, logistics or any other type of support was enough, as well as direction, coordination and global supervision of the activities[291]. Lastly, the ICJ in *Genocide*, stated that the acts of the people under instructions of the State would not be attributable to the latter, only the actions of these organs themselves[292]. Thus, the responsibility is due to the commands given or control exercised, not because of the behavior of those who have been instructed or controlled[293]. Nonetheless, this interpretation is criticizable because it deviates from the general framework of the liability system and does not fit the letter of article 8 - which aims to hold the state responsible for the conduct of private individuals who act under its instructions or control, in a way that is equivalent to a state organ[294].

Furthermore, for the purposes of international responsibility, intention and guilt are irrelevant, and whenever a state does not comply with the legal requirements, unlawfulness is verified[295]. In this context, considering that every breach presupposes attribution, "identifying the source of harm is crucial for the allocation of legal consequences"[296]. Since, "when a transgressor can be identified, penalties can be

[285] *Ibid.* 276.
[286] Antonopoulos, 2021, p. 116-117.
[287] *Ibid.* 276.
[288] *Ibid.* 276.
[289] Lopes *et al*., 2019.
[290] *Ibid.* 276.
[291] *Ibid.* 276.
[292] *Ibid.* 276.
[293] *Ibid.* 276.
[294] *Ibid.* 276.
[295] *Ibid.* 276.
[296] Margulies, 2013, p. 503.

assessed, and retaliation and deterrence are possible"[297]. However, considering the development of new technologies as well as the contemporary tendency of outsourcing activities involving the exercise of public power[298] - namely the trend in armed forces to outsource specialized work[299] - new concerns and issues are arising regarding the attribution of state responsibility in the cyber domain. Because, if, on one hand, it is accepted that actions in cyberspace can constitute a breach of international law - giving rise to international responsibility[300] - on the other, there are still doubts regarding law's application and interpretation in this domain.

In this context, due to technical difficulty in identifying the actual source of the attack, the attribution of legal responsibility is more challenging[301]. Once, in opposition to kinetic attacks, states forces do not "typically distinguish their weapons and personnel with clearly markings"[302]. On the contrary, the parties involved precisely take advantage of the anonymity provided by it. Also, depending on the States' objective, "attribution of malicious cyber activity can trace to machine, to one or more persons operating the machine (…) and to a person or entity that is found to be ultimately responsible for that activity"[303]. Moreover, although "a recipient or a third party investigating a cyber attack may be able to discern the owner of a particular computer (…) a sophisticated sender can readily make this information far less useful for identifying the source"[304].

Additionally, in the often multistage attacks, "the attacker will commandeer one computer with code that converts that computer into a platform for attacking a second computer"[305], so "senders can 'spoof' other IP addresses so that a computer that originally sent the message is disguised as another machine"[306]. Besides the "identification of the machines that launched the attack"[307], it also must be identified the person who did it, and in this case, "even if we have resolved the difficult technical question of forensic attribution, we must then consider the legal question of when an attack traced to a particular source within a state can be attributed to the state itself"[308]. Because a sender

[297] Margulies, 2013, p. 503.
[298] *Ibid.* 276.
[299] *Ibid.* 5.
[300] Antonopoulos, 2021.
[301] Margulies, 2013.
[302] *Ibid.* 301, p. 503.
[303] Banks, 2017, p. 1503.
[304] *Ibid.* 301, p. 503.
[305] *Ibid.* 301, p. 503.
[306] *Ibid.* 301, p. 503.
[307] Shackelford & Andres, 2011, p. 985.
[308] *Ibid.* 301, p. 504.

may be located in a country, but may act on behalf of another and "route a malicious packet through servers in country Y in the course of attacking country Z"[309].

In this sense, the former Assistant Attorney General for the US National Security Division affirmed:

> Attributing activity on the Internet is challenging. Hackers often route their malicious traffic through third-party proxies they either rent or compromise. An attacker in Eastern Europe that uses a botnet of compromised computers in the Middle East to conduct a DDoS attack against a U.S. target creates a false narrative that actors located in the Middle East were responsible for that act[310].

Thus, he continues, "even attributing an attack to the actual originating computer may be insufficient; we may know the machine used to execute a hack, but not the person or group that controlled it"[311]. Moreover, in this context, the National Academies of Science stated that:

> It may be difficult even to know when a cyberattack has begun, who the attacker is, and what the purpose and effects of the cyberattack are/were. Indeed, it may be difficult to identify even the nature of the involved party (…) Knowing the nature of the party is an important element in determining the appropriate response. And, of course, knowing which country, terrorist group, or individual is in fact responsible is essential if any specific response involving attack is deemed appropriate[312].

In this regard, William Banks argues that States should make some "tradeoffs between secrecy and transparency, and publicly identify some public-infrastructure 'red lines' and attribution benchmarks that can help States create an international roadmap for deterrence of harmful cyber intrusions in the future"[313]. Considering this, and the fact that "legal attribution is vital for international law, which governs state responsibility for harm

[309] *Ibid.* 301, p. 504.
[310] Banks, 2017.
[311] *Ibid.* 310, p. 1493.
[312] *Ibid.* 310, p. 1493..
[313] *Ibid.* 310, p. 1493.

to other states"[314], "determining an appropriate standard for attribution is critical (…) in building a functioning regime of international cyber law"[315]. Following this reasoning, "most scholars and states agree that international law governs state responsibility in cyber domain"[316]. In this context, the Tallinn Manual rule 15, which provides that "cyber operations conducted by organs of a State, or by persons or entities empowered by domestic law to exercise elements of governmental authority, are attributable to the State"[317], is aligned with the narrow interpretation of state responsibility adopted in international law. Given this, it is accepted that "states are responsible for cyber-related acts of their own officials, agents, contractors, non-State actors, and other States to the extent they actually control the operations"[318].

However, for actions taken by a private group to be attributed to a State, it must be demonstrated the "existence of a real link between the (…) group performing the act and the State machinery". Following this reasoning, Article 8 RSIWA, as referred, provides that a "conduct of a person or entity is attributable to the state when a 'group (…) is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct'"[319]. Moreover, the Tallinn Manual rule 17 states that "cyber operations conducted by a non-State actor are attributable to a State when: (a) engaged in pursuant to its instructions or under its direction or control; or (b) the State acknowledges and adopts the operations as its own"[320]. That is, groups or individuals carrying out operations under the control of a state. But this criteria requires "more than mere endorsement or tacit approval of the non-State actor's cyber operations"[321].

Within this context, if "attribution in cyberspace is still fraught with evidentiary difficulties"[322], an additional challenge is the attribution to a state of acts practiced by private or non-state groups. Because as provides Tallin Manual 2.0, international law requires a granular analysis, considering "the reliability, quantum, directness, nature (…) and specificity of the relevant available information"[323]. Therefore, comprehending Article 8 provisions is essential to establish the State responsibility for certain acts.

---

[314] *Ibid.* 301, p. 504.
[315] Shackelford & Andres, 2011, p.984.
[316] *Ibid.* 301, p. 505.
[317] *Done*, 2023, p. 344.
[318] *Ibid.* 310, p. 1496.
[319] *Ibid.* 300, p. 117.
[320] *Ibid. 210*, p. 94.
[321] *Ibid. 210*, p. 99.
[322] Macak, 2016, p. 410.
[323] *Ibid. 210*, p. 81-82.

In this scenario, the ILC commentaries identified three autonomous criteria in article 8: (1) instruction; (2) direction; (3) control, thus being sufficient the establishment of any one of them to characterize the act as attributable to the state[324].

6.1. INSTRUCTION

The state must instruct the non-state actor, demanding it to engage in the conduct[325]. That is, the State instructs an actor, outside of its official structure, to engage in a certain act on its behalf. For example, if the government specifically instructs "an IT department within a university to carry out a Distributed Denial of Service (…) attack against a designated target"[326], "the resulting operation would be attributable to the State in question"[327]. In this context, the submission of the non-state actor before the state can be characterized by mere acceptance on the instructions and acting accordingly[328]. As stated by the ICJ in *Genocide*, "the instructions must be given specifically 'in respect of each operation in which the alleged violations occurred'"[329].

Thus, the act of encouraging "unspecified 'patriotic' hackers to engage in offensive action would not suffice for the purposes of attribution"[330]. That is, the State encouragement in relation to a non-state actor to "undertake a malicious cyber intrusion is not sufficient for State responsibility"[331]. Also, although having common objectives indicates political alignment, without further evidence, it is not sufficient to establish a relation of subordination[332]. Lastly, "the resulting act must be traceable in its material components back to the instructing State"[333], meaning that the instructions shall demonstrate the State's intention to authorize the unlawful act - in a way that transmits a specific desire of the latter, as stated in *Tehran Hostages*[334].

6.2. DIRECTION

According to the ICJ in *Bosnian Genocide*, the criterion of direction is met when "an organ of the State (...) provided the direction pursuant to which the perpetrators of the

[324] Macak, 2016.
[325] *Ibid.* 324.
[326] *Ibid.* 324, p. 415.
[327] *Ibid.* 324, p. 415.
[328] *Ibid.* 324.
[329] *Ibid.* 324, p. 415.
[330] *Ibid.* 324.
[331] *Ibid.* 310, p. 1508.
[332] *Ibid.* 324, p. 415.
[333] *Ibid.* 324, p. 416.
[334] *Ibid.* 324.

wrongful act acted"[335] - implying the need of a continuous relationship "that goes beyond the simple issuance of instructions with no further follow-up"[336], between the State and the private actor. Following this reasoning, Crawford stated that "'direction' implies a continuing period of instruction, or a relationship between the state and a non-State entity such that suggestion or innuendo may give rise to responsibility"[337]. In this sense, if a state maintains a subordination relationship with a person or group and guides its conduct, "it may incur responsibility for their individual acts even in the absence of express instructions to commit those"[338].

6.3. CONTROL

As a corollary of its sovereign power over its own territory, a State may be presumed to have "some capacity to control private acts committed in its territory"[339]. However, the question is which kind and level to control a State must exercise to the conduct be attributable to it[340]. To identify the cases in which control exists, the ICJ formulated, in *Nicaragua*, the 'effective control' test – which was re-affirmed in *Bosnian Genocide*. For this test to be met, the State must go beyond mere supporting the private actor, "must be involved in planning the operations, choosing the targets and the provision of operational support throughout"[341]. That is, "must be able to control the beginning of the operation, the way it is carried out, and its end"[342]. It does not require "control over each potentially wrongful act but only over a broader course of action within which such acts would have been committed"[343]. The clearest example "is one in which the state has specifically instructed private groups to engage in a cyber attack (…) Arming and training a private group engaged in violence"[344].

However, "mere funding is insufficient, even when a state has provided 'heavy subsidies'"[345], and the Tallinn Manual, although recognizes that providing an OAG "with malware and the training necessary to use it to carry out cyber attacks against another

---

[335] *Ibid.* 324, p. 417 *apud* Case Concerning the Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v Serbia and Montenegro), 2007.
[336] *Ibid.* 324, p. 417-418. .
[337] *Ibid.* 324, p. 418 *apud* Crawford, J., State Responsibility: The General Part, 2013.
[338] *Ibid.* 324, p. 418.
[339] *Ibid.* 324, p. 420.
[340] *Ibid.* 324.
[341] *Ibid.* 324., p. 421
[342] Talmon, 2009, p. 9.
[343] *Ibid.* 324, p. 421
[344] *Ibid.* 301, p. 507.
[345] *Ibid.* 301, p. 507.

State"[346] qualify as use of force[347], follows the ICJ comprehension that funding a hacktivist group conducting cyber operations would not be use of force[348]. Nevertheless, this test imposes a very high standard and, considering that evidence gathering is challenging in cyberspace, its use may lead to negative findings in many cases – and, consequently, non-attribution of the responsibility to a state.

On the other hand, the Appeals Chamber of the ICTY, in *Tadic*, proposed the 'overall control' test[349], which demands the State to provide "the non-State entity with financial and training assistance, military equipment and/or operational support, and to participate in the organisation, co-ordination or planning of operations of the entity in question"[350]. In this case, if the State, for example, provides a malware, "to a non-State group of hackers and co-ordinated the choice of targets (…), its conduct would likely satisfy the test of overall control, although it would fall short of the standard of effective control"[351]. However, the use of this test was limited, by the ICTY, to OAG and it its marked "by a misunderstanding of the distinction between primary and secondary rules of international law"[352], being rejected in by the ICJ in *Bosnian Genocide* [353].

Nevertheless, even if the effective control test is the appropriate standard "for the purposes of the last criterion in Article 8, there are good reasons why this test may gradually be losing its relevance to modern challenges"[354]. Moreover, "the ILC's approach may plausibly be seen as allowing for a more liberal test under specific circumstances"[355]. On its commentaries, the Commission "did not insist on the use of the *Nicaragua* test without exception, nor did it reject the *Tadic* test"[356]. Instead, allowed a context-based flexibility, noting that it "is a matter for appreciation in each case whether particular conduct was or was not carried out under the control of a State, to such an extent that the conduct controlled should be attributed to it"[357]. That is, the requirement of control levels may vary according to the context[358]. In this regard, it has been suggested

[346] Ibid. 210, p. 332.
[347] *Ibid.* 301.
[348] Ibid. 210.
[349] *Ibid.* 324.
[350] *Ibid.* 324, p. 422.
[351] *Ibid.* 324, p. 422.
[352] *Ibid.* 324, p. 423.
[353] *Ibid.* 324.
[354] *Ibid.* 324, p. 423.
[355] *Ibid.* 324, p. 424.
[356] *Ibid.* 324, p. 424.
[357] *Ibid.* 324, p. 424.
[358] Tsagourias, 2016.

that Article 55 RSIWA, "may bolster the case for flexibility"[359]. However, currently, it would be "premature to speculate about the existence of such specific rules in the sense required by Article 55"[360].

Finally, regarding the *Nicaragua* test, it can be pointed that, even if the decision was correctly made at the time, currently it should be "seen through the historical prism of its origin, which was far removed from the modern reality of cyberattacks"[361]. Thus, "if this decision were extended to cyber militias, it would mean that State sponsors of cyber attacks would only be held accountable if their effective control could be proven beyond any doubt"[362]. And, considering the "technical challenges of proving the identity of cyber attackers (…) such a standard could give a free pass to state sponsorship of cyber attacks"[363]. Therefore, it is necessary to reexamine the concept of control in cyberspace, since a more flexible comprehension - like overall control standard - would improve cybersecurity[364]. Lastly, according to the ICJ in *Bosnian Genocide*, there is no doubt that a relation between a State and a private actor does not fall within the scope of article 8 when the latter acts as a complete dependent of the State - of which is a merely instrument[365]. Instead, the private group is a *de facto* organ of the state, and the latter is responsible for their conduct under Article 4 of the Draft[366].

Given the above, new tools and techniques both improve and include attribution capabilities. Additionally, "other challenges can greatly complicate attribution and cyber response when an immediate response is required"[367]. Moreover, the Tallin Manual "fails to acknowledge aspects of the *Nicaragua* and *Tadić* decisions that might have supported a broader reading of state responsibility"[368], missing the opportunity to cite them to "temper its reliance on the pat test announced in the Draft Articles"[369]. There are: the tribunal's view of "aid as a burden-shifting device, with the presumption of state control"[370] and the tribunal's textual discussion of the shared elements between the Republic of Yugoslavia and a genocidal paramilitary group.

---

[359] *Ibid.* 324, p. 425.
[360] *Ibid.* 324, p. 425.
[361] *Ibid.* 324, p. 425.
[362] Shackelford & Andres, 2011, p. 987.
[363] Shackelford & Andres, 2011, p. 987.
[364] *Ibid.* 324.
[365] *Ibid.* 324.
[366] *Ibid.* 324.
[367] *Ibid.* 310, p. 1510.
[368] *Ibid.* 301, p. 508.
[369] *Ibid.* 301, p. 509
[370] *Ibid.* 301, p. 509

In addition, when interpreting restrictively State responsibility, the RSIWA "unduly discounted the need for due diligence in monitoring non-state actors' use of state aid"[371]. After the attacks on September 11th, international law started to pay "greater attention to states' obligations to disrupt networks of violent non-state actors operating from their territory, including groups actually receiving state assistance"[372]. Due to this change, the "Manual's reliance on the ILC's approach is particularly risky"[373]. Since, after this date, the RSIWA "may not be an accurate account of the law"[374]. Lastly, although "the law governing kinetic armed conflicts may contribute little (…) to the law applicable to state responsibility for cyber attacks"[375], the status of the effective and overall control tests in cyberspace is open to serious issues due to the attribution asymmetry in those different environments[376].

In this regard, Peter Margulies proposes the Virtual Control test, under which the State attacked can request more information to the state in virtual control. Thus, the information produced by this state "may show that it was in fact uninvolved in the attack or was unable to control the individual or entity responsible for the attack. Alternatively (…) may show the virtual controller's responsibility"[377]. If the State in control does not provide the information, the victim can pursue other means, including the use of force - in self-defense - if a cyber-attack crosses "the threshold into an armed attack under art 51 of the UN Charter"[378]. Additionally, this approach "would shift the burden in (…) the use of state infrastructure for an attack"[379]. Since, according to it, launch an attack using State infrastructure should "create a rebuttable presumption that the state owning the infrastructure is responsible"[380]. Therefore, if a state does not demonstrate that it has invested in anti-hacker measures and adequate digital controls, it fails to meet its burden[381]. Consequently, it may be sanctioned by international bodies as well as deal with self-defense from the victim state[382].

---

[371] *Ibid.* 301, p. 509
[372] *Ibid.* 301, p. 509
[373] *Ibid.* 301, p. 509.
[374] *Ibid.* 301, p. 514
[375] *Ibid.* 301, p. 514
[376] *Ibid.* 301.
[377] *Ibid.* 301, p. 514
[378] *Ibid.* 301, p. 515
[379] *Ibid.* 301, p. 515
[380] *Ibid.* 301, p. 515
[381] *Ibid.* 310.
[382] *Ibid.* 301.

7. CONCLUSION

Undoubtedly, cyber operations during conflicts represent a genuine risk to both civilians and States. Given this, realizing that these operations do not take place in a legal vacuum is essential to protect civilians and civilian infrastructure[383]. Nevertheless, as exposed in this work, although it is accepted that principle of distinction is applicable to cyber operations in armed conflicts, this mere recognition does not end the discussion. Since the partially non-physical character of the cyber domain and the interconnectivity between military and civilian networks poses legal and practical challenges to the application IHL principles and rules[384]. That is, the practical application of the existing rules faces many obstacles, especially considering the dual nature of cyber infrastructure and the difficulty of attributing attacks. Once, besides being difficult to transpose some rules from the kinetic to the cyber environment, there is a lack of consensus on the comprehension of certain norms in this context.

In addition, other issues such as the participation of civilians or organized armed groups in cyber war raises a unique set of questions and harms[385]. In this sense, groups such as the IT Army of Ukraine, challenge the traditional rules of conflicts, raising regulatory and ethical questions regarding their status, protection, attributability and compliance with IHL. Moreover, there is an increasing difficult to predict the escalation of the involvement of those, as technology and cyber war evolve[386]. Therefore, immediate action is needed from the international community to fill the current gap concerning the IHL applicability on the conduct and status of individuals and groups engaging in cyber operations[387].

Furthermore, one of the key issues in this context is the State's responsibility attribution. Since, as referred, unlike traditional warfare, in cyber operations identification of perpetrators is harder, and States may struggle to meet their obligations under IHL, as well as to be found responsible for unlawful acts. Additionally, although a legal framework, providing general attribution rules, exists, its interpretation and application in the cyber domain is still debated. Thus, states should endeavor to establish criteria or measures in this regard - such as seeking agreements with other States - aiming to

[383] *Ibid.* 5.
[384] *Ibid.* 1.
[385] *Ibid.* 240.
[386] *Ibid.* 240
[387] *Ibid.* 185

establish a more concrete customary international law for attribution in the cyber domain[388].

Lastly, the interpretation of current law is restricted to the state's practice and the available scholarly discourse due to the specific treaty provisions and court rulings. And, since the effectiveness of norms depends on their acceptance and consistent application by international actors, a general clarification and further development of this subject – both practical and theorical – is needed, to ensure the granting of IHL principles in the modern warfare. Therefore, as stated by the UN Secretary General António Guterres "we need to find a minimum of consensus in the world on how to integrate these new technologies in the laws of war that were defined decades ago in a completely different context"[389].

8. BIBLIOGRAPHIC REFERENCES

Antonopoulos, C. (2021). State responsability in cyberspace. In N. Tsagourias & R. Buchan (Eds.), *Research Handbook on International Law and cyberspace*, 113–129. Edward Elgar Publishing.

Lopes, J. A. A., Queiroz, B. M., Moreira , F. C., Abreu, L. C., Campos, M. F., Tavares, M. I., & de Sousa, B. R. (2019). *Regimes Jurídicos Internacionais,* 2. Universidade Católica Editora Porto.

Lopes, J. A. A., Queiroz, B. M., Moreira , F. C., Abreu, L. C., Campos, M. F., Tavares, M. I., & de Sousa, B. R. (2020). *Regimes Jurídicos Internacionais,* 1. Universidade Católica Editora Porto.

Azeredo Lopes, J. A., Menezes Queiroz, B., Castro Moreira , F., Carvalho Abreu, L., Fontaine Campos, M., Tavares, M. I., & Reynaud de Sousa , B. (2020). *Regimes Jurídicos Internacionais,* 1. Universidade Católica Editora Porto.

Banks , W. (2017). State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0 [Review of *State Responsibility and Attribution of Cyber Intrusions After Tallinn 2.0*]. *Texas Law Review*, *95*(7), 1487–1513. https://texaslawreview.org/state-responsibility-attribution-cyber-intrusions-tallinn-2-0/.

Biggio, G. (2024). The Legal Status and Targeting of Hacker Groups in the Russia-Ukraine Cyber Conflict. *Journal of International Humanitarian Legal Studies*, *15*, 142–182. https://brill.com/view/journals/ihls/15/1/article-p142_006.xml.

Brig. Gen. Wallace, D., Col. Reeves, Shane., & Maj. Powell, T. (2021). Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines. Harvard National Security Journal, 12, 164–197. https://harvardnsj.org/wp-

[388] *Ibid*. 310.
[389] *Ibid.* 5, p. 363.

content/uploads/2021/02/HNSJ-Vol-12-Wallace-Reeves-and-Powell-Direct-Participation-in-Hostilities-in-the-Age-of-Cyber.pdf.

Biggerstaff, W. C. (2023). The Status of Ukraine's "IT Army" Under the Law of Armed Conflict - Lieber Institute West Point. Lieber Institute West Point. https://lieber.westpoint.edu/status-ukraines-it-army-law-armed-conflict/

Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight. (1868). The Hague Peace Conferences and Other International Diplomacy *1899–1914.* https://ihl-databases.icrc.org/en/ihl-treaties/st-petersburg-decl-1868/declaration?activeTab=.

Dinstein, Y. (2002). Legitimate Military Objectives under the Current Jus in Bello. International Law Studies, 78, 139–172. /https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1361&context=ils.

Done, W. D. (2023). The Information Technology Army of Ukraine and Cyber Warfare Doctrine. *Journal of Strategic Security*, *16*(4), 15–33. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2127&context=jss.

Doswald-Beck, L. (2002). Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. *Internacional Law Studies*, *76*, 163–185. https://digital-commons.usnwc.edu/ils/vol76/iss1/17/.

Flecker, D. (2007). Individual and State Responsibility for Intelligence Gathering. *Michigan Journal of International Law*, 28(3), 687–709. https://repository.law.umich.edu/cgi/viewcontent.cgi?params=/context/mjil/article/1174/&path_info=

Geib, R., & Lahmann, H. (2012). Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space. *Israel Law Review*, *45*(3), 381–399. https://heinonline.org/HOL/Page?handle=hein.journals/israel45&div=27.

Lieber, F., General Order No. 100, U.S. War Department. (1898). Instructions for the government of armies of the United States in the field. U.S. Government Printing Office. https://tile.loc.gov/storage-services/service/ll/llmlp/Instructions-gov-armies/Instructions-gov-armies.pdf.

Gisel, L., Rodenhäuser, T., & Dörmann, K. (2020). Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross*, *102*(913), 287–334. https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/twenty-years-ihl-effects-of-cyber-operations-during-armed-conflicts-913.pdf.

Hathaway, O. A., Khan, Azmat., & Revkin, Mara. (2024). THE DANGEROUS RISE OF "DUAL-USE" OBJECTS IN WAR. *Duke Law School Public Law & Legal Theory Series*, 1–97. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4938707.

Huang, Z., & Ying, Y. (2020). The application of the principle of distinction in the cyber context: A Chinese perspective. In *International Review of the Red Cross*, *102* (913), 335–365. Cambridge University Press. https://international-review.icrc.org/articles/principle-of-distinction-cyber-context-chinese-perspective-913.

Iaria, A. (2023, February 17). Debate on a Digital Emblem: The Specific Protection of Healthcare Facilities. Lieber Institute West Point. https://lieber.westpoint.edu/debate-digital-emblem-specific-protection-healthcare-facilities/.

ICJ, International Court of Justice. (1996). Legality of the threat or use of nuclear weapons: Advisory opinion (para. 86). International Court of Justice. https://www.icj-cij.org/en/case/95.

ICRC, International Committee of the Red Cross. (1987). General introduction to the Commentary on Protocol II. In *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Martinus Nijhoff Publishers. https://ihl-databases.icrc.org/en/ihl-treaties/apii-1977/part1/commentary/1987

ICRC, International Committee of the Red Cross. (2020). International humanitarian law and cyber operations during armed conflicts. ICRC position paper submitted to the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, November 2019. *International Review of the Red Cross*, *102*(913), 481–492. https://international-review.icrc.org/sites/default/files/reviews-pdf/2021-03/ihl-and-cyber-operations-during-armed-conflicts-913.pdf

ICRC, International Committee of the Red Cross. (1977). Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts *(Protocol II)*. https://ihl-databases.icrc.org/ihl/INTRO/475

ICRC, International Committee of the Red Cross. (1977). Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I). https://ihl-databases.icrc.org/ihl/INTRO/470

ICRC, International Committee of the Red Cross. (1949). Geneva Convention relative to the Treatment of Prisoners of War (Third Geneva Convention). https://ihl-databases.icrc.org/en/ihl-treaties/gciii-1949.

ILC, International Law Commission. (2001). Draft articles on the responsibility of states for internationally wrongful acts. United Nations. https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf.

Instructions for the Government of Armies of the United States in the Field (1898). https://tile.loc.gov/storage-services/service/ll/llmlp/Instructions-gov-armies/Instructions-gov-armies.pdf

Kirichenko, D. (2023). Ukraine's Volunteer IT Army Confronts Tech, Legal Challenges. CEPA. https://cepa.org/article/ukraine-volunteer-it-army-confronts-tech-legal-challenges/rmy-confronts-tech-legal-challenges/

Macak, K. (2015). Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law. *Israel Law Review*, *48*(1), 55–80. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2456955.

Macak, K. (2016). Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of Cyber Operations by Non-State Actors. *Journal of Conflict and Security Law*, *21*(3), 405–428. https://www.jstor.org/stable/26298208?saml_data=eyJpbnN0aXR1dGlvbklkcyI6WyJjYj

ViNDU4Ny0wYzJlLTQ2MTktYjNiNC1iNGUwNzJjN2QyZDQiXSwic2FtbFRva2VuIjoiMDFmOTQxZDktNzY4NC00NzY4LWExODAtYTc1MmMzYmQ0ZDg0In0&seq=1

Margulies, P. (2013). Sovereignty and cyber attacks: technology's challenge to the law of state responsibility. *Melbourne Journal of International Law*, *14*, 498–519. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2557517.

Mavropoulou, E. (2015). Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyber Attacks. *Journal of Law & Cyber Warfare*, *4*, 23–93. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4067446.

McCormack, T. (2018). International Humanitarian Law and the Targeting of Data. *International Law Studies*, *94*, 223–240. https://digital-commons.usnwc.edu/ils/vol94/iss1/9/.

Mc Hugh, G., & Bessler, M. (2006). Humanitarian negotiations with armed groups: A manual for practitioners. United Nations Office for the Coordination of Humanitarian Affairs. https://interagencystandingcommittee.org/sites/default/files/migrated/2014-12/Human_Neg_Manual.pdf

Meyer, J. M. M., (2001). Tearing down the facade: a critical look at the current law on targeting the will of the enemy and air force doctrine. *Air Force Law Review*, 143–182. https://research.ebsco.com/c/ljojij/viewer/pdf/lqumnmvoov.

Melzer, N. (2011). Cyberwarfare and International Law. In *UNIDIR Resources*. https://unidir.org/files/publication/pdfs/cyberwarfare-and-international-law-382.pdf.

Melzer, N. (2009). Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law. *International Committee of the Red Cross*. https://www.icrc.org/sites/default/files/external/doc/en/assets/files/other/icrc-002-0990.pdf.

ICRC, International Commite of the Red Cross, Official Records of the Diplomatic Conference on the Reaffirmation and Development of International Humanitarian Law Applicable in Armed Conflicts (1978). Geneva, 1974-1977. Volume IV. https://maint.loc.gov/rr/frd/Military_Law/pdf/RC-records_Vol-6.pdf

Pacholska, M. (2023). "Neither criminal nor civil": russian state responsibility for conduct of hostilities violations in Ukraine. *Texas Tech Law Review*, *56*, 151–170. hein online. https://dare.uva.nl/search?identifier=50b68cc8-9f07-42f4-90f6-3c9ad03019ad.

Render-Katolik, A. (2023). The IT Army of Ukraine, Strategic Technologies Blog, CSIS. https://www.csis.org/blogs/strategic-technologies-blog/it-army-ukraine

Schmitt, M. N. (2011). Cyber Operations and the Jus in Bello: Key Issues [Review of *Cyber Operations and the Jus in Bello: Key Issues*]. *International Law Studies* , *87*, 89–110. https://digital-commons.usnwc.edu/ils/vol87/iss1/7/.

Schmitt, M. N. (2014). Rewired warfare: Rethinking the law of cyber attack. *International Review of the Red Cross*, *96*(893), 189–206. https://international-review.icrc.org/sites/default/files/irrc-893-schmitt.pdf

Schmitt, M. N. (Ed.). (2013). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. https://csef.ru/media/articles/3990/3990.pdf.

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge University Press. chrome-https://ilmc.univie.ac.at/fileadmin/user_upload/p_ilmc/Bilder/Bewerbung/Case_2/Michael_N._Schmitt_-_Tallinn_Manual_2.0_on_the_International_Law_Applicable_to_Cyber_Operations-Cambridge_University_Press__2017_.pdf

Shackelford, S., & Andres, R. B. (2011). State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem. In *Georgetown Journal of International Law*, 42 (4) 971-1016. https://heinonline.org/HOL/Page?lname=Shackelford&public=false&collection=journals&handle=hein.journals/geojintl42&men_hide=false&men_tab=toc&kind=&page=971.

Stubblefield, E. (2024). Hacktivists as Combatants: What Ukraine's Counteroffensive to Russia's Cyberwarfare Means for Civilian Hackers' Status Under the Laws of War. *Fordham Urban Law Journal*, *52*(1), 217–250. https://perma.cc/S298-CU7Q.

Sucharitkul, S. (1996). State Responsibility and International Liability under International Law, in *Loyola of Los Angeles International and Comparative Law Journal*, 9th ed., 18 (4), 821-839. https://digitalcommons.law.ggu.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1225&context=pubs.

Sweney, G. (2005). Saving Lives: The Principle of Distinction and the Realities of Modern Warfare. *International Lawyer*, *39*(3), 733–758. https://scholar.smu.edu/til/vol39/iss3/6http://digitalrepository.smu.edu.

Talmon, S. (2009). The Various Control Tests in the Law of State Responsibility and the Responsibility of Outside Powers for Acts of Secessionist (16/2009). http://ssrn.com/abstract=1402324.

Tsagourias, N. (2016). Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts. *Journal of Conflict and Security Law*, *21*(3), 455–474. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3242718.

Ukraine's IT army is a world first: here's why it is an important part of the war. (2023). University of Portsmouth. https://www.port.ac.uk/news-events-and-blogs/blogs/security-and-risk/ukraines-it-army-is-a-world-first-heres-why-it-is-an-impo.

U.S. Department of the Army. (2019). The commander's handbook on the law of land warfare *(FM 6-27/MCTP 11-10C)*. https://irp.fas.org/doddir/army/fm6_27.pdf.

Wallace, D., & Reeves, S. R. (2013). The Law of Armed Conflict's "Wicked" Problem: Levée en Masse in Cyber Warfare. *International Law Studies*, *89*, 646–668. https://digital-commons.usnwc.edu/ils/vol89/iss1/1/.