AHMAD KHALIL, S. ANANDHA KRISHNA RAJ

Challenges to the Principle of Distinction in Cyber Warfare: Navigating International Humanitarian Law Compliance

Abstract

This paper examines the profound challenges confronting the principle of distinction in cyber warfare, while considering the evolving nature of modern armed conflicts. This paper emphasizes the necessity of reaching an agreement on the classification of cyber operations during conflicts as "attacks", regardless of their physical or nonphysical consequences, to preserve the relevance of the distinction principle. Furthermore, this paper highlights the need for comprehensive legal frameworks tailored to the nuances of cyberspace and the urgent requirement to bridge the gap between traditional international humanitarian law (IHL) and the unique difficulties posed by digital conflict. Additionally, this paper examines the compliance of Russian cyberattacks against Ukraine with the principle of distinction. Because technology continually redefines the limits of warfare, it is crucial to uphold these principles to safeguard humanity amid the challenges of modern warfare.

KEYWORDS: Cyberspace Warfare, International Humanitarian Law, Principle of Distinction, Cyberattacks, Civilian Protection

AHMAD KHALIL, PhD candidate, Vellore Institute of Technology, School of Law (VITSOL), Chennai, India, ORCID – 0009-0007-0615-9812, e-mail: ahmad.khalil2020@vitstudent.ac.in

S. ANANDHA KRISHNA RAJ, associate professor, Vellore Institute of Technology, School of Law (VITSOL), Chennai, India, ORCID – 0009-0001-0177-1689, e-mail: anandha.krishnaraj@vit.ac.in

HTTPS://DOI.ORG/10.36128/PRIW.VI49.769

1 Introduction

The evolution of warfare has transcended traditional boundaries, spanning land, sea, air, and even space. More recently, however, a new domain has emerged as the frontline of conflict – cyberspace. Cyber warfare represents a distinct and unprecedented dimension of modern warfare, distinct from conventional kinetic warfare. While IHL attempts to provide a framework for regulating conflict, it faces profound challenges when applied to the unique characteristics of cyber warfare. This research paper delves into the complex landscape of cyber warfare and specifically examines the problematic application of the principle of distinction in this domain.

Cyber warfare poses many novel challenges due to its sui generis nature. For IHL to apply, there must be an armed attack, a concept clarified in Article 49 of Additional Protocol I to the Geneva Conventions. This criterion gives rise to considerable debate and scrutiny when applied to cyberattacks[1]. In particular, cyberattacks are often characterized by their anonymity, making it extremely difficult, if not impossible, to determine the identity of the attackers. This paper also highlights the contentious issues surrounding attribution in the cyber domain. Moreover, the core principles of IHL, including necessity, proportionality, and distinction, face profound challenges when applied to the cyber domain[2]. The question of how these principles should be interpreted and applied in cyber warfare remains a topic of ongoing discussion and research. To this end, a report by the Secretary General of the United Nations aptly recognized that cyber warfare presents „new and unique" challenges, signifying the need for a comprehensive examination[3].

---

1 International Committee of the Red Cross, *International Humanitarian Law and Cyber Operations during Armed Conflicts*, 27 October 2022. https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts. [assessed: 13.07.2023].

2 Jack McDonald, „Blind Justice? The Role of Distinction in Electronic Attacks" *Ethics and Policies for Cyber Operations*, (2016): 17-32. https://doi.org/10.1007/978-3-319-45300-2_2.

3 Joint Inspection Unit of the United Nations System, C*ybersecurity in the United Nations System Organizations (JIU/REP/2021/3).*, 2021. https://www.unjiu.org/news/cybersecurity-united-nations-system-organizations-jiurep20213-0.

While the cyber domain poses a wide array of challenges[4], this research article focuses explicitly on the limitations of applying the principle of distinction in cyber warfare, assuming the existence of an ongoing armed conflict as recognized under Article 49 of Additional Protocol I (API). The principle of distinction is one of the pillars of IHL, requiring a clear distinction between combatants and civilians and prohibiting the targeting of the latter.

This paper proposes a set of recommendations to address the intricacies and difficulties surrounding the principle of distinction in cyber warfare. These recommendations, intended for the consideration of the International Committee of the Red Cross (ICRC), aim to provide a framework that can guide the application of the principle of distinction in the unique and challenging context of cyber warfare. By doing so, this research article seeks to contribute to the ongoing dialogue on the regulation of cyber warfare under international law.

2 The Meaning of Attacks and Armed Conflicts in Cyberspace

The distinction is a fundamental principle of IHL and is a critical framework that demarcates the boundaries of conflict. It stipulates that during times of war, enemy combatants (excluding those hors de combat, such as the wounded, sick, and those who have surrendered) and military objectives can be targeted, while enemy civilians and civilian objects must be safeguarded from attack[5]. However, a pressing question arises: what constitutes an „attack"? API and Customary International Law define an attack as „acts of violence against the adversary, whether in offense or defense" (AP I, 1977, Article 49). Although somewhat detached from the conventional notion of an offensive action, this interpretation encompasses both offensive and defensive actions. Crucially, the litmus test for an attack within

4 Edward Geist, „Deterrence Stability in the Cyber Age" *Strategic Studies Quarterly*, No. 4 (2015): 44-61. https://doi.org/https://www.jstor.org/stable/26271277.

5 Nils Melzer, „The Principle of Distinction Between Civilians and Combatants", [in:] *The Oxford Handbook of International Law in Armed Conflict*, ed. Andrew Clapham, Paola Gaeta (Oxford: Oxford University Press, 2014), 296-331. https://doi.org/10.1093/law/9780199559695.003.0012.

the context of IHL is the commission of „acts of violence". To qualify as an attack, an act must result in loss of life, injury to persons, or material damage to property. This definition remains agnostic as to whether the violence is directed against enemy combatants and military objectives or against enemy civilians and civilian objects.[6].

It is worth noting that an attack does not have to be kinetic. Thus, a „Computer Network Attack" (CNA) is considered an attack under the IHL, provided it results in acts of violence. According to this, merely „hacking" an enemy computer system to obtain intelligence does not qualify as an attack under IHL and does not represent a legitimate CNA. Similarly, according to IHL standards, doing things like breaking through a computer's firewall, inserting a worm into digital software, obtaining control over codes, retrieving secret data, or interfering with communications are not considered CNAs[7]. These activities are not considered attacks because they lack the essential element of force.

However, a paradigm shift occurs when a hostile computer—military or civilian—takes control and causes casualties to humans or serious harm to tangible property. An example would be the permanent disablement of the target machine or the incapacitation of life-supporting software[8].

Defining the necessary concepts related to cyber warfare is vital to understanding how IHL operates in the event of launching cyber operations during the war. These concepts include the definition of „cyber weapons", „cyber-attacks", and discerning the parameters of „cyber armed conflicts", whether international or internal. Clarity in these definitions is essential, as it triggers the application of IHL, providing protection to involved actors while ensuring the protection of uninvolved civilians[9]. Without precise definitions, there is a legal void, leaving the civilian population vulnerable

6 Michael Gervais, „Cyberattacks and the Laws of War" *SSRN Electronic Journal*, (2011). https://doi.org/10.2139/ssrn.1939615.

7 Giacomo Biggio, „International Humanitarian Law and the Protection of the Civilian Population in Cyberspace: Towards a Human Dignity-Oriented Interpretation of the Notion of Cyber Attack under Article 49 of Additional Protocol I" *The Military Law and the Law of War Review*, No. 1 (2021): 114-140. https://doi.org/10.4337/mllwr.2021.01.06.

8 Amit Sharma, „Cyber Wars: A Paradigm Shift from Means to Ends" *Strategic Analysis*, No. 1 (2010): 62-73. https://doi.org/10.1080/09700160903354450.

9 , Adasi Nsanawaji Igakuboon, „An Appraisal of the Legal Framework for the Protection of Civilians in Cyber-Warfare under International Humanitarian Law" *International Journal of Research and Scientific Innovation*, No. 07 (2022): 14-26. https://doi.org/10.51244/ijrsi.2022.9702.

during conflict, which fundamentally contradicts the primary purpose of IHL, which is safeguarding civilians.

Starting with the concept of „cyber weapons", it is essential to note that there is no universal consensus on their definition within the international legal framework. While there is a definition for the broader term „weapon", the specificity of „cyber weapons" remains a point of contention. The Tallinn Manual 2.0, for instance, defines cyber weapons as „cyber means of warfare that are used, designed, or intended to be used to cause injury to, or death of, persons or damage to, or destruction of, objects, that is, that result in the consequences required for qualification of a cyber operation as an attack"[10]. However, this definition necessitates physical consequences, excluding cyber tools that cause loss of functionality. A broader definition, proposed by some experts, characterizes „cyber weapons as computer code used or designed to be used with the intent of threatening or causing physical, functional, or mental harm to structures, systems, or living beings"[11]. This interpretation aligns with the United States Air Force's regulation on the Legal Reviews of Weapons and Cyber Capabilities, which defines „weapons as devices designed to kill, injure, disable, or temporarily incapacitate people or destroy, damage, or temporarily incapacitate property or material"[12]. Such a definition accommodates a range of cyber weapons, from those causing physical damage to those inducing temporary loss of functionality, without encompassing cybercrimes or cyber-espionage activities that do not escalate to acts of warfare. Balancing this definition is crucial to prevent overly broad interpretations that could hinder enforcement.

Regarding „armed conflicts" in cyberspace, there is no precise universal definition within IHL. IHL can only be applied in cases where there is an armed conflict. The Geneva Conventions (GCs) can be used for „cases of declared war or any other armed conflict that may arise between two or more parties". It follows Common Article 2.

The use of armed force between states, or an ongoing armed conflict between government authorities and organized armed groups, or between such groups within a state, is generally considered to constitute an armed

10 Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017).

11 Thomas Rid, Peter McBurney, „Cyber-Weapons" *The RUSI Journal*, No. 1 (2012): 6-13. https://doi.org/10.1080/03071847.2012.664354.

12 David Stephen Alberts, John Garstka, Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority* (CCRP Publication, 2005).

conflict. This use of armed force is the threshold that triggers the application of IHL[13].

However, not every use of force necessarily qualifies as an armed conflict. Sporadic, isolated, or temporary events do not meet the conditions for armed conflict, known as the threshold[14]. In such cases, other legal regimes, such as international human rights law (IHRL) or law enforcement mechanisms, govern cyber operations. While IHRL persists during armed conflict, IHRL takes precedence due to its specificity in regulating conduct during hostilities.

The ICJ, in its Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*, affirmed the application of IHL principles to all forms of warfare and all types of weapons, including those of the future[15]. Consequently, during armed conflicts, cyber operations are subject to IHL. Now, with an understanding of these crucial definitions and principles, we turn to the overarching theme of this article: the possibility of applying IHL to cyber warfare and the obstacles it encounters. This discussion aims to illuminate the intricacies of applying IHL to the ever-evolving landscape of cyber warfare and to propose recommendations for addressing these challenges.

3 The Challenges of Implementing IHL in the Realm of Cyber Warfare

The existing framework of IHL does not explicitly prohibit cyber weapons the way that some conventional, biological, and chemical weapons have been banned. Nonetheless, Article 36 of API, sometimes known as the „weapons review" provision, emphasizes that IHL is a flexible body of law. This provision mandates states to evaluate new weapons, means, or methods of warfare from a legal standpoint to ascertain whether their use

13 Scott J. Shackelford, „From Nuclear War to Net War: Analogizing Cyberattacks" *International Law*, No. 1 (2009): 191-250. P200. https://doi.org/https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10239/SSRN-id1396375.pdf.

14 Melzer, „The Principle of Distinction between Civilians and Combatants", 296-331. https://doi.org/10.1093/law/9780199559695.003.0012.

15 ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996. https://www.icj-cij.org/case/95. [assessed: 27.07.2023].

would breach international law. Article 36 underscores that IHL extends its purview to technologies and weapons developed after the establishment of these laws, highlighting the relevance of emerging technologies within the framework of IHL. It aligns with the stance taken by the ICJ in its Advisory Opinion on the *Legality of the Threat or Use of Nuclear Weapons*, which affirmed that IHL's rules and principles could be applied to „all forms of warfare and to all kinds of weapons, including those of the future". Consequently, before using any „cyber weapons" in military operations, states must comply with IHL by conducting a legal examination[16].

The critical task is determining the scope of IHL's applicability to cyber operations, as this body of law bestows various obligations and protections during armed conflicts. Importantly, IHL pertains solely to cyber operations that transpire within or bear a connection to an armed conflict. Such conflicts are classified into International Armed Conflicts (IAC) and Non-International Armed Conflicts (NIAC). The classification of the armed conflict dictates the specific IHL rules applicable, underscoring the necessity of delineating the criteria for each to ascertain the relevant rules. In cyber operations, several challenges emerge in establishing the presence of either an IAC or a NIAC, ultimately shaping the application of IHL to these scenarios.

In the following sections, we will explore the nuances of IACs and NIACs in cyberwarfare.

3.1. IACs in Cyberspace: Criteria and Challenges

The qualification of a conflict as an IAC is based on the provisions of Common Article 2 of the GCs, which states that the Conventions apply „to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them". This provision, which reflects customary international law, establishes that whenever hostile armed force is used between two or more states, an IAC is at play. The brevity or intensity of the use of armed force is not a determining factor; its mere occurrence triggers the application of IHL. Furthermore, there is no specific form prescribed for the use of force, which means that states may engage in cyberattacks, military operations, or a mixture of the two during wars.

16 Ibidem, paras 78-79.

Complications arise when non-state actors or private individuals engage in operations that can be assigned to a state, thus transforming the nature of the conflict from internal to international. States typically engage in cyber operations through intermediaries, such as private companies, to disguise direct responsibility. The critical determinant in these situations is the establishment of the state's „effective control" over the cyber operation. This criterion can be particularly difficult to meet in cyberspace, where the perpetrators or the point of attack may span multiple jurisdictions, making attribution and accountability even more elusive[17].

The generally accepted criteria for qualifying a conflict as an IAC are drawn from Common Article 2(1) of the GCs, which extends the application of the Convention „to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them". International customary law is reflected in this clause. Additionally, an IAC may only be qualified if „a resort to armed forces between states", as stated in the Tadic case. Therefore, IHL rules emerge when the first shot is fired; an interpretation articulated in Pictet's „first shot theory". Rule 82 of the Tallinn Manual 2.0 states, „an IAC exists whenever there are hostilities, which may include or be limited to cyber operations, between two or more states"[18].

A significant development by the International Group of Experts (IGE) was the reference to the term „hostilities" rather than the expression „resort to armed forces" used in traditional IAC[19]. This linguistic shift helps interpret international cyber-armed conflicts more effectively, given that attempting to prove the „use of armed forces" in cyberspace is impractical. Most academics contend that if a state is responsible for a cyber operation and produces effects akin to a kinetic attack, it meets the threshold for an armed conflict. However, equating cyber operations with kinetic attacks is problematic because the damage caused by cyber weapons often differs from that caused by traditional weapons.

17 Jeremy Richmond, „Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?" *Fordham International Law Journal*, No. 3 (2012): 842-894, 846. https://doi.org/https://ir.lawnet.fordham.edu/ilj/vol35/iss3/1.

18 Schmitt, Supra, 10.

19 Clara Mathonet, *Protection of Civilians in the Era of Cyber Warfare: A Critical Analysis of International Humanitarian Law Towards a Treaty Restricting the Use of Cyber Weapons* (Thesis: University of Amsterdam, 2020).

The intensity required for resorting to armed force remains a contentious issue. Some academics say hostilities must intensify to a particular degree to be considered an IAC, necessitating more than a sporadic or isolated event. In their view, situations falling below this threshold are categorized as internal disturbances and tensions. On the other hand, the International Criminal Tribunal for the former Yugoslavia (ICTY), in the Mucic case, found that „the existence of armed force between states is sufficient of itself to trigger the application of IHL"[20]. According to the ICRC, there is no stipulated minimum level of intensity for an IAC, as confirmed in the Commentary to Common Article 2 and Article 1 of API. Given that the objective of Common Article 2 is to provide the widest possible protection to the victims of war, the existence of an IAC does not require a minimum threshold of violence to ensure the applicability of the rules of IHL, thereby preventing any gaps in the protection afforded by international law.

3.2. NIAC in Cyberspace: Criteria and Challenges

A NIAC must meet certain requirements, as stated in the Tadic case. First, there must be a minimum level of intensity in the hostilities, and second, the non-governmental parties to the conflict need to be sufficiently organized.

In cyber warfare, no non-state actor cyberattack has ever been violent enough to cause a NIAC. Therefore, they don't include the kind of sustained armed violence required to achieve the threshold, and isolated cyber events like data theft or network attacks are inadequate to create a NIAC[21].

Another critical element is that a NIAC can only exist between well-organized parties capable of continuing military actions. It requires a distinct armed group with an identifiable organizational structure that can be seen and verified. However, it is challenging to demonstrate such an organization in cyber operations, given that cyberattacks are often conducted by loosely coordinated or even disorganized groups of hackers.

The basis for recognizing the presence of a NIAC is Common Article 3 of the 1949 GCs, which addresses „armed conflict not of an international

20 Prosecutor v. Zdravko Mucic aka „Pavo", Hazim Delic, Esad Landzo aka „Zenga", Zejnil Delalic (Appeal Judgement), IT-96-21-T, International Criminal Tribunal for the former Yugoslavia (ICTY), 16 November 1998. https://www.refworld.org/cases,ICTY,41482bde4.html. [assessed: 3.08.2023].

21 Melzer, supra, 13.

character occurring in the territory of one of the High Contracting Parties". However, this article provides no explicit definition of „armed conflict not of an international character". According to the ICTY, in the Tadic case[22], a NIAC arises „whenever there is protracted armed violence between governmental authorities and organized armed groups or between such groups within a state". The term „protracted" indicates a certain degree of intensity. Therefore, unlike an IAC, a NIAC requires a minimum level of organization and intensity among the parties involved.

Regarding the required intensity level, the ICTY suggested a variety of factors, including the number, length, and ferocity of individual encounters, as well as the kinds of weapons employed, number of casualties, amount of material destroyed, and UN Security Council involvement, to assess whether protracted armed violence exists. Under these intensity criteria, IHL applies to cyber operations during an ongoing NIAC. However, it is only under exceptional circumstances that stand-alone cyber operations would trigger a NIAC[23].

Second, there must be a minimum level of organization within the groups involved in the conflict. While state armed forces are presumed to meet this requirement, the criteria for non-state armed groups outlined by the ICTY include the existence of disciplinary rules, a command hierarchy, a headquarters, territorial control, access to weapons, military equipment, recruits, military training, a unified military strategy, military tactics, and the ability to negotiate agreements such as ceasefires or peace agreements.

In summary, there is no question that cyber operations carried out within the context of an ongoing IAC or NIAC are subject to IHL. Nevertheless, some challenges remain for standalone cyber operations. The criteria developed in case law to qualify a conflict as an IAC or a NIAC, mainly in relation to kinetic operations, are not entirely suitable for cyber operations. These criteria need to be adapted to cyberspace, especially those used to qualify a conflict as a NIAC. Existing thresholds, particularly the requirement of a minimum level of organization within groups engaged in hostilities, are inappropriate in cyberspace. The high threshold could result in stand-alone cyber operations never meeting the NIAC criteria, creating a legal vacuum

22 Prosecutor v. Dusko Tadic aka „Dule" (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction), IT-94-1, International Criminal Tribunal for the former Yugoslavia (ICTY), 2 October 1995. https://www.refworld.org/cases,ICTY,47fdfb520.html. [accessed: 7.08.2023].

23 Anthony Cullen, „The Concept of Non-International Armed Conflict", [in:] *International Humanitarian Law* (Cambridge: Cambridge University Press, 2010).

that leaves civilians unprotected during conflict. Given the lack of state practice on cyber operations, there is an obligation to establish well-defined criteria tailored to cyberspace in a cyber treaty.

4 Challenges to the Principle of Distinction in Cyberspace Warfare

The paramount obligation in the context of armed conflicts is to direct cyberattacks solely against military objectives and refrain from targeting civilian objects. Any object not a military objective is considered a civilian object under IHL. Military objectives are rigorously circumscribed, encompassing only objects that, by their nature, location, purpose, or use, substantially contribute to military actions, and depending on the situation, its partial or complete destruction, capture, or neutralization would result in an evident military advantage. Notably, under IHL, categorizing civilian infrastructure as 'critical infrastructure' bears no legal significance[24]. In the ICT realm, civilians and the military often share the same Internet infrastructure and utilize digital communication and storage services. It is known as „dual use". Suppose, however, that the civilian ICT infrastructure is instrumental in furthering military operations. In that case, it may become a military target. However, its use contributes significantly to military operations only under the following two conditions, and its destruction provides an obvious military advantage[25].

In the complex and interconnected domain of cyberspace, determining military advantage and civilian harm becomes complicated. Cyber operations can take diverse forms, and their compliance with the principle of distinction can be achieved in various ways. In scenarios where operators intrude into a target to execute operations, they possess situational awareness, facilitating compliance with the principle of distinction. In other

24 Mohammad Bitar, Chakka Benarji, „Drone attacks during armed conflict: quest for legality and regulation" International Journal of Intellectual Property Management , No. 3-4 (2023): 397-411. https://doi.org/10.1504/IJIPM.2023.134058.

25 Paul Ducheine, Terry Gill, *From Cyber Operations to Effects: Some Targeting Issues* (Dissertation, Militair Rechtelijk Tijdschrift, 2018), 39.

cases, cyber tools and malware may be employed[26]. These tools can be designed and programmed to exclusively target specific objects, avoiding indiscriminate harm. However, the inherent interconnectedness of cyberspace means that an operation aimed at one system may inadvertently affect others. It is essential that those planning or conducting cyber operations make reasonable efforts to determine the nature of their targets. This includes assessing the operational environment, testing cyber tools in simulated conditions, and putting technical safeguards in place like „kill switches", „system-fencing", and „geo-fencing" to prevent tools from spreading indiscriminately[27].

IHL rules governing the conduct of hostilities, including those derived from the principle of distinction, apply primarily to cyber operations considered as „attacks" under IHL. In the context of cyber operations, an attack is commonly understood as actions that may lead to injury or damage to people or property. Different states have varying interpretations regarding the effects of cyber operations that qualify as „attacks". While some countries take a broad stance, encompassing cyber operations that disrupt non-physical systems, others restrict it to physical damage. This diversity in interpretation has raised concerns, especially when non-physical cyber operations that significantly impact civilians or civilian infrastructure may go unregulated. To address this challenge, a comprehensive approach is needed to clarify the status of cyber operations under IHL, emphasizing their treatment as „attacks" regardless of the nature of the effects[28].

Even cyber operations not classified as „attacks" under IHL are not exempt from constraints during armed conflicts. IHL rules on necessity, civilian protection, protection of medical facilities, humanitarian relief, and the directive to direct operations exclusively against military objectives apply universally. Thus, it is crucial to prevent any potential erosion

26 Aaron Brantly, Max Smeets, „Military Operations in Cyberspace", [in:] *Handbook of Military Sciences* (Cham: Springer, 2020), 1-16. https://doi.org/10.1007/978-3-030-02866-4_19-1.

27 Michael N. Schmitt, „Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations" *International Review of the Red Cross*, No. 910 (2019): 333-355. https://doi.org/10.1017/s1816383119000018.

28 Elizabeth Mavropoulou, „Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyberattacks" *Journal of Law & Cyber Warfare*, No. 2 (2015): 23-93. https://doi.org/https://www.jstor.org/stable/26441253.

of civilian protection in cyberspace and ensure that military operations comply with distinction, necessity, and proportionality principles.

As we navigate the complex landscape of cyber warfare within the framework of IHL, the principle of distinction emerges as a linchpin in the protection of civilian lives and infrastructure. Developing a consensus on the characterization of cyber operations as „attacks", regardless of their physical or non-physical effects, is vital. In this fast-evolving digital arena, adhering to these fundamental principles of IHL is pivotal to preserving the sanctity of human life and protecting the vital civilian infrastructure on which modern society relies. The growing importance of autonomous artificial intelligence (AI) in warfare adds another layer of complexity to upholding the principle of distinction. While AI promises to reduce human error, it requires rigorous oversight and programming to ensure compliance with the principles of IHL, underscoring the importance of human responsibility in this evolving landscape.

In conclusion, ensuring that cyber warfare complies with IHL is an ongoing challenge that requires the attention of the international community. Adherence to the principle of distinction is non-negotiable, as it is the bedrock of humanitarian protection in armed conflict, whether waged in the physical or digital realm. Cyber operations must be subject to rigorous scrutiny and regulation, encompassing the „effects-based" approach and leaving no room for ambiguity concerning what constitutes an „attack". The principles of distinction, necessity and proportionality must remain at the forefront of discussions on cyber warfare in order to protect civilian lives and critical infrastructure. The dynamic development of AI in military operations requires careful evaluation to maintain ethical and legal standards in this ever-evolving landscape[29].

The principle of distinction embodies the world's commitment to preserving humanity amid the challenges of modern warfare. As technology continues to redefine the boundaries of conflict, upholding these principles is more important than ever.

29 James Johnson, „The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability" *Journal of Cyber Policy*, No. 3 (2019): 442-460. https://doi.org/10.1080/23738871.2019.1701693.

5 The Russian-Ukrainian conflict: Russian Cyberattacks and the Erosion of Distinction in Civilian Targeting

Since the onset of the armed conflict between Ukraine and Russia in February 2022, cyberattacks have become a significant component of the conflict. These cyber operations have targeted military and government networks and affected critical infrastructure and civilian entities. The consequences of such cyberattacks are far-reaching, potentially exposing the civilian population to harm and violating the fundamental principle of distinction under IHL.

5.1. Violations of the Principle of Distinction

5.1.1. DDoS Attacks on Civilian Entities

During the conflict, Distributed Denial of Service (DDoS) attacks have emerged as a prevalent cyberattack, constituting 88.8% of all incidents documented by the CyberPeace Institute. These attacks targeted various sectors, including public administration, media, ICT, finance, and transportation. Notably, civilian entities such as nonprofit organizations were not spared from these DDoS attacks, emphasizing the indiscriminate nature of these operations[30].

5.1.2. Phishing Campaigns Targeting Civilians

Various cyberespionage campaigns have been attributed to threat actors, including the Russian state-sponsored actor APT28. Phishing emails with deceptive subject lines and contents related to the ongoing conflict were used to compromise the devices of Ukrainian civilians and public administration entities. These attacks targeted government and civilian sectors, underscoring the challenges of distinguishing between combatants and non-combatants in cyberspace.

30 Goverment websites of Ukraine, Computer Emergency Response Team of Ukraine Cyberattack (CERT-UA), Distribution of Emails with „Instructions" on „updating the Operating System". cert.gov.ua, 28 April 2023. https://cert.gov.ua/article/4492467. [accessed: 20.08.2023].

5.1.3. Pro-Russian Hacktivist Collective: People's CyberArmy

During the second quarter of 2023, pro-Russian threat actors and hacktivist collectives accounted for a significant portion of the recorded cyber incidents. People's CyberArmy, in particular, claimed responsibility for numerous attacks, further complicating the attribution of these operations. The involvement of such hacktivist groups raises concerns about their affiliation and underscores the challenges in identifying and distinguishing between state-sponsored and non-state actors in cyberspace.

Table 1. Most sectors impacted by cyberattacks in Ukraine in 2023

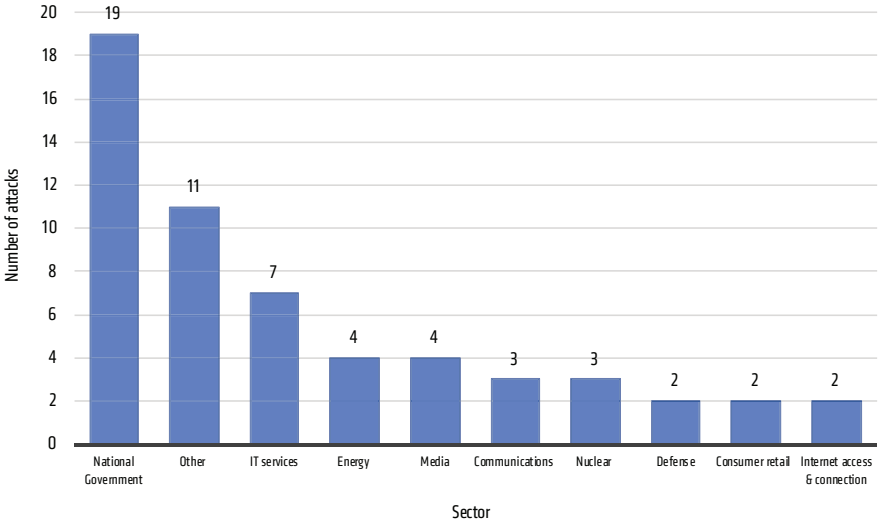
Sector	Number of Incidents	Effiction in Percentage
Public administration	31	55 %
Media	11	120%
ICT	11	10%
Financial	11	42.1%
Transportation	10	900%
Administrative/Sup	8	300%
Energy	7	40%
Trade	4	42.9%
Education	4	300%
Nonprofit	4	20%

Source: Computer Emergency Response Team of Ukraine (CERT-UA), 2023[31]

The table presents a breakdown of cyber incidents in different sectors, demonstrating the prevalence and impact of cyberattacks on various areas during the Ukraine conflict. Notably, the public administration sector faced the highest number of incidents, accounting for 55% of all cases. In contrast, the financial sector experienced a decrease in attacks, with a decline of 42.1%, while the transportation sector saw a staggering 900% increase in incidents, highlighting the dynamic nature of cyber warfare's impact on different sectors. In addition, the table shows the significant involvement of non-profit organizations and educational institutions, both of which were affected by cyber incidents, with a 300% increase in each category, underscoring the indiscriminate reach of such attacks across civilian sectors.

31 Ibidem.

Chart 1: The cyberattacks that targeted Ukraine, which Russia launched following the commencement of the war, were categorized by sector.



Source: Microsoft[32]

The chart shows the breakdown of Russia's cyberattacks on Ukraine since the start of the war, categorized by sector and number of attacks. Analyzing the data, several key observations can be made:

National Government: This sector experienced the highest number of cyber-attacks, with nineteen recorded incidents. Directly targeting the national government is a significant concern, as these attacks can disrupt government operations, compromise sensitive information, and undermine the functioning of a sovereign state.

Other: The „Other" category of eleven attacks suggests that various unspecified sectors were also targeted. It is imperative that these sectors be identified in order to understand the scope of the attacks and better assess their impact.

IT Services: With seven attacks, IT services suffered considerable cyber intrusions. Since IT services are the backbone of many critical systems, attacks in this sector can have widespread repercussions, affecting other industries as well.

32 Microsoft, *An Overview of Russia's Cyberattack Activity in Ukraine Report*, April 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Energy: With four attacks, the energy sector includes critical infrastructure such as power plants and utilities. Targeting this sector can lead to disruptions in energy supply, impacting civilian life and essential services.

Media: With four attacks, the media sector plays a crucial role in providing information to the public. Targeting media outlets can hamper the flow of accurate information, potentially causing misinformation and chaos.

Communications: Cyber-attacks on communication infrastructure (3 attacks) can disrupt essential communication networks, affecting the government, military, and civilian populations.

Nuclear: The nuclear sector was targeted three times. Any cyber intrusion in this sector raises serious concerns, as it can potentially impact nuclear safety and security, endangering civilians and the environment.

Defense: Although two attacks were reported in the defense sector, such attacks can have serious implications, compromising national security and the safety of civilians.

Consumer Retail: While the consumer retail sector (2 attacks) may not seem critical at first glance, targeting these areas can affect the economy and consumers' access to goods and services, indirectly impacting civilian life.

Internet Access & Connection: Cyber-attacks on internet access and connection infrastructure (2 attacks) can severely disrupt communication and connectivity for the civilian population, affecting their daily lives.

In conclusion, the data from these cyber-attacks indicates that the Russian actions have not respected the principle of distinction. By targeting a wide range of sectors, including national government, IT services, energy, media, and nuclear facilities, the attacks have breached the fundamental principle of IHL, which obligates belligerents to distinguish between civilian and military targets. The indiscriminate targeting of these sectors poses a grave risk to civilian lives, critical infrastructure, and essential services, underscoring the need to strengthen IHL to address the evolving cyber warfare landscape and enhance the protection of non-combatants.

5.2. Impacts on Civilian Population

5.2.1. Destructive Cyberattacks

Some cyberattacks led to destructive outcomes, exemplified by the deployment of wiper malware. These attacks resulted in the deletion of data and damage to systems, making recovery impossible. One notable case was the wiper attack on a border control station, which slowed the process of allowing refugees to cross into neighboring countries. These actions

directly affected civilians and critical infrastructure, highlighting the risks they face in cyber conflict.

5.2.2. Disruptive Attacks on Critical Infrastructure

Cyberattacks targeting critical infrastructure, including public administration, energy, ICT, and finance, had far-reaching implications. They disrupted the provision of essential services and connectivity, affecting the civilian population's access to vital resources. Disruption of these services illustrated the potential harm inflicted on non-combatants[33].

5.2.3. Data Weaponization and Disinformation

The theft and leak of data, driven by data weaponization tactics, had a profound impact. Hack and leak operations expose sensitive information, potentially placing individuals at risk. Moreover, disinformation and propaganda hindered the civilian population's access to accurate information, potentially inciting misunderstandings, conflicts, and human rights violations[34].

5.3. Concluding Remarks

The case study of cyberattacks during the conflict in Ukraine serves as a stark example of the challenges and violations of the principle of distinction in cyberspace. The indiscriminate nature of cyber operations, their potential to disrupt critical infrastructure and essential services, and the blurring of distinctions between non-state and state-sponsored actors underscore the urgent need to address these issues within the framework of IHL. Adapting IHL to the evolving landscape of cyber warfare is critical to ensuring that the principle of distinction is respected and that civilians are protected in armed conflict.

As cyberattacks increasingly become a tool of warfare, the international community must recognize the imperative of addressing the unique challenges posed by these operations and upholding the principles of IHL to protect civilians and civilian infrastructure in an interconnected and vulnerable digital world.

33 CERT-UA supra 29.
34 Schmitt, „Wired Warfare 3.0", 333-355.

6 Conclusion and Recommendation

The principle of distinction, deeply embedded in the fabric of IHL, serves as one of the oldest and most fundamental tenets of human civilization's endeavor to humanize the horrors of warfare. Recognized by the International Court of Justice as a „cardinal" and „intransgressible" principle, it has historically guided the conduct of warfare. In the rapidly evolving landscape of modern warfare, however, cyberspace presents complex challenges that require careful consideration. As we have explored, the application of the principle of distinction in cyber warfare encounters many complexities that the international community must confront.

Unlike traditional warfare, cyber warfare occurs within a borderless, interconnected, and often ambiguous realm. The interconnectedness and „dual-use" nature of cyberspace make it exceedingly challenging to distinguish between civilian and military objects, combatants, and non-combatants. Distinguishing between combatants and civilians in cyberspace, a crucial aspect of the principle of distinction becomes increasingly elusive due to the shared nature of information technology networks and the civilian expertise essential for their operation. The principle of „direct participation in hostilities" in cyberspace remains open to interpretation. It presents blurred lines, where actions as diverse as designing a computer program for cyberattacks and financing military operations may be considered direct participation.

The blurring of lines extends to the classification of cyber objects as civilian or military. The dynamic nature of cyberspace and the unpredictable consequences of cyber operations make the application of traditional IHL definitions of military objectives and civilian objects problematic. Cyberspace does not fit neatly into established categories, potentially putting essential civilian infrastructure at risk during armed conflict.

In light of these challenges, there is an urgent need to address several critical aspects of the principle of distinction in cyberspace warfare. The first is a comprehensive evaluation of cyber operations to determine when they should be considered 'attacks' under IHL. The principle of distinction primarily applies to „attacks" that may result in injury or damage to people or property. The diversification of cyber operations necessitates clear criteria for determining which cyber activities qualify as „attacks", regardless of their physical or non-physical effects. This clarification would ensure that the principle of distinction is consistently applied.

In addition, the inherent interconnectedness of cyberspace requires that those planning or conducting cyber operations take appropriate measures to minimize indiscriminate harm. These measures should include an in-depth assessment of the operational environment, the simulated testing of cyber tools, and the implementation of technical mechanisms to control and confine the effects of these tools, such as „system-fencing", „geo-fencing", and „kill switches".

The integration of autonomous AI systems into warfare further underscores the importance of ensuring compliance with the principle of distinction. While AI has the potential to reduce human error, the responsibility for programming and controlling AI systems in warfare should be robustly governed by ethical and legal standards.

The case study of cyberattacks in the ongoing conflict in Ukraine reveals a troubling trend. Russian cyber operations, including DDoS attacks, phishing campaigns, and destructive malware deployments, indiscriminately targeted critical civilian infrastructure and organizations. The evident blurring of lines between state-sponsored actors and hacktivist collectives further complicates the attribution of these attacks. These actions contravene the fundamental principle of distinction under IHL, as civilians and civilian objects have been directly affected. It underscores the urgent need to adapt and reinforce IHL to address the evolving landscape of cyber warfare, prioritizing the protection of non-combatants and their vital infrastructure during armed conflicts.

In conclusion, the principle of distinction remains non-negotiable in the ever-evolving landscape of modern warfare, regardless of whether it unfolds in the physical or digital realm. As technology continues to redefine the boundaries of conflict, upholding these principles becomes more crucial than ever. The international community must be responsible for adapting IHL to the intricacies of cyberspace to preserve the sacredness of human life and protect the vital civilian infrastructure upon which modern society depends. Addressing the challenges to the principle of distinction in the context of cyber warfare is a task that demands the concerted efforts of policymakers, legal experts, and the global community. The core principles of IHL, including the principle of distinction, stand as our collective commitment to preserving humanity in the face of the ever-advancing frontiers of warfare. Furthermore, enhancing cybersecurity education and awareness is a fundamental step toward strengthening the application of the principle of distinction in cyber warfare. By equipping both military and civilian stakeholders with the knowledge and tools to navigate the

complexities of cyberspace, it is possible to promote compliance with IHL, protect civilian lives and infrastructure, and adapt to the evolving nature of conflicts in the digital age. This Recommendation is consistent with the overarching goal of preserving humanity amidst the challenges of modern warfare, as the principle of distinction remains a pillar of IHL in both the physical and digital realms.

Bibliography

Alberts David Stephen, John Garstka, Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP Publication, 2005.

Biggio Giacomo, „International Humanitarian Law and the Protection of the Civilian Population in Cyberspace: Towards a Human Dignity-Oriented Interpretation of the Notion of Cyber Attack under Article 49 of Additional Protocol I" *The Military Law and the Law of War Review*, No. 1 (2021): 114-140. https://doi.org/10.4337/mllwr.2021.01.06.

Bitar Mohammad, Benarji Chakka, ,,Drone attacks during armed conflict: quest for legality and regulation" International Journal of Intellectual Property Management , No. 3-4 (2023): 397-411. https://doi.org/10.1504/IJIPM.2023.134058.

Brantly Aaron, Max Smeets, „Military Operations in Cyberspace", [in:] *Handbook of Military Sciences*. 1-16. Cham: Springer, 2020). https://doi.org/10.1007/978-3-030-02866-4_19-1.

Cyberspace and Instability, ed. Robert Chesney, James Shires, Max Smeets. Edinburgh: Edinburgh University Presss, 2023.

Cullen Anthony, The Concept of Non-International Armed Conflict [in:] *International Humanitarian Law*. Cambridge: Cambridge University Press, 2010.

Ducheine Paul, Terry Gill, *From Cyber Operations to Effects: Some Targeting Issues*. Dissertation, Militair Rechtelijk Tijdschrift, 2018.

Geist Edward, „Deterrence Stability in the Cyber Age" *Strategic Studies Quarterly*, No. 4 (2015): 44–61. https://doi.org/https://www.jstor.org/stable/26271277.

Gervais Michael, „Cyberattacks and the Laws of War" *SSRN Electronic Journal*, (2011). https://doi.org/10.2139/ssrn.1939615.

Government websites of Ukraine, Computer Emergency Response Team of Ukraine Cyberattack (CERT-UA), Distribution of Emails with „Instructions" on „updating the Operating System". cert.gov.ua, 28 April 2023. https://cert.gov.ua/article/4492467.

ICJ, *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996. https://www.icj-cij.org/case/95.

Igakuboon Adasi Nsanawaji, „An Appraisal of the Legal Framework for the Protection of Civilians in Cyber-Warfare under International Humanitarian Law" *International Journal of Research and Scientific Innovation*, No. 7 (2022): 14-26. https://doi.org/10.51244/ijrsi.2022.9702.

International Committee of the Red Cross (ICRC), Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977

International Committee of the Red Cross, International Humanitarian Law and Cyber Operations during Armed Conflicts, 27 October 2022. https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts.

Johnson James, „The AI-Cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability" *Journal of Cyber Policy*, No. 3 (2019): 442-460. https://doi.org/10.1080/23738871.2019.1701693.

Joint Inspection Unit of the United Nations System, Cybersecurity in the United Nations System Organizations (JIU/REP/2021/3)., 2021. https://www.unjiu.org/news/cybersecurity-united-nations-system-organizations-jiurep20213-0.

Mathonet Clara, *Protection of Civilians in the Era of Cyber Warfare: A Critical Analysis of International Humanitarian Law Towards a Treaty Restricting the Use of Cyber Weapons*. Thesis, University of Amsterdam, 2020.

Mavropoulou Elizabeth, „Targeting in the Cyber Domain: Legal Challenges Arising from the Application of the Principle of Distinction to Cyberattacks" *Journal of Law & Cyber Warfare*, No. 2 (2015): 23-93. https://doi.org/https://www.jstor.org/stable/26441253.

McDonald Jack, „Blind Justice? The Role of Distinction in Electronic Attacks" *Ethics and Policies for Cyber Operations*, (2016): 17-32. https://doi.org/10.1007/978-3-319-45300-2_2.

Melzer Nils, „The Principle of Distinction Between Civilians and Combatants", [in:] *The Oxford Handbook of International Law in Armed Conflict*, ed. Andrew Clapham, Paola Gaeta. 296-331. Oxford: Oxford University Press, 2014. https://doi.org/10.1093/law/9780199559695.003.0012.

Microsoft, *An Overview of Russia's Cyberattack Activity in Ukraine Report*, 22 April 2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

Richmond Jeremy, „Evolving Battlefields: Does Stuxnet Demonstrate a Need for Modifications to the Law of Armed Conflict?" *Fordham International Law Journal*, No. 3 (2012): 842-894. https://doi.org/https://ir.lawnet.fordham.edu/ilj/vol35/iss3/1.

Rid Thomas, Peter McBurney, „Cyber-Weapons" *The RUSI Journal*, No. 1 (2012): 6-13. https://doi.org/10.1080/03071847.2012.664354.

Schmitt Michael N., „Wired Warfare 3.0: Protecting the Civilian Population During Cyber Operations" *International Review of the Red Cross*, No. 910 (2019): 333-355. https://doi.org/10.1017/s1816383119000018.

Schmitt Michael N., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press, 2017.

Shackelford Scott J., „From Nuclear War to Net War: Analogizing Cyberattacks" *International Law*, No. 1 (2009): 191-250. https://doi.org/https://dlc.dlib.indiana.edu/dlc/bitstream/handle/10535/10239/SSRN-id1396375.pdf.

Sharma Amit, „Cyber Wars: A Paradigm Shift from Means to Ends" *Strategic Analysis*, No. 1 (2010): 62-73. https://doi.org/10.1080/09700160903354450.

Sohail Humna, „Fault Lines in the Application of International Humanitarian Law to Cyberwarfare" *Journal of Digital Forensics, Security and Law*, (2022). https://doi.org/10.15394/jdfsl.2022.1761.