Syiah Kuala Law Journal
FAKULTAS HUKUM UNIVERSITAS SYIAH KUALA
Vol.8(1) April 2024, pp. 35-47
ISSN 2580-9059 (online)
2549-1741 (cetak)

UNTANGLING THREATS: HUMANITARIAN LAW'S ADAPTATION TO DETERMINE CYBER OPERATIONS IN ARMED CONFLICT

Gabriela Meinar Regina[1], Davilla Prawidya Azaria[2]
[1,2)] Faculty of Law, Pembangunan Nasional Veteran Jakarta University

Info Artikel
Received : 20/01/2024
Approved : 30/03/2024

Keywords:
Armed conflict, Conduct of war, Cyber attack, International humanitarian law.

Abstract
This discussion highlights the need to evaluate international legal systems to effectively deal with the complex challenges posed by cyber attacks in armed conflicts. The Tallinn Manual, created by a group of legal experts, serves as a comprehensive guide for navigating this constantly changing landscape, offering a common language and framework for addressing cyber threats worldwide. Following its recommendations has significant legal and political implications, offering important clarification on how existing legal rules apply to cyberspace. At the same time, it shows a commitment to upholding the rule of law in this rapidly changing environment. However, ongoing challenges like evolving technology and issues with attribution emphasize the importance of international cooperation and flexible legal approaches in creating norms and principles for governing cyber operations.

I. INTRODUCTION

The current era we are experiencing is undoubtedly undergoing a transformative phase for humanity. In due time, all human activities may find their focal point beyond the confines of Earth's atmosphere. In the context of future warfare, the implications of such profound transformation will directly influence the concepts of conflict, its locales, and the instruments involved. These changes will reflect radical departures from our present understanding and this transformation will shape how wars unfold, identify the parties engaged in conflicts, determine the theaters of future battles, and even ascertain the underlying reasons for wars to be waged.

The most devastating cyber attack in history took place in Estonia in 2007. On April 27 of that year, a series of extensive cyber assaults targeted various Estonian government entities, including banks, parliament, newspapers, and broadcasters. This attack was in response to Estonia's disagreement with Russia regarding the relocation of the Bronze Soldier of Tallinn, a significant Soviet-era memorial, in Tallinn's war cemeteries. Initially, the Estonian government swiftly pointed fingers at the Kremlin, accusing it of direct involvement in the strike. However, when Estonia's defense minister admitted to lacking evidence linking the cyberattack to the Kremlin, it became clear that the accusations were not entirely founded. Russia has since dismissed the allegations as

"groundless," and both NATO and the European Commission experts have been unable to establish concrete proof of the Russian government's official participation. Estonia, in the aftermath of the attack, advocated for a focus on enhancing cybersecurity protection and incident management as the best course of action (Herzog, 2011).

Recent instances we can examine include the cyber assaults amid the conflict between Russia and Ukraine. Since the onset of the conflict, Ukraine has recurrently suffered from cyber intrusions. Predominantly, cyber assaults targeted Ukrainian power utilities, leading to significant power outages affecting over 225,000 individuals across the nation in December 2015. Subsequently, in December 2016, Kiev experienced another blackout following a similar attack. Furthermore, cyber assailants targeted Ukraine's governmental and commercial computer networks. Notably, in June 2017, the NotPetya cyber strike, attributed to Russia, wreaked havoc on computer systems globally, resulting in billions of dollars in damages. In January 2022, almost 70 Ukrainian government bodies fell victim to a recent cyber onslaught. These attacks have had profound repercussions, including power disruptions and financial setbacks. (Priyono, 2022).

The dilemma adds by the literature review where the authors argue that the instrumentalization of the internet as a tool of warfare poses a significant threat to international peace and security, and that the existing legal framework is inadequate to address this challenge. They emphasize the increasing importance of the internet as a weapon and the need for a more comprehensive approach to its regulation. The authors contend that the lack of international cooperation and a universal approach to cyber warfare are primary obstacles to effective regulation, and that the current legal framework is fragmented and incomplete. The authors here also summarizes the social, normative, and ethical aspects of regulating cyber warfare and proposes solutions to this dilemma. They assert that a new legal framework is necessary to address the challenges posed by cyber warfare, and that this framework should be based on principles of international law, including sovereignty, non-intervention, and the prohibition of the use of force (Simovic, Rasevic, Vladimir, 2020).

Hence, amidst the rapid development of modern warfare, where battles transcend physical boundaries and unfold within the complex realm of cyberspace, the effectiveness of the international legal framework in governing the techniques and methods of cyber warfare has come under intense scrutiny. This paper aims to delve into two critical aspects of this issue. Firstly, it examines the integration and response of the international legal framework to cyber attacks within the context of armed conflict. This involves assessing the challenges of regulating cyber attacks during conventional armed conflicts and deepening our understanding of cyber warfare in such scenarios, setting the stage for an analysis of the preceding statement. Secondly, an in-depth exploration is undertaken to

ascertain the Tallinn Manual's significance as a comprehensive guide aimed at bridging the regulatory gap pertaining to cyber attacks during armed conflicts. This involves a thorough analysis of its relevance, inherent advantages, and its alignment with established humanitarian law principles and the broader concept of humanity. Furthermore, a critical examination of the challenges it faces in effectively implementing these regulations is also addressed.

A comprehensive review is essential to ascertain whether the International Humanitarian Law body, serving as a pivotal role in the sphere of warfare and armed conflict, operates as a comprehensive framework of rules and principles crafted to alleviate the humanitarian toll of such situations & The International Committee of the Red Cross (ICRC) serves as the vanguard of IHL, acting as an impartial and independent global entity which their mission is encompasses the delivery of humanitarian aid and protection to victims of armed conflict and other forms of violence worldwide which makes this mandate involves promoting and advancing IHL, providing vital humanitarian assistance, supporting national Red Cross and Red Crescent Societies, and engaging in dialogue with states and armed groups to foster understanding and adherence to IHL. The ICRC has a key role, but many other groups also help enforce and spread IHL. These include the UN, different international courts and groups, and more humanitarian organizations. Together, they can tackle the complex issues of the digital battlefield.

II. METHODS

This study centers on an examination of cyber attacks within the framework of armed conflict and the position of the Tallinn Manual in addressing this critical issue. The research adopts a normative juridical approach, leveraging prior cases and existing research to explore potential gaps in the current legal provisions related to cyber warfare. Through a comparative analysis of contemporary state practices and recent regulations, the study aims to shed light on areas where the regulation of cyber warfare techniques within the Rome Statute may be lacking. By identifying these deficiencies, this paper strives to contribute to a deeper comprehension of the existing regulations, ultimately facilitating the refinement of the regulatory framework governing cyber warfare. Primary sources, including the Geneva Conventions and its additional protocols and The Tallinn Manual on Cyber Warfare, are central to this research, complemented by secondary materials like textbooks, journals, and prior research. Employing a qualitative methodology involving data collection, reduction, analysis, and interpretation of legal materials, this study takes a significant step towards bridging the gap between the rapidly evolving nature of cyber warfare and the sufficiency of existing legal mechanisms.

III. ANALYSIS AND DISCUSSION

3.1. Applying Existing IHL for Addressing Cyber Attacks in Armed Conflict

According to the knowledge of the CheckPoint Software Technologies, which releases data in real time, over 255 million cyber attacks in peacetime were documented on the day this report was written. During periods of armed conflict, cyber operations are frequently integrated with conventional military strategies, it is stated that cyber attacks have significant benefits over traditional ones since they are low-cost, long-range, quick, and forceful tactics of coercion or devastation, frequently with little chance of prosecution. While the incorporation of cyber methods introduces novel tactical avenues not always available in traditional warfare, it also introduces its own set of hazards. Cyber operations offer the possibility for warring parties to achieve their military goals without harming civilians or damaging civilian infrastructure, which is a positive development. However, recent cyber activities, often taking place outside formal warfare, demonstrate that skilled actors can disrupt the provision of vital services to civilian populations.

In the realm of modern warfare driven by technology, traditional definitions of attack and conflict find themselves outpaced. As the frequency and sophistication of these attacks surge, there arises a pressing need to explore diverse avenues for their prevention and retribution. Resorting to legal measures appears to be the logical course of action. Yet, this domain of law remains in its nascent stages, lacking a comprehensive global treaty that governs such behavior. Instead, we turn to the framework of International Humanitarian Law (IHL) to regulate actions 'in the midst of a conflict', and International Criminal Law (ICL) to criminalize actions and establish penalties 'post-conflict'.

According to the ICRC, there is unquestionable application of International Humanitarian Law (IHL) to cyber operations during armed conflict. This regulation places constraints on cyber activities, treating them akin to any other weapon, means, or method of combat used in both traditional and modern warfare contexts (ICRC, 2019). Within the context of Cyber Operation, IHL assumes paramount importance since assailants often execute attacks without prior warning. In numerous instances, classifying these acts as an attack during war proves to be a formidable challenge due to their virtual nature, which grants perpetrators a shroud of anonymity. The cornerstone of IHL lies in the Geneva Conventions (GCs) and their Additional Protocols (APs). These conventions encompass a spectrum of critical aspects related to armed conflicts, ranging from the care of the wounded to the safeguarding of civilian populations. A notable addition in 2005 introduced an Extra Protocol, which addressed the adoption of an Additional Distinctive Emblem. This progression signifies an

extensive departure from the well-established and globally recognized regulations governing traditional kinetic warfare, underlining the unique complexity posed by cyber warfare.

When states ratify International Humanitarian Law (IHL) agreements, they aim to regulate both present and prospective armed conflicts. These agreements incorporate provisions that anticipate the emergence of new methods and technologies of warfare, with the expectation that IHL will govern them. For instance, if IHL didn't apply to future methods and tactics of warfare, Article 36 of the 1977 Additional Protocol I wouldn't mandate an evaluation of their legality within existing IHL frameworks. The Advisory Opinion of the International Court of Justice regarding the Legality of the Threat or Use of Nuclear Weapons provides significant backing to this assertion. The Court affirmed that the principles and rules of International Humanitarian Law (IHL) apply not only to current forms of warfare and weapons but also to those anticipated in the future. According to the ICRC, this judgment extends to the use of cyber operations during armed conflict.

Since as early as 1996, the United States has adopted a national security-focused approach towards cyberspace. Over time, this focus has intensified, with President Obama acknowledging cyber threats as among the most significant challenges to both economic stability and national security. He also highlighted the inadequacy of the nation's preparedness in addressing these threats. The United States has not simply made rhetorical commitments; it has allocated substantial financial and organizational resources to bolster its cybersecurity efforts. Government agencies, the military, industry players, and academic institutions are actively engaged in research and policy formulation, evident from the plethora of published papers on the subject. While a comprehensive discussion of the American approach is beyond the scope of this article, it is clear that cybersecurity garners widespread attention across various sectors. Similarly, though cyberspace remains a relatively young domain, its potential ramifications have not escaped the notice of global national security stakeholders, even though specific practices and details often remain concealed under layers of secrecy in many countries.

Also, the member nations of the Shanghai Cooperation Organization also introduced their own International Code of Conduct for Information Security (SCO Code of Conduct), which was adopted by the United Nations General Assembly in 2011. The SCO Code of Conduct highlights the necessity to prevent the potential utilization of information and communication technologies for purposes conflicting with the goals of upholding international stability and security, and which could harm the integrity of a nation's infrastructure, impacting its security. It also underscores the

requirement for enhanced coordination and universal cooperation among nations to counter the unlawful exploitation of information technologies. Moreover, it emphasizes the significance of safeguarding the security, continuity, and stability of the Internet, and the protection of information and communications technology networks from threats and vulnerabilities. It also reaffirms the importance of a shared understanding of Internet security matters and the need for further cooperation on both national and international levels (Gechik, 2017).

3.2. Mapping the Tallinn Manual's Impact on Cyber Conflict Regulation

A notable contribution to this subject originates from NATO in the form of the Tallinn Manual (Schmitt, 2017). Crafted by an international panel of experts, the manual holds no legal binding but offers guidance on the application of existing laws of armed conflict to cyber warfare. A closer examination and evaluation of the manual's overarching approach, which notably underscores concerns regarding the methodology of cyber warfare, can be seen in one of its stipulated rules:

> "The use of means or methods of cyber warfare that lack discrimination is prohibited. Such means or methods are considered indiscriminate when they cannot be: a) precisely aimed at a particular military target or b) constrained in their consequences in accordance with the demands of the law of armed conflict, and hence possess the potential to strike military targets as well as civilians or non-military entities without distinction. "

While the Tallinn Manual has significantly advanced the discourse on applying international law to cyber operations, its integration into the broader framework of international humanitarian law (IHL) has encountered notable challenges. The manual, which primarily addresses the application of existing legal norms to cyber warfare, faces hurdles in adapting to the nuanced intricacies of IHL. One of the foremost challenges lies in the evolving nature of technology and cyber capabilities. Traditional IHL frameworks were designed with conventional warfare in mind, often involving physical, kinetic operations. Adapting these principles to the realm of cyberspace, where the effects may be less tangible and immediate, presents a unique set of difficulties. The manual's attempts to categorize cyber activities, while commendable, can encounter resistance and skepticism from legal scholars and practitioners who grapple with the digital intricacies of modern conflict.

Another concern arises from the emergence of non-international cyber conflicts. One criterion for classifying such conflicts is the control of a portion of the attacked country's territory by the insurgent faction. In the context of cyber warfare,

does this imply that rebels have gained control over a segment of the country's entire infrastructure or cyber operations? This remains an open question.

Furthermore, the attribution problem in cyberspace complicates the application of IHL. Determining the source of a cyber-attack can be a complex and elusive endeavor, which can impact the assessment of responsibility and accountability under IHL. This ambiguity can lead to challenges in holding states or entities accountable for cyber operations that may have violated established legal norms. Another significant challenge lies in the varying interpretations and perspectives of states regarding the application of IHL to cyber activities. The manual acknowledges that the formulation of its rules was informed solely by the military manuals of four nations: Canada, Germany, the United Kingdom, and the United States. Consequently, there exists the possibility that the manual could be biased and influenced by a Western perspective on warfare and conflict. Different states may have divergent views on the threshold for the use of force in cyberspace, as well as the proportionality of responses to cyber incidents. This diversity of opinion can hinder the development of consensus on how IHL principles should be extended to cover cyber warfare. Additionally, the international community has yet to establish a universally accepted set of rules specifically tailored for cyberspace. While the Tallinn Manual provides valuable guidance, it does not carry the same weight as an internationally ratified treaty. The absence of a widely adopted legal framework for cyber operations within IHL poses a challenge for states seeking a clear and standardized set of rules to govern cyber conflict.

Organizations like the Shanghai Cooperation Organization (SCO) have expressed interest in governing cyber warfare, and a collaborative endeavor between SCO and NATO could potentially yield more universally accepted outcomes. Secondly, the team of experts encounters difficulties when attempting to apply terms such as "use of force" to the cyber domain. The determination of when a "use of force" transpires holds significant significance as it marks the point at which a state violates the UN Charter. Rule 11 strives to define "use of force" in the cyber domain but concedes that the assessment of whether "force" is employed in a cyber attack remains subjective and contingent on a Schmitt Analysis.

It can be concluded that while states form international treaties, the Tallinn Manual is crafted by experts, placing it outside the realm of international agreements. An intriguing question arises: what happens in the event of a cyberwar when there's still a legal void concerning rules of cyber warfare? The ICRC has responded to this by stating that if cyber warfare yields effects akin to those of conventional weapons or war, the same provisions that apply to traditional weaponry would be relevant. The

International Court of Justice, in its Advisory opinion on the legality of the threat or use of nuclear weapons in 1996, also upholds this position, affirming that humanitarian law can be extended to all forms of warfare and weaponry, present and future (ICJ).

Despite all the challenges, The Tallinn Manual provides a complete framework for the legal control of cyber operations, which is especially significant given the potentially disastrous implications of cyber operations, which can disrupt and destroy critical components of modern societies. The Manual contains particular Rules that form a framework for the legal control of cyber operations, each of which is supplemented by a Commentary that explains the Rule's legal foundation and its interpretation in relation to contemporary standards. This serves to clarify the complicated legal concerns underlying cyber activities, with special emphasis on those requiring jus ad bellum and jus in bello. Overall, the Tallinn Manual contributes significantly to the progress of international law in the field of cyber warfare.

The principle of proportionality in humanitarian law is a fundamental guideline that plays a crucial role in maintaining the appropriate balance between the use of armed force and the achievement of its objectives. The underlying concept of this principle is that when armed force is employed, the proportion or balance between the type of weapons used and the intended outcome must be carefully preserved. This refers to the importance of minimizing disproportionate negative impacts on those not directly involved in the conflict, such as civilians and vital civilian infrastructure. A central point of the proportionality principle is human control over weapon use. This plays a crucial role in reducing the risk of errors or unnecessary harm due to decisions made by machines or automated technology. By maintaining direct human control, the potential to make contextual assessments and consider complex human factors can be better ensured, thereby minimizing the risk of disproportionate loss. Moreover, the principle of proportionality also asserts that the use of weapons must align with the framework of international humanitarian law. This emphasizes the importance of compliance with internationally agreed-upon humanitarian norms to ensure that actions taken do not violate fundamental principles of human rights and humanitarian norms. In the context of cyber attacks, the principle of proportionality serves as a guideline to avoid unnecessary or excessive damage or suffering to infrastructure, computer systems, and sensitive data. It also plays a role in protecting civil liberties and privacy, as well as preventing negative impacts that could trigger economic and social instability. The proportionality principle in cyber operations also imposes international responsibility that guides the behavior of states and armed groups to maintain acceptable standards of conduct in their actions in the digital realm. By

adhering to this principle, actions in cyber attacks become more ethical, humane, and in line with the humanitarian values underlying international humanitarian law. The Tallinn Manual itself also establishes limitations on attacks against individuals, objects, and methods, ensuring that actions taken remain within the boundaries and constraints of international law.

The principle of "unnecessary suffering" in humanitarian law refers to the prohibition of using means and methods of warfare that cause excessive or undue suffering to combatants or individuals affected. This principle is articulated in various agreements and legal instruments, both in international and non-international armed conflicts. It encompasses the use of weapons that result in damage or injury beyond legitimate military necessity, or that is disproportionate to the expected military advantage. In the context of cyber warfare, the principle of "unnecessary suffering" holds significant implications for the methods of warfare employed in cyber attacks. Cyber warfare involves attacks and defenses in the digital realm, with impacts that can be felt in the form of critical infrastructure damage, data breaches, and economic instability. Employing methods that cause undue suffering or excessive harm, such as damaging healthcare systems, public infrastructure, or overall civilian safety, may violate the principle of "unnecessary suffering" in humanitarian law. Applying the principle of "unnecessary suffering" in cyber context, it also underscores the need to avoid using techniques or methods that can cause excessive suffering or harm without strong military justification. This principle raises critical questions about the ethics and humanity of employing cyber technology as a weapon, as well as the importance of developing clear international guidelines and standards to regulate behavior in the cyber domain.

IV. CONCLUSION

The concept of cyber warfare is not novel or implausible anymore; real-world experiences have demonstrated the genuine potential to substitute conventional warfare, particularly due to the technological advancements that bolster cyber warfare. Nonetheless, there is a noticeable absence of well-defined international regulations specifically overseeing cyber warfare, leaving customary laws of war in force to this day. Consequently, all entities, whether they be corporations or nations, must ready themselves by heightening their cybersecurity measures to deter or mitigate the repercussions of a cyber assault. Conducting regular simulations to enhance the skills of information technology personnel and implementing robust cyber defense systems are practical measures aimed at reducing the occurrence of cyber attacks. The Tallinn Manual, a pivotal contribution by a consortium of experts, offers valuable insights into

applying established legal norms to cyber warfare. It is crucial to recognize that IHL is adaptable and has, in the past, successfully incorporated new forms of warfare. The Tallinn Manual, while not legally binding, offers a comprehensive framework for navigating the complexities of cyber operations. By emphasizing principles of proportionality and minimizing unnecessary suffering, it contributes significantly to the progress of international law in the realm of cyber operation.

Bibliography

Crumbaugh, B.S., Jennifer A. (2008). The Morality of A U.S. Preemptive Strike on Iran's Nuclear Program: A Just War Analysis. Georgetown University Washington, D.C.

European Commission. (2010, August 26). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe*. accessed August 28, 2023, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0245R(01)&from=EN.

ICJ. (1996, July 8). The legality of the Threat or Use of Nuclear Weapons, Advisory Opinion. ICJ Rep. The Netherlands: The Hague.

Garrie, D. (2012). "Cyber Warfare, What Are the Rules?" Source: Journal of Law & Cyber Warfare 1 (1).

Gechlik, Mei. n.d. "Appropriate Norms of State Behavior in Cyberspace: Governance in China and Opportunities for US Businesses. A Hoover Institution Aegis Series Paper No. 1706.

Geneva Conventions (1949).

Haaretz, *Israel Suffered Massive Cyber Attack During Gaza Offensive*, accessed August 28, 2023, https://www.haaretz.com/1.5065382.

Herzog, S. (2011). Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses. *Journal of Strategic Security 4*(2), 49-60.

Kovács, L (2018). Cyber Security Policy and Strategy in the European Union and Nato. *Land Forces Academy Review 23* (1): 16–24.

Kumar, A. (2019). Placing Cyber Warfare Within The Rome Statute Framework. *A Reflection Journal*, Vol.70.

Lancelot, J.F. (2020). Cyber-Diplomacy: Cyberwarfare and the Rules of Engagement. *Journal of Cyber Security Technology*, 1–15.

Lewis, J. (2002). Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies.

Maskun, M., and Azhar, R. (2021). Cyber Warfare: National Security in Dealing with a Changing Method of War. *Kanun Jurnal Ilmu Hukum 23* (3), 477–90.

Menski, W (2006). Comparative Law in a Global Context, The Legal Systems of Asia and Africa. Cambridge: Cambridge University Press.

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

Nguyen, NK. (2014). The International Humanitarian Law Implications of the 'Tallinn Manual. E-International Relations, 1-9.

NYTimes, *Obama Order Sped Up Wave of Cyberattacks Against Iran*. accessed August 28 2023, The New York Times: Middle East, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave- of-Cyber attacks-against iran.html?_r=2&.

Simović, M., Živorad R., and Simović, V. (2020). Cyber Warfare and International Cyber Law: Whither.? *Journal of Criminology and Criminal Law 58* (3): 23–37.

Priyono, U. (2022). Cyber Warfare as Part of Russia and Ukraine Conflict. *Jurnal Diplomasi Pertahanan 8* (2): 44.

Protocol Additionals to The Geneva Conventions (1977).

Robinson, M., Jones, K., and Janicke H. (2015). Cyber Warfare: Issues and Challenges. *Computers & Security 49* (March), 70–94.

Schmitt, M. (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal, Volume 54*.

Suharto, M. A. (2015) "Analisis Yuridis Mengenai Cyber Attack Dalam Cyber Warfare Berdasarkan Hukum Humaniter Internasional (Studi Kasus Cyber Attack Negara Amerika Serikat Terhadap Program Pengembangan Nuklir Negara Iran Pada Tahun 2009)." *Brawijaya Law Student Journal (3).*

Tabansky, L. (2011). Basic Concepts in Cyber Warfare. *Military and Strategic Affairs Volume 3*.

ThreatMap, Live Cyber Threat Map, accessed August 30 2023, https://threatmap.checkpoint.com/.

Vatis, Michael A. (2010). *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*. National Research Council.

Wang, G. (2021). Are There International Rules Governing Cyberspace.? *Journal of International and Comparative Law 8:2*, 357-384.

Werner, W. G., & Kessler, O. (2013). Expertise, uncertainty and international law, a study of the Tallinn manual on cyberwarfare. *Leiden Journal of International law, 26(04)*, 793-810.