




Open Access Article

 <https://doi.org/10.35741/issn.0258-2724.59.1.21>

Research article

Social Sciences

NAVIGATING MODERN WARFARE CHALLENGES: A REVIEW OF THE EVOLUTION OF INTERNATIONAL HUMANITARIAN LAW IN CYBERWARFARE

应对现代战争挑战：网络战国际人道主义法演变回顾

Shafiq Ur Rahman ^a, Mahmood Ahmed Shaikh ^a, Muhammad Tahir ^b, Imran Naseem ^c, Sriyanto Sriyanto ^d,
Nur Fatihah Abdullah Bandar ^e, Khalid Zaman ^{f,*}

^a Bahria University Law School, Bahria University
Islamabad, Pakistan, shafiq1971@gmail.com

^b School of Law, Karachi University
Karachi, Pakistan, drtahir949@gmail.com

^c Department of Pakistan Studies and International Relations, Abbottabad University of Science and Technology
Abbottabad, 22620, Pakistan, drimran.naseem@aust.edu.pk

^d Social Studies Department, Universitas Muhammadiyah Purwokerto
Jawa Tengah, 53182, Indonesia, sriyanto1907@gmail.com

^e Faculty of Cognitive Sciences and Human Development, Universiti Malaysia Sarawak
Kota Samarahan, 94300, Sarawak, Malaysia, abnfatihaa@unimas.my

^f Department of Economics, The University of Haripur
Haripur, Khyber Pakhtunkhwa, 22620, Pakistan, khalid_zaman786@yahoo.com

* Corresponding author: khalid_zaman786@yahoo.com.

Received: December 15, 2023 ▪ Reviewed: January 9, 2024
▪ Accepted: February 17, 2024 ▪ Published: February 29, 2024

Abstract

The need for states to discuss treaty making in the domain of cyber warfare emerges from complexities and obstacles concerning cyber operations. The Tallinn Handbook provides valuable guidance, but it is not a treaty; hence, the manual is not a binding document. There can be differing interpretations and practices among states regarding the application of international law to disputes involving cyberspace. To address these discrepancies and encourage more collaboration in cyber activities, there is a growing recognition of the need for states to engage in discussions and negotiations on the establishment of treaties around the world specific to warfare in cyber space. Treaty-making can bring about more concrete and binding governance to elucidate the states' rights and obligations, uphold transparency, and create standards of conduct in cyberspace. This study offers a thorough analysis of the evolutionary trajectory of International Humanitarian Law (IHL) to solve problems resulting from innovative modes of the warfare. It explicitly focuses on the regulation of cyber warfare and identifies



and evaluates key provisions and mechanisms within IHL relevant to this context. This research assesses the adequacy of existing IHL provisions in effectively governing cyber warfare and proposes essential advancements or amendments to address the gaps in law and complications connected to this evolving from the issues therein. The study offers insights into how IHL can adapt to the demands of the modern battlefield, particularly in the domain of cyber warfare. Two potential paths can be underscored for resolution of the issue in hand: the creation of a dedicated treaty for cyber-armed conflicts or the evolution of state practices into binding customs. In this evolving landscape, interpreting existing IHL provisions and their use in cyber warfare remains crucial to maintain alignment with the underlying humanitarian principles of IHL. The study initially anticipates continued engagement in damaging cyber conflicts driven by a cyber-arms race, which might ultimately lead to the development of new norms, albeit over an extended period. Treaty-making is the best way to deal with the situation provided state parties to IHL make a collaborative endeavor in this behalf.

Keywords: International Humanitarian Law, cyberwarfare, Geneva Conventions, Additional Protocols, warfare challenges

摘要 由于网络行动的复杂性和障碍，各国需要讨论网络战领域条约的制定。《塔林手册》提供了宝贵的指导，但它不是一项条约；因此，该手册不是具有约束力的文件。各国对于国际法适用于涉及网络空间的争端可能有不同的解释和做法。为了解决这些差异并鼓励网络活动方面的更多合作，人们越来越认识到各国有必要参与讨论和谈判，以在世界各地建立专门针对网络空间战争的条约。条约的制定可以带来更具体和有约束力的治理，以阐明国家的权利和义务，维护透明度，并制定网络空间的行为标准。本研究对国际人道法(国际人道法)的演变轨迹进行了全面分析，以解决创新战争模式带来的问题。它明确关注网络战的监管，并确定和评估国际人道法中与此相关的关键条款和机制。这项研究评估了现有国际人道法条款在有效管理网络战方面的充分性，并提出了重要的进步或修正案，以解决法律上的空白以及与此相关的问题所带来的复杂性。该研究深入探讨了国际人道法如何适应现代战场的需求，特别是在网络战领域。可以强调解决当前问题的两条潜在途径：制定专门针对网络武装冲突的条约或将国家实践演变为具有约束力的习惯。在这个不断变化的形势下，解释现有国际人道法条款及其在网络战中的使用对于保持与国际人道法基本人道原则的一致性至关重要。该研究最初预计，网络军备竞赛引发的破坏性网络冲突将继续参与，这可能最终导致新规范的制定，尽管需要很长一段时间。只要国际人道法缔约国为此共同努力，缔结条约是处理这种情况的最佳方式。

关键词: 国际人道法、网络战、日内瓦公约、附加议定书、战争挑战

I. INTRODUCTION

The international legal experts trace humanitarian law within a broader historical context encompassing various codes of warfare such as the Hammurabi Code that have spanned different periods and cultures. The noteworthy contribution toward the advancement of international humanitarian law (IHL) was made by Swiss-based businessman Henry Dunant (1787–1875) who happened to witness the battlefield of Solferino and was greatly affected by the major humanitarian crisis he observed. According to Palmieri [1], Dunant founded the International Committee of the Red Cross (ICRC) in February 1863. His actions marked the

inception of the tradition contributing to the establishment of the Geneva Conventions in 1864, 1906-1929, and 1949 (the Geneva Conventions 1949, 1125 UNTS 3). The term “IHL” made its debut during the 1970s, emerging from collaborative efforts by diverse stakeholders with varying objectives. This novel concept of IHL found formal expression through its codification in the Additional Protocols of 1977 to the Geneva Conventions. World War I (1914-1918) witnessed the use of large-scale and unprecedented methods of warfare that included the deployment of poisonous gas during war, the beginning of aerial bombardments, and the arrest of hundreds of thousands of prisoners. These innovations and tactics marked a significant

departure from previous conflicts and contributed to the unique and disastrous nature of World War I. Therefore, the international community adopted the following additional convention protocols. In WWII (1939-1945), the causality rate of civilian-military personnel was 50:50 against the ratio of 1:10 in WWI. The fourth Geneva Convention was created in 1949 as a new instrument for the protection of civilians by the international community in response to the horrifying impacts of war on people and the startlingly high death toll [2].

A. Scope of the Study

This study encompasses an analysis of the evolutionary path of IHL concerning its adaptation to confront emerging challenges posed by innovative modes of warfare. It also delves into the identification and evaluation of the key provisions and mechanisms embedded within IHL that are specifically relevant to the regulation of cyber warfare. A particular emphasis is placed on assessing whether the existing IHL provisions are adequate in effectively governing the complex realm of cyber warfare. This research further investigates and proposes essential developments or amendments within IHL. This exploration is prompted by the escalating phenomenon of cyber warfare and aims to address the associated legal gaps and challenges inherent in this evolving form of conflict. In addition, this study seeks to offer insights into how IHL can evolve to meet the demands of the modern battlefield.

B. Research Questions

The study formulated the following three research questions for investigation and analysis. They have been carefully crafted to facilitate a comprehensive examination of the topic and offer a framework for addressing core issues related to IHL and its adaptation to the challenges presented by modern warfare, particularly cyberwarfare:

1. How has IHL evolved in response to the issues brought about by novel forms of warfare?
2. What are the key provisions and mechanisms within IHL that pertain to regulating cyber warfare? Are the existing provisions in IHL adequate to effectively regulate and govern cyber warfare?
3. What specific developments or amendments, if any, in IHL need to be reviewed to address issues arising from the emergence of cyber warfare?

C. Research Objectives

Based on the three stated research questions, three research objectives of the study are as follows:

1. To analyze the evolution of IHL in addressing emerging challenges presented by innovative modes of warfare;
2. To identify and evaluate the essential provisions and mechanisms in IHL related to the regulation of cyber warfare, with a focus on determining the sufficiency of existing IHL provisions in effectively governing cyber warfare;
3. To review and propose necessary developments or amendments within IHL in response to the growing phenomenon of cyber warfare, with the aim of addressing the legal gaps and challenges associated with this evolving form of conflict.

D. Literature Review

This study's literature review is divided into two parts to aid readers in grasping the material thoroughly. To better understand how IHL has developed and how it relates to the problems posed by cyber warfare, this research splits the literature review into two parts. This tack will help readers understand how IHL came to be and how it is now being used to deal with the intricacies of modern combat, especially in the cyber arena.

This section examines the historical progression of IHL. Viewed through this historical lens, the progress of IHL in response to the changing dynamics of armed conflict and new difficulties becomes clear. It sheds light on the guiding ideas and conventions that have molded IHL and aided its adaptation to changing conflict dynamics. For ease of understanding, the main treaties that set the pace for IHL are discussed below:

- a) The First Geneva Convention for the Amelioration of the Condition of the Wounded in Armies in the Field, 1864, was a response to the behavior of belligerents after the 2nd Italian War of Independence (29 April 1859–11 July 1859) fought by the 2nd French Empire and the Savoyard (also known as Franco-Austrian War, Sardinian War, or Austro-Sardinian War). The French victory in the Battle of Solferino on June 24, 1859, ended the war. Swiss businessman Henry Dunant (1828-1910), who happened to witness the Battlefield of Solferino, saw the devastating effects of war. After returning to Geneva, he wrote a book "A Memory of Solferino in 1862", which paved the way for 13 states' envoys to gather and adopt at Geneva on August 22, 1864.

b) Later St. Petersburg Declaration of 1868 aimed at prohibiting the use of certain projectiles in wartime.

c) The conventions on the laws and customs of war on land and the application of the principles of the 1864 Geneva Convention to maritime warfare were enacted in the Hague in 1899.

d) In 1906, the Geneva Convention of 1864 was reviewed for further developments. In 1907, the Hague Conventions of 1899 were reviewed, and working for the adoption of new conventions was discussed.

e) Worldwide, people saw the emergence of new, massive forms of combat during World War I, which lasted from 1914 to 1918. The introduction of poisonous gas during the war, the beginning of aerial bombardments, and the arrest of hundreds of thousands of prisoners during the war were all notable advances during this fight. These innovative approaches marked a radical change from previous battles and contributed to the unique and catastrophic nature of World War I. In 1925, the international community unanimously ratified the Geneva Protocol, which prohibits the use of asphyxiating, poisonous, or other gases and bacteriological methods of warfare. In 1929, two further agreements were appended to the 1906 Geneva Convention, resulting in the renaming of the collective set as the Geneva agreements with the purpose of reviewing and enhancing the original 1906 Convention, as well as addressing the treatment of prisoners of war. These actions were implemented in response to emerging risks.

f) The death toll took a dramatic turn during World War II (1939–1945), with citizens and service members losing lives at a rate of approximately one to one. This was a radical change from the 1:10 ratio during World War I. The entire community stepped forward in reaction to the shocking number of casualties and the devastating effect of war on civilian populations. The Fourth Geneva Convention, a new legal document, was adopted in 1949 after altering previous agreements. This convention was specifically designed to ameliorate the condition of wounded and sick military personnel in the field (GC-I), the situation of sick, wounded, and shipwrecked military personnel at sea (GC-II), handle prisoners of war (GC-III), and enhance the safeguarding of civilians during armed conflict (GC-IV).

g) The 1954 Hague Convention was established to safeguard cultural property during times of armed conflict.

h) In 1972, the world community ratified a

convention that prohibits the development, production, and stockpiling of bacteriological (biological) and toxin weapons and mandates their destruction.

i) The Sanctions Convention of 1976 forbade the use of environmental modification techniques in hostile contexts, whether military or otherwise.

j) In 1977, two Additional Protocols were adopted in reaction to the human-cost effects of national liberation wars, which common Article 3 of the 1949 Conventions only partially addressed. The two 1949 Geneva Protocols that were added to the four original Conventions focused on enhancing victim protection and non-international armed conflicts.

k) The Red Crescent and Red Cross signs have served as universal symbols of aid to those who have been harmed in armed wars since the 19th century. The introduction of the red crystal emblem marks a new milestone in their extensive history of IHL by adopting an additional distinctive emblem (Protocol III) on December 8, 2005.

l) The Tallinn Manual [3] was developed by NATO's Cooperative Cyber Defense Centre of Excellence (CCDCOE) to respond to cyber operations violating the use of force and self-defense rules. In 2017, the Tallinn Manual 2.0 expanded the examination of international law governing everyday cyber incidents that do not escalate up to the point of use of force or hostilities.

In this section, we examine the current problems with cyber warfare as they pertain to IHL. Cyberwarfare has become more significant in contemporary combat situations, and this article delves into the peculiarities and nuances of this emerging field. It also addresses the issue of whether the current rules and procedures of IHL are sufficient to control and regulate cyberwarfare. Here, we narrow our emphasis to works published in 2017 and after to address the issues that have arisen since the release of the Tallinn Manual 2.0 in 2017.

The study is divided into three parts corresponding to the established objectives after describing the research goals and the research goals of the research questions and evaluating the current literature. These three parts, taken as a whole, will shed light on the study's aims and help us comprehend how IHL is changing to meet the demands of contemporary combat, especially in cyber operations. Section 2 will assess the historical evolution of IHL concerning its responses to emerging challenges posed by innovative modes of warfare. This part of the research provides a comprehensive understanding

of how IHL has adapted to confront the changing landscape of warfare. Section 3 focuses on identifying and evaluating the core provisions and mechanisms within IHL related to the regulation of cyber warfare. This evaluation emphasizes the sufficiency of existing IHL provisions in effectively governing the complex domain of cyber warfare.

Before concluding and putting forth recommendations, Section 4 reviews and implores specific changes or additions within IHL. These proposals address the evolving challenges and legal gaps associated with cyber warfare. By doing so, this study contributes to the ongoing discourse on adapting IHL to this contemporary form of conflict.

II. IHL RESPONSE TO THE CHALLENGES OF NOVEL FORMS OF WARFARE

Throughout history, technology has continually advanced to create more sophisticated tools for warfare. In the modern era, which began after the French Revolution, systematic scientific research has fueled technological innovation, impacting both civilian and military realms. The European powers used their technological edge to conquer and colonize other nations. Dunant [4] posited that if a nation's acquisition of advanced and formidable weaponry leads to shorter durations of future battles, such wars are likely to become more violent and result in more bloodshed.

A. Novel Warfare at a Glance

The present post-modern or knowledge age is witnessing an unprecedented technological revolution, influencing both civil and military domains. This article delves into current technological trends in warfare and briefly touches on anticipated future technologies [5]. The emergence of ironclad ships during the 1860s, the invention of the machine gun in the 1890s, the introduction of manned aircraft and tanks in the 1920s–1930s, the advent of aircraft carriers and radar in the 1930s–1940s, and the development of nuclear weapons in the 1940s–1950s represent significant milestones in the progression of military technology. Each of these advancements brought about revolutionary changes in the conduct of warfare. According to Toffler and Toffler [6], how we wage war reflects our approach to generating wealth. Unprecedented destructive power was brought about by the development of nuclear weapons in the 1940s and 1950s. In parallel with the function

of mass manufacturing in economies, the war plans of the Warsaw Pact and NATO armies centered on attrition warfare. The impact of technology on ground combat led to this shift in military philosophy. Moving away from weapons of mass destruction toward precision-based combat was the Gulf War in the 1990s. This heralded the Third Wave of combat, which focused on tactics informed by information and emphasized movement. The confrontation highlighted the use of advanced weapon systems and enhanced surveillance, showcasing the lightning-fast advancements in combat technology.

B. Hybrid Warfare

Hybrid warfare presents new challenges to modern military strategy. It combines technological advancements, information warfare, battlefield digitization, and conventional modernization. Instead of standalone military options, it involves the coordinated use of all “elements of national power” across a range of activities, from stability to armed conflict. In the context of Pakistan, hybrid warfare, primarily driven by challengers such as India, aims to weaken, subjugate, or destabilize the country, making it a critical subject of analysis and concern. The 2006 Israel–Hezbollah conflict typified hybrid warfare, where Hezbollah integrated political activities with decentralized resistance forces operating among civilian populations [7]. The term “hybrid war” was coined in the aftermath of the same conflict [8]. Hybrid warfare, similar to conventional conflict, seeks to establish dominance over the adversary. When executed skillfully and in the right combination, the tools of hybrid warfare, which encompass regular military forces, economic pressure, diplomacy, proxy utilization, inciting local unrest, information warfare, and cyber attacks, can generate significant disruptions within the targeted state, whether at home or abroad. This approach's unique advantage lies in its ability to engage every element of the adversary, allowing the initiator to circumvent the UN Laws and Geneva Conventions related to upholding fundamental human rights and safeguarding non-combatants [3]. The conflict continuum in a hybrid environment can be categorized into four stages:

I. *Orchestrated instability*: internal fissures and structural inadequacies exploited to destabilize the inner front;

II. *Proxy sanctum*: use of proxies to undermine stability;

III. *Coercion*: military movements and

exercises, overt threats to intimidate, economic coercion;

IV. *Coup de grace*: use of a military instrument to give a final blow.

C. Information Warfare

The information age has brought forth a shift in military strategy, emphasizing domination of information systems for achieving military objectives. This approach relies on a fusion of technologies to enhance combat efficiency, including surveillance instruments, integrated information inside armaments, and artificial intelligence. Several countries are allocating their defense budgets toward information dominance platforms in response to the widespread use of data-intensive electronic components in contemporary weapons systems. Cyber attacks targeting both civilian and military networks may have significant consequences, even if they do not cause any physical harm. In this digitized battlefield, IW involves accessing, tampering with, and exploiting the adversary's information while defending against similar actions. The electromagnetic spectrum is now a critical battleground, and future wars may prioritize psychological paralysis over force destruction or territorial capture. Armed forces seek to establish "information deterrence" alongside nuclear and conventional deterrence against potential adversaries [5].

D. Artificial Intelligence (AI)

AI has become a fundamental part of our daily lives, impacting various sectors such as healthcare, education, finance, and entertainment. AI, particularly machine learning, can have a profound societal impact by making decisions that affect individuals and communities, which raises ethical concerns. With AI's continuous evolution, there is a growing need for effective governance mechanisms to manage its use and address potential risks. Ensuring impartiality and preventing biases in AI systems, ensuring transparency in AI decision-making, safeguarding privacy in data-driven AI, and fostering expertise in both technical and regulatory aspects are crucial aspects of AI governance. Regulating AI is a complex task because of its technical intricacies, rapid development, and widespread application across industries. Regulatory frameworks must strike a balance between fostering innovation and preventing potential harm. They should emphasize accountability, transparency, and fairness in AI systems while also encouraging competition and deterring misuses [9].

E. IHL and Ethical Concerns

The ICRC [10] engaged in discussions concerning AI and the contentious matter of "killer robots," addressing appeals from specific nations and advocacy organizations to prohibit these weapons. According to the ICRC, it is imperative to retain human control over weapon systems and the application of force to guarantee adherence to international law and address ethical considerations. Therefore, states are urged to collaborate promptly in defining constraints on autonomy within weapon systems. The US official stance (9 April 2018) on ethical concerns of AI is that it endorses IHL as an effective framework for regulating all weapons, including autonomous ones, in armed conflict. They emphasize the importance of IHL principles such as necessity, humanity, distinction, and proportionality in the development and use of such weapons. The USA views autonomy and machine learning as tools to improve IHL implementation, thereby reducing risks to civilians and friendly forces. Acknowledging the complexity of issues related to lethal autonomous weapons systems (LAWS), they advocate a cautious, evolving approach rather than supporting immediate negotiations for a binding agreement. Steinhoff [11] hinted that from a worldwide standpoint, there have been debates about the need for proactive international prohibitions on AI-powered lethal autonomous weapon systems due to ethical apprehensions surrounding these advanced technologies. Detractors of these lethal weapon systems emphasize a range of ethical issues, including operational hazards, fragmented accountability, and the appropriateness of their deployment in times of armed conflict. The primary concern pertains to aspects such as human supervision, the capacity to intervene and deactivate the system, the technical prerequisites for predictability and dependability, including the algorithms employed, and operational restrictions covering the weapon's intended function, the nature of the target, the operational setting, the time frame of activity, and the extent of mobility within an area. To uphold ethical and legal standards, comparable limitations on autonomy within weapon systems may be required to ensure that a substantial degree of human oversight is retained.

F. Cyber Attacks

Cyber warfare, an emerging field in computer science, has the capacity to disrupt power grids, cripple economies, and incite political turmoil.

Various entities are engaged in cyber warfare, ranging from nation states to individual hackers. Cyber warfare attacks encompass techniques, targets, and consequences. There are many economic, socio-political, and infrastructure ramifications resulting from cyber warfare. Strategies are needed to mitigate the harm caused by such attacks, emphasizing the significance of gleaned insights from these tactics and offering recommendations to forestall future cyber threats [12].

III. IHL PROVISIONS REGULATING CYBERWARFARE

IHL consists of the Geneva Conventions 1949 and their Additional Protocols of 1977 and 2005. None of these documents have any mention of the term ‘cyber.’

A. The Geneva Conventions and Additional Protocols

In this section, we explore how IHL regulates cyber operations to prevent violations of international law. International law plays a vital role in assessing the legality of new weapons and ensuring compliance with international obligations. States are to ensure that new weapons comply with IHL (Art 36 of the 1977 Protocol I to the Geneva Conventions). States parties to the Geneva Conventions have called for rigorous and multidisciplinary reviews of new weapons to prevent technological advancements from undermining legal protections. The rapid development and use of cyber operations in armed conflict exemplify the challenges posed by evolving technology in international law. When attacks—acts of violence against the adversary, whether in offense or defense—are present, any disagreement, whether on a global or local scale, may be described as an armed conflict. According to the Geneva Conventions, 1977, Article 49 of Protocol I, when talking about cyber operations, it is crucial to specify the kind of attack.

Both civilian and military users extensively depend on and use cyberspace. The main objective of this system is to safeguard civilian populations and infrastructure against cyber attacks while minimizing unintended harm to an acceptable extent in relation to the expected military advantage. If these conditions cannot be met, the cyber attack should not proceed. The concept of collateral damage includes both direct and indirect consequences, emphasizing the need to consider all possible effects when assessing proportionality in planning and executing a cyber attack. These challenges highlight the need for

states to exercise extreme caution when resorting to cyber attacks [13].

B. Other Legal Discourses

Do restrictions exist for cyber warfare? Do the networks, computers, and cyber infrastructure used by the public have any defenses against cyber attacks? The Tallinn Manual, in which the ICRC participated as an observer, presents an affirmative response from international legal and military professionals. This section discusses the manual and other legal discourses related to the topic.

1) *The Tallinn Manual, 2013*

The Tallinn Manual, released in 2013, explores the applicability of international law to cyberwarfare and traditional battles. It specifically focuses on jus ad bellum and IHL. The document was authored by a diverse group of more than twenty experts at the NATO CCDCOE in Tallinn between 2009 and 2012. The Tallinn Manual upholds the distinction between international and non-international armed conflicts, although it acknowledges that cyber operations, in isolation, may be deemed armed conflicts owing to their detrimental outcomes. A cyber attack is defined as any cyber-operation, whether offensive or defensive, that is expected to result in injury or death to persons or property. According to specialists, damage in the digital realm refers to the incapacity to function, regardless of the approach used. To guarantee that cyber operations intended to disrupt civilian networks are bound by the limits of IHL regarding the targeting of people, this interpretation is crucial in practical terms.

2) *The Tallinn Manual 2.0, 2017*

Version 2.0 expanded upon the 2013 edition and addressed new and emerging challenges in the field of cyber operations. It provided further insights and analysis into topics such as state responsibility for cyber operations, due diligence obligations of states, the attribution of cyber operations, and the application of IHL to cyberspace. The Tallinn Manual 2.0 aimed to refine and update the legal framework and considerations for cyber warfare considering evolving technologies and threats. The IRRC has concluded that the increasing use of cyber operations in contemporary armed conflicts has raised significant concerns, particularly regarding the potential human cost. The ICRC emphasizes that IHL applies to cyber operations just as it does to any other form of warfare, emphasizing the need for compliance with existing IHL principles and rules. It is crucial to emphasize that acknowledging the relevance of IHL to cyber

operations does not endorse or validate cyber warfare. The use of force by nations, whether in the form of cyber or physical attacks, is nonetheless bound by the United Nations Charter and other applicable regulations of international law.

3) *Proposal by the Shanghai Cooperation Organization (SCO), 2011*

According to the SCO, cyberwar is defined as the act of spreading information detrimental to the spiritual, moral, and cultural aspects of other countries. In September 2011, many countries presented a proposal for an international code of conduct for information security to the UN Secretary-General. The United States' strategy, in contrast, places political issues under the protection of free speech and concentrates on harming the body and economy. This disagreement has made the West reluctant to pursue international agreements for the control of cyber weapons. However, according to Kaspersky [14], US officials did support negotiations with Russia over a plan to restrict military assaults in cyberspace.

4) *The USA-Russia Cyberwar Hotline, 2013*

Putin and Obama agreed to establish a secure cyberwar hotline in June 2013. By establishing this connection, the US cybersecurity coordinator and the Russian deputy secretary of the Security Council would be able to have private conversations. For direct crisis management in the case of an incident involving information and communication technology security, it would be helpful. A new treaty to prohibit cyberwar on the internet has been proposed by Ukrainian specialist in international law Alexander Merezhko. Cyberwar, in this study, is defined as interference with another state's information, technological, political, or economic sovereignty via the use of the internet and related technologies. According to Professor Merezhko, the internet should continue to be a public asset free of military tactics.

5) *NISTIR, 2017*

The 2017 Cybersecurity Framework (CSF), which describes the implementation details for the manufacturing environment, was published in the US by NISTIR on March 20, 2017. Using the whitepaper, firms can lower their cybersecurity risk while adhering to industry best practices and sector goals. The profile provides manufacturing systems with a voluntary, risk-based method for enforcing cybersecurity laws and reducing cyber-risk. The framework does not replace but only enhances existing standards and industry guidelines for manufacturers.

C. Proposed Digital Geneva Convention (2017)

During the 2017 RSA Conference, the president of Microsoft proposed the implementation of the Digital Geneva Convention (DGC) as a means to restrict the capacity of nation states to engage in hacking activities targeting the civilian sectors of our economic and political infrastructures in response to cyber attacks. They suggested conducting inquiries into distinct factions, implementing a synchronized protocol for revealing software and hardware flaws, and forming an authoritative organization to supervise cyber operations to protect Internet users. In addition, he pledged to refrain from aligning himself with belligerent nations and to maintain a stance of impartiality in conflicts.

1) *Six Principles of DGC*

Microsoft claims that the proposed Digital Convention's legal authority should be based on the following six principles:

I. The private sector, key infrastructure, and high-tech enterprises should not be targeted.

II. Support for the private sector's efforts to identify, stop, respond to, and recover from cyber attacks should be provided.

III. Rather than being hoarded, sold, or otherwise abused, system vulnerabilities should be reported to suppliers.

IV. Cyber weapons should be produced with caution; those that are created should be small, highly focused on their targets, and non-reusable.

V. The spread of cyber weapons must not be acceptable.

VI. Violent actions ought to be restricted to prevent widespread and random cyber attacks.

IV. REVIEW OF IHL IN THE PERSPECTIVE OF CYBERWARFARE CHALLENGES

Treaty-making to address novel forms of warfare was necessitated in the aftermath of WWII, primarily in the context of airspace as a new domain. According to Spaight [15], the next step is to explain why it is more advantageous to develop a new and distinct code, rather than expanding upon and incorporating existing regulations that regulate land combat. Diamond [16] mentions that cyber warfare is not outside the realm of law; it falls under the purview of IHL, particularly in the context of armed conflict. However, applying IHL to cyber warfare poses numerous challenges because of its secretive nature and the unique methods. Determining whether cyber operations are linked to armed conflicts is often complex, making it difficult to

determine which IHL rules apply. Moreover, the interpretation of existing rules for this new form of warfare is unclear. From a humanitarian perspective, it is crucial to address these issues and ensure that IHL effectively protects civilians and infrastructure in cyber warfare. This may involve reinterpreting existing rules and possibly developing new, stricter ones to safeguard humanitarian values.

A. Terms ‘Cyber-Attack’, ‘Cybercrime,’ and ‘Cyber Warfare’

There is frequent overlap in the usage of the phrases “cybercrime,” “cyber attack,” and “cyber warfare.” without a clear distinction, making it difficult to establish effective legal responses to transnational cyber activities. The nature of a cyber-threat depends on who initiated it, the target involved, and the perpetrator’s intentions. For instance, a cyber-attack might use methods that, under different circumstances, would be considered cybercrime. However, cyber warfare typically follows a previous cyber-attack. To comprehend the relationship between these concepts, it is essential to consider them individually.

1) Cyber-Attack

As stated by Waxman [17], a cyber-attack refers to any deliberate effort to modify, interrupt, or obliterate computer systems or networks, as well as the data or software included inside them.

The NRC Report in 2009 defined cyber-attack as: intentional acts to demolish, deteriorate, trick, or interfere with computer networks or systems, or the data and/or applications that are stored on or transmitted over them. A cyber attack is an intentional assault on IT systems in cyberspace, with the objective of compromising the security of these systems, including their confidentiality, integrity, and availability. This definition is outlined in the German Cyber Security Strategy.

The National Cyber Strategy of the United Kingdom categorizes cyber attacks into four main groups: “electrical attack,” “subversion of supply chain,” “manipulation of radio spectrum,” and “disruption of unprotected electronics using high-power radiofrequency”:

- a. Unauthorized dissemination of sensitive information;
- b. Authorized users are unable to access mission-critical information systems;
- c. Possible exploitation of data owing to loss of integrity;
- d. Deliberate physical damage caused by failures in information systems resulting from orders.

According to the US Joint Staff Directories, 2011, a cyber-attack is an offensive action that specifically targets an opponent’s crucial cyber systems, assets, or functions using computers or related networks or systems, with the purpose of causing disruption or destruction. Cyber-attacks do not simply attempt to destroy the targeted computer systems or data. The intermediate delivery vehicles used in a cyber attack might include human operators, implanted code, electrical transmitters, or peripheral devices. There may be substantial temporal and spatial intervals between the initiation and execution of a cyber-attack.

Cyberwarfare, as defined by the ICRC, refers to the use of electronic methods to participate in aggressive actions that either meet the criteria of or occur during an armed conflict, as outlined by IHL. According to Section 30 of the Tallinn Manual [3], cyber-attacks include both offensive and defensive cyber operations that are expected to inflict injury or death on people or property.

These explanations assume that cyber-attacks and armed attacks are interchangeable, with the latter including the use of physical force to penetrate a state’s defenses, considering the purpose and size. The word ‘computer’ in the concept of a cyber-attack encompasses not just traditional computing equipment such as desktops and laptops but also artificial intelligence devices that govern various systems, including traffic lights, elevators, water terminals, washing machines, TVs, mobile phones, and even traffic lights.

2) Cyber Crime

Cybercrime is any crime that is committed or facilitated by a computer network or hardware device. The term “cybercrime” refers to a broad variety of illegal actions carried out online, such as child pornography, online privacy violations, cyber-squatting, and other related crimes. Differentiating cybercrime from cyber-attacks presents a conceptual issue because of the broad nature of cybercrimes, particularly the wide range of criminal behaviors in the digital environment. An example of this intricacy can be seen in the situation where someone hacks into a vital national database, such as the social security system or a museum, for political or national security purposes but without causing any disruptions to the database. Another scenario involves a non-state actor engaging in unlawful activities through computer networks, causing network disruption but lacking political or national security objectives. These situations highlight the intricacies and confusion inherent in attempting to conceptually differentiate between

cyber-attacks and cybercrimes.

3) *Cyber Warfare*

Billo and Chang [18] defined cyberwarfare as troops arranged along nation-state borders that engage in both offensive and defensive operations and use computers to electronically attack other computers or networks. The main goal is to gain the upper hand over a rival by jeopardizing a computing device's availability, integrity, or confidentiality. Brenner and Clarke [19], elaborating the term "cyberwarfare," discussed the character of warfare in cyberspace from both attack and defense angles. It may be noted here that both these definitions of cyber warfare confine the notion of 'war' exclusively to the realm of information technology, specifically within computer systems and networks. Therefore, some more relevant definitions need to be explored. Cyberwarfare, as defined by Theohary and Rollins [20], refers to activities between states in cyberspace that are akin to armed assaults or the application of force. These actions can elicit a military reaction, which may include the appropriate use of physical force. Teo [21] defines the act of causing physical harm or devastation by the use of projectiles such as bombs, missiles, bullets, and similar items as kinetic force or warfare. Based on the information provided, it can be inferred that cyberwarfare refers to an internet-based attack that has the capacity to do as much damage as a conventional military attack. From this perspective, cyber-warfare distinguishes itself from traditional forms of armed conflict by beginning with an online attack and culminating in fatalities and property destruction. Cyber attack, cybercrime, and cyberwarfare are interconnected concepts with complex definitions and interdependencies. While cybercrime may occur independently of cyber-attacks or cyber warfare, often the former is initiated by a cyber-attack. In some instances, cybercrime may be seen as a type of cyberwarfare, especially when it serves as the trigger or becomes engaged in a cyber-attack that initiates or is part of a cyber-war. Responsibility for activities in all three zones may only be attributed to non-state actors when these three concepts are aligned. Sohail [22] delved into complex debates surrounding the application of IHL in the context of cyber warfare, emphasizing the need for interpretative clarity and potential solutions, acknowledging the challenges arising from IHL's origins in conventional warfare. Despite states' reluctance to embrace norms limiting cyber weapons, the Tallinn Manual offers hope for the future of IHL in cyber warfare.

B. Cyber Attacks in the Context of IHL

IHL holds states legally accountable for the actions of their armed forces, operatives, organs, and non-state actors under their guidance or command. It is challenging to attribute the attacks to specific nations or people because of the anonymity and global reach of the internet [23]. States are subject to liability under IHL for cyber-attacks in several ways, including the following:

- a. Cyber attribution;
- b. The state's obligation;
- c. Effects of state accountability.

Various courts and tribunals have created and implemented numerous attribution standards, particularly effective control and overall control standards. The efficiency of the control standard necessitates a state's direct, decisive influence over the specific operation or conduct of non-state actors, such as giving orders. This standard has been used by the International Court of Justice (ICJ) in cases such as Nicaragua and the United States in 1986 but criticized for being overly strict and impractical in the context of cyber attacks, where states can use proxies or hackers without direct involvement. The overall control standard requires a state's general influence over the policy or strategy of non-state actors, such as providing support or training. In cases such as Tadic and the Bosnian Genocide, the International Criminal Tribunal for the former Yugoslavia (ICTY) applied this criterion [24]. The ability to adapt is commendable, particularly in the context of cyber attacks, where states may have influence without actually being in charge. Nevertheless, neither norm is comprehensive and widely embraced.

C. Customary International Law and Cyberwarfare

International Law is still in its infancy regarding cyberspace law and has yet to fully comprehend the legal ramifications of cyber warfare [25]. This means that there are no internationally codified and binding rules for the regulation of cyber operations. International law applies to cyberwarfare by way of analogy. The response of customary international law to cyber warfare can be investigated considering two distinct prepositions:

- I. The development and crystallization of new norms of customary international law specific to cyber warfare is difficult at best and impossible at worst;
- II. The existing norms of customary international law apply to cyberwarfare by

analogy because of their general nature.

1) *Development of Rules of Customary*

International Law Specific to Cyber-Warfare

The aforementioned propositions demonstrate that cyberwarfare is subject to the general rules of customary international law. However, the question of developing new norms of CIL is a topic of debate among scholars of international law. Some scholars believe that cyberspace and cyber warfare are relatively new concepts that have only been in place for a short period; thus, there is no strong set of legislation regulating how the state acts in cyberspace. Some also argue that customary international law is slow to develop and cannot match the pace of the rapidly developing cyber infrastructure [26]. Furthermore, some scholars argue that crystallization of new CIL norms is unlikely [27].

2) *Applying Customary International Law to Cyberwarfare*

Among academics and in state practice, the customs of international law and customary international law drafted after World War II apply to cyber warfare because they are general in nature and thus have a scope of applicability to cyber operations [28]. The following have been recognized by the International Law Commission's Articles on State Responsibility for Internationally Wrongful Acts, the Tallinn Manual of International Law Applicable to Cyber Warfare, the UN Charter 1945, and the Geneva Conventions 1949:

- I. Attribution of state liability;
- II. Principle of non-intervention;
- III. Principle of sovereignty;
- IV. Principle of prohibition of the use of force.

There remain many gray areas in the execution of the abovementioned principles in cyber warfare; nevertheless, international law experts and states do agree that these principles of customary international law govern and apply to cyber warfare [9].

D. Potential Amendments Needed

The current international legal regulations pertaining to a state's liability for cyber attacks are still being developed. To boost the efficiency of present regulations in holding States responsible for cyber attacks, numerous modifications might have to be made. Creating more detailed guidelines for cyber attack attribution is one possible change. Creating a list of elements to consider when condemning cyber attacks, such as the attack's complexities, the use of tools and techniques that are endorsed by the state, and the engagement of state officials, could

be a way of achieving this. Determining the extent of state responsibility for cyber attacks is another potential issue. For example, it is questionable whether cyber attacks carried out by criminal organizations or private enterprises are the fault of a state or not. State accountability for any cyber attacks that fall within the scope of its responsibility would be strengthened by making the extent of the state's negligence transparent. Creating stronger mechanisms for holding the state accountable for cyber attacks is essential. This may involve developing new international bodies charged with investigating and penalizing cyber attacks or developing new dispute resolution procedures.

E. ICRC Position

Cyber-attacks can impair vital services and disrupt vital civilian infrastructure, whether they occur inside or outside military conflicts. Existing IHL principles, such as distinction, proportionality, and precautions in attack, protect civilian infrastructure during armed conflicts. This protection extends to medical facilitation centers, which are vital for civilian perseverance. Employment of cyber tools that cause indiscriminate damage is prohibited during armed conflicts. While specific objects can be the target of certain cyber tools, without indiscriminate harm, the interconnected nature of cyberspace means that they can inadvertently affect various other systems. Thus, cyber tools pose a genuine risk that may not comply with IHL, either intentionally or unintentionally. The ICRC highlights the necessity for the international community to acknowledge the relevance of IHL, considering the circumstances of cyber activities during armed conflicts. They call for discussions among experts to evaluate the suitability of existing IHL rules and laws and welcome ongoing intergovernmental discussions initiated by the General Assembly of the United Nations. States' interpretation of the current IHL regulations will dictate how much protection they have from the effects of cyber operations. States ought to be unambiguously committed to applying IHL in a way that protects civilian data and infrastructure. If the necessity arises, new regulations should fortify and enhance the current legal structure, which encompasses IHL.

V. CONCLUSION AND RECOMMENDATIONS

Based on this study, it is concluded that IHL was designed for conventional warfare and did not anticipate cyber attacks. It focuses on key debates within IHL related to cyberwarfare.

Acknowledging that these debates are rooted in the interpretation of general terms in IHL, it is suggested that these debates may persist until some practical legal solution is reached. The study proposes two potential solutions: the creation of a new convention specific to cyber-armed conflicts and the development of binding customs through consistent state practices. Despite states' reluctance to create new norms, the Tallinn Manual offers hope for the future of IHL in cyberwarfare. Believing that a new norm will take time to emerge, the article predicts an increase in devastating cyber conflicts due to a cyber-arms race. In the meantime, attacking states may interpret existing laws to evade responsibility, particularly concerning civilian data. While cyber weapon treaties could address the issue, they may not be pursued due to increased military reliance on cyber capabilities. This study suggests that treaty-making may become possible once state practice is fully developed, reflecting evolving norms. Until then, the existing IHL rules should govern cyber warfare and be interpreted on the basis of the foundational values of IHL.

To successfully tackle the obstacles presented by cyber-attacks, it is necessary to continuously adapt and collaborate internationally and support states and relevant organizations in developing technical skills and knowledge to protect critical infrastructure from cyber-attacks through capacity-building efforts. Training programs, information sharing, and technical assistance are all part of this package. The state must spread and improve digital literacy across the country so that individuals can protect their own data and make informed choices in the digital world. It is recommended to spread the word to states, armed forces, and relevant stakeholders about the need to protect critical infrastructure during cyber warfare and the responsibilities under IHL and examine and revise local legal arrangements to ensure that they adequately address cyber-attacks on vital infrastructure and comply with international obligations under IHL. Discussions on treaty making could focus on areas such as the prohibition of certain types of cyber attacks, rules governing state conduct in cyberspace, mechanisms for attribution of cyber operations, and the establishment of cooperative mechanisms for sharing information and responding to cyber incidents. By engaging in treaty-making discussions, states can work toward establishing common understandings and standards in addressing the legal, ethical, and security challenges presented by cyber warfare. This would contribute to greater stability,

predictability, and accountability in cyberspace, ultimately ensuring a more secure and trustworthy digital environment.

DECLARATIONS

Author Contributions

Conceptualization, S.U.R., M.A.S. and M.T.; methodology, S.U.R., M.A.S., M.T., I.N., S.S., N.F.A.B. and K.Z.; validation, S.U.R., M.A.S., M.T., I.N., S.S., N.F.A.B. and K.Z.; formal analysis, S.U.R., M.A.S., M.T., I.N., S.S., N.F.A.B. and K.Z.; investigation, S.U.R., M.A.S. and M.T.; resources, I.N., S.S., N.F.A.B. and K.Z.; data curation, S.U.R.; writing—original draft preparation, S.U.R., M.A.S., M.T., I.N., S.S., N.F.A.B. and K.Z.; writing—review and editing, S.U.R., M.A.S., M.T., I.N., S.S., N.F.A.B. and K.Z.; visualization, S.U.R.; supervision, S.U.R.; project administration, I.N., S.S., N.F.A.B. and K.Z.; funding acquisition, S.S., N.F.A.B. and K.Z. All authors have read and agreed to the published version of the manuscript.

Data Availability Statement

No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest

The authors declare no conflict of interest.

REFERENCES

- [1] PALMIERI, D. (2015) How warfare has evolved – A humanitarian organization's perception: The case of the ICRC, 1863–1960. *International Review of the Red Cross*, 97 (900), pp. 985-998.
- [2] INTERNATIONAL COMMITTEE OF THE RED CROSS (2014) *International Humanitarian Law: Answers to Your Questions*. [Online] Available from: <https://www.icrc.org/en/doc/assets/files/other/icrc-002-0703.pdf> [Accessed 15/10/23].
- [3] SCHMITT, M.N. (ed.) (2013) *Tallinn Manual on the International Law Applicable to CyberWarfare*. New York: Cambridge University Press.
- [4] DUNANT, H. (1947) *A Memory of*

Solferino. London: Cassell for the British Red Cross Society.

[5] ANAND, V. (1999) Impact of technology on conduct of warfare. *Strategic Analysis*, 23 (1), pp. 137-150.

[6] TOFFLER, A. and TOFFLER, H. (1995) *War and anti-war: Survival at the dawn of the 21st century*. New York: Warner Books.

[7] HOFFMAN, F.G. (2007) *Conflict in the 21st century: The rise of hybrid wars*. Arlington, Virginia: Potomac Institute for Policy Studies.

[8] MUMFORD, A. and CARLUCCI, P. (2023) Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, 8 (2), pp. 192-206.

[9] MARWALA, T. (2023) Artificial Intelligence in Politics. In: *Artificial Intelligence, Game Theory and Mechanism Design in Politics*. Singapore: Palgrave Macmillan, pp. 41-58.

[10] INTERNATIONAL COMMITTEE OF THE RED CROSS (2018) *Ethics and autonomous weapon systems: An ethical basis for human control?* [Online] Available from:

<https://www.icrc.org/en/document/ethics-and-autonomous-weapon-systems-ethical-basis-human-control> [Accessed 19/10/23].

[11] STEINHOFF, J.K. (2023) *An Ethical Dilemma: Weaponization of Artificial Intelligence*. [Online] Small Wars Journal. Available from:

<https://smallwarsjournal.com/jrnl/art/ethical-dilemma-weaponization-artificial-intelligence#:~:text=Due%20to%20the%20ethical%20concerns,of%20use%20during%20armed%20conflict> [Accessed 19/10/23].

[12] ATREWS, R.A. (2020) Cyberwarfare: Threats, Security, Attacks, and Impact. *Journal of Information Warfare*, 19 (4), pp. 17-28.

[13] INTERNATIONAL COMMITTEE OF THE RED CROSS (2013) *What Limits Does the Law of War Impose on Cyber Attacks?* [Online] Available from:

<https://www.icrc.org/eng/resources/document/s/faq/130628-cyber-warfare-q-and-a-eng.htm> [Accessed 15/05/22].

[14] KASPERSKY, E. (2017) *A Digital Geneva Convention? A Great Idea*. [Online] Forbes. Available from:

<https://www.forbes.com/sites/eugenekaspersky/2017/02/15/a-digital-geneva-convention-a-great-idea/?sh=14598dc21e6e> [Accessed 19/10/23].

[15] SPAIGHT, J.M. (1924) *Air Power and War Rights*. London: Longmans Green & Co.

[16] DIAMOND, E. (2014) Applying international humanitarian law to cyber warfare. *Law and National Security*, 67 (1), pp. 67-84.

[17] WAXMAN, M.C. (2011) Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4). *Yale Journal of International Law*, 36, pp. 421-422.

[18] BILLO, C.G. and CHANG, W. (2004) *Cyber warfare: An analysis of the means and motivations of selected nation states*. Institute for Security Technology Studies at Dartmouth College.

[19] BRENNER, S.W. and CLARKE, L.L. (2010) Civilians in Cyberwarfare: Conscripts. *Vanderbilt Journal of Transnational Law*, 43, pp. 1011-1076.

[20] THEOHARY, C.A. and ROLLINS, J.W. (2015) *Cyberwarfare and Cyberterrorism: In Brief*. [Online] Congressional Research Service. Available from:

<https://sgp.fas.org/crs/natsec/R43955.pdf> [Accessed 19/10/23].

[21] TEO, C.H. (2008) *The Acme of Skill: Non-Kinetic Warfare*. Air University Press.

[22] SOHAIL, H. (2022) Fault Lines in the Application of International Humanitarian Law to Cyberwarfare. *Journal of Digital Forensics, Security and Law*, 17 (1), 8.

[23] MUELLER, G.B., JENSEN, B., VALERIANO, B., MANESS, R.C., and MACIAS, J.M. (2023) *Cyber Operations during the Russo-Ukrainian War: From Strange Patterns to Alternative Futures*. Washington, District of Columbia: Center for Strategic and International Studies.

[24] CASSESE, A. (2007) The Nicaragua and Tadić Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia. *European Journal of International Law*, 18 (4), pp. 649-668.

[25] RABOIN, B. (2011) Corresponding evolution: International law and the emergence of cyber warfare. *Journal of the National Association of Administrative Law Judiciary*, 31 (2), pp. 602-668.

- [26] KITTICHAISAREE, K. (2017) *Public international law of cyberspace*, Vol. 32. Cham: Springer.
- [27] SCHMITT, M.N. (2020) Taming the lawless void: tracking the evolution of international law rules for cyberspace. *Texas National Security Review*, 3 (3), pp. 32-47.
- [28] DELERUE, F. (2020) *Cyber operations and international law*, Vol. 146. Cambridge University Press.

参考文献:

- [1] PALMIERI, D. (2015) 战争如何演变——人道组织的看法：红十字国际委员会的案例，1863-1960。《红十字国际评论》，97 (900)，第 985-998 页。
- [2] 红十字国际委员会 (2014) 《国际人道主义法：问题解答》。[在线] 可从：<https://www.icrc.org/en/doc/assets/files/other/icrc-002-0703.pdf> [访问日期：15/10/23]。
- [3] 施密特, M.N. (编辑) (2013年) 《适用于网络战的国际法塔林手册》。纽约：剑桥大学出版社。
- [4] DUNANT, H. (1947) 索尔费里诺的回忆。伦敦：卡塞尔代表英国红十字会。
- [5] ANAND, V. (1999) 技术对战争行为的影响。战略分析, 23 (1), 第 137-150 页。
- [6] TOFFLER, A. 和 TOFFLER, H. (1995) 战争与反战：21世纪初的生存。纽约：华纳图书。
- [7] 霍夫曼, F.G. (2007) 21世纪的冲突：混合战争的兴起。弗吉尼亚州阿灵顿：波托马克政策研究所。
- [8] MUMFORD, A. 和 CARLUCCI, P. (2023) 混合战争：通过其他方式延续模糊性。《欧洲国际安全杂志》，8 (2)，第 192-206 页。
- [9] MARWALA, T. (2023) 政治中的人工智能。见：政治中的人工智能、博弈论和机制设计。新加坡：帕尔格

- 雷夫·麦克米伦，第 41-58 页。
- [10] 红十字国际委员会 (2018) 道德与自主武器系统：人类控制的道德基础？[在线] 可从以下网址获取：<https://www.icrc.org/en/document/ethics-and-autonomous-weapon-systems-ethical-basis-human-control> [访问日期：19/10/23]。
- [11] 斯坦霍夫, J.K. (2023) 道德困境：人工智能武器化。[在线] 小战争杂志。可从：<https://smallwarsjournal.com/jrnl/art/ethical-dilemma-weaponization-artificial-intelligence#:~:text=Due%20to%20the%20ethical%20concerns,of%20use%20during%20armed%20conflict> [访问日期：23年10月19日]。
- [12] ATREWS, R.A. (2020) 网络战：威胁、安全、攻击和影响。《信息战杂志》，19 (4)，第 17-28 页。
- [13] 红十字国际委员会 (2013) 战争法对网络攻击有何限制？[在线] 可访问：<https://www.icrc.org/eng/resources/documents/faq/130628-cyber-warfare-q-and-a-eng.htm> [访问日期：22年5月15日]。
- [14] KASPERSKY, E. (2017) 数字日内瓦公约？一个好主意。[在线] 福布斯。来源：<https://www.forbes.com/sites/eugenekaspersky/2017/02/15/a-digital-geneva-convention-a-great-idea/?sh=14598dc21e6e> [访问日期：23年10月19日]。
- [15] SPAIGHT, J.M. (1924) 空中力量和战争权利。伦敦：朗曼斯格林公司
- [16] DIAMOND, E. (2014) 将国际人道法应用于网络战。法律与国家安全, 67 (1), 第 67-84 页。
- [17] 韦克斯曼, M.C. (2011) 网络攻击和使用武力：回到第2(4)条的未来。《耶鲁国际法杂志》，36，第 421-422 页。
- [18] 比洛, C.G. CHANG, W. (2004) 网络战：对选定民族国家的手段和动机的分析。达特茅斯学院安全技术研究所。
- [19] 布伦纳, S.W. 和 CLARKE, L.L. (2010) 网络战中的平民：义务兵。《范德比尔特

跨国法杂志》，43，第 1011–1076 页。

[20] 西奥哈里, C.A. 和罗林斯, J.W. (2015)

网络战和网络恐怖主义：简介。[在线]国会研究服务。可从：<https://sgp.fas.org/crs/natsec/R43955.pdf> [访问日期：19/10/23]。

[21] TEO, C.H. (2008)
技能的极致：非动能战争。航空大学出版社。

[22] SOHAIL, H. (2022)
国际人道法在网络战中的应用的断层。数字取证、安全与法律杂志, 17 (1), 8。

[23] MUELLER, G.B.、JENSEN, B.、VALERIANO, B.、MANESS, R.C. 和 MACIAS, J.M. (2023) 俄罗斯-乌克兰战争期间的网络行动：从奇怪的模式到替代的未来。华盛顿哥伦比亚特区：战略与国际研究中心。

[24] CASSESE, A. (2007)
根据国际法院关于波斯尼亚种族灭绝的判决重新审视尼加拉瓜和塔迪奇试验。《欧洲国际法杂志》，18 (4), 第 649-668 页。

[25] RABOIN, B. (2011)
相应的演变：国际法和网络战的出现。《全国行政法司法协会杂志》，31 (2), 第 602-668 页。

[26] KITTICHAISAREE, K. (2017)
网络空间国际公法, 卷。32。
查姆：施普林格。

[27] 施密特, M.N. (2020)
驯服无法无天的虚空：追踪网络空间国际法规则的演变。《德克萨斯国家安全评论》，3 (3), 第 32-47 页。

[28] DELERUE, F. (2020)
网络运营和国际法, 卷。146。
剑桥大学出版社。