https://doi.org/10.33472/AFJBS.6.6.2024.5534-5541

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

Cyber Warfare and the Principle of Distinction under International Humanitarian Law: Some Critical Reflections

Dr. Satish Hanmantrao Mane[1], Prof. Dr. Pooja Prashant Narwadkar[2], Sanjay Jayram Aher[3], Aditya Kedari[4], Aishwarya Yadav[5] and Dr. Sapna Sukrut Deo[6]

[1]I/c Principal, Bharati Vidyapeeth's Yashawantrao Chavan Law College, Karad, India
[2]Principal, New Law College, Sangli, India
[3]Assistant Professor, Bharati Vidyapeeth New Law College, Sangli, India
[4]Assistant Professor, School of Law, MIT ADT University, Pune and
Ph.D. Research Scholar, SIU, Pune, India
[5]Assistant Professor, DES Shri Navalmal Firodia Law College, Pune, India
[6]Professor, School of Law, MIT ADT University, Pune, India
Email: satishhmane75@gmail.com[1], pnarwadkar@yahoo.com[2],
aditya.kedari@mituniversity.edu.in[4], sapna.deo@mituniversity.edu.in[6]

Article Info

Volume 6, Issue 6, June 2024

Received: 14 April 2024

Accepted: 11 May 2024

Published: 05 June 2024

doi: 10.33472/AFJBS.6.1.2024.5534-5541

ABSTRACT:

Cyber warfare has emerged as a prominent phenomenon in contemporary society. By numerous scholars, it is commonly referred to as the fifth domain of combat, following land, water, air, and space. The cyberspace is predominantly artificial and offers numerous distinct options for adversarial entities to get desired outcomes, even in the absence of physical force. It is a realm where anonymity is prevalent, making it challenging to establish a causal relationship between any effect, especially when compared to other natural mediums. One of the fundamental concepts of International Humanitarian Law is the principle of distinction, which is significantly undermined by this medium. The present paper examines the utilization of the principles of distinction in relation to the delineation of combatants and military objectives within the framework of cyber warfare. The analysis suggests that numerous scenarios in the context of cyber warfare have the potential to undermine the meticulous implementation of the concept of differentiation. There is a necessity to cultivate legal reasoning regarding these ambiguous areas, and one facet of such reasoning may involve recognizing cyber warfare as a distinct weapon rather than a means and tactics of warfare. This could potentially introduce novel methods to govern cyber warfare.

Keywords: Cyber, warfare, humanity, law, civilizations.

1. Introduction

The advent of computer and internet technologies has presented significant prospects for human civilizations. Both governmental entities and corporate entities are increasingly dependent on this technology for the purpose of regulation and the efficient operation of nearly all their operations. Major examples of the utilization of computer and internet technologies include atomic reactors, power grids, aviation, rail, and metro traffic controls, financial systems, and crucial and life-saving equipment at hospitals. Contemporary human societies have developed a significant reliance on computer technology, to the extent that any disruption or manipulation within this domain could potentially result in disastrous consequences. Therefore, the utilization of cyber media by nations to carry out military operations against enemies' computer systems during armed conflict is a highly appealing choice. The fundamental essence of computer technology is in the transmission of data between computer systems, facilitated by human beings. Human agency has built computer network applications to facilitate the design of data flow and desired outcomes. The connection between human agents and the specific design and outcome, albeit it may be distant, is essential. Computer programming often involves a series of intermediary automatic stages in order to achieve the desired end product. However, it is crucial to acknowledge that the initial design by a human person is also vital. The causal relationship may be distant or challenging to establish, but it is always present. A comprehensive global physical infrastructure, such as satellites, routers, and underwater cables, plays a crucial role in facilitating the intended data transfer process. Therefore, all activities occurring in the realm of cyberspace are the outcome of deliberate data transmission from one computer system or systems to another, involving intermediary stages and aided by global infrastructures.

Moreover, military actions conducted via cyber mediums encompass three crucial criteria. Firstly, the human agents responsible for data transfer encompass individuals who play a crucial role in the insertion or execution of a certain computer program within the system. The technicians involved in the construction of such a program do not automatically become involved in any conflict operations within the cyber domain. The current climate does not appear conducive to engaging in a comprehensive examination of the accumulation and development of computer programs within the context of the disarmament discussion. The second crucial element pertains to the implementation of data transfer, specifically the program itself.

The program's architecture, the intermediary processes it employs, and its dissemination over other systems are all crucial considerations in the cyber domain. The third crucial element is to the infrastructures that facilitate the movement of data. These encompass many components including as routers, sea cables, satellites, and computer systems.

The word 'cyber warfare' is a highly regarded concept, and its different definitions basically encompass two elements. Firstly, it is important to note that warfare is carried out in the realm of cyberspace through the utilization of computer network systems and programming. Put simply, it refers to the act of conducting warfare in cyberspace using cyber means and methods.[1] Thus, to kill or capture the persons involved in cyber warfare or to damage or destroy cyber infrastructure by the kinetic force are not the subject matter of cyber warfare. It, however, does not preclude the discussions about who are the persons involved in cyber warfare or to ascertain how the infrastructure supporting the cyber warfare become the military objective.

According to the second criterion, the scope is limited to acts that fall under the purview of International Humanitarian Law (IHL). According to one definition, the term "cyber warfare" specifically pertains to a limited range of cyber-attacks that can be classified as armed attacks or take place within the framework of an ongoing armed conflict. According to Cordula Droege, the term 'cyber warfare' encompasses the means and techniques of warfare that involve cyber operations that are equivalent to or carried out inside the framework of an armed conflict, as defined by International Humanitarian Law (IHL).[2]

The phrase 'cyber warfare' specifically refers to the use of cyber means and methods of warfare that are carried out within the framework of an ongoing armed conflict, as defined by International Humanitarian Law (IHL). Cybercrime and cyber terrorism are not encompassed under the scope of International Humanitarian Law (IHL). Similarly, within the scope of this article, the term 'cyber warfare' encompasses the cyber activities carried out inside the framework of an ongoing armed conflict as defined by International Humanitarian Law (IHL). The text refrains from engaging in any deliberation over the classification of a specific cyber activity as either a use of force or a threat to use of force.

This paper initially examines the distinctiveness of the cyber realm and the factors contributing to its susceptibility as a key platform for conducting conflict. In the subsequent section, an analysis is conducted on the definition of the term 'attack' and its potential interpretations when used to the context of cyber warfare. Subsequently, it briefly examines the concept of differentiation in relation to cyber warfare. This conversation has been conducted around the criteria for being recognized as combatants in cyber warfare in order to receive combatant rights and immunities, as well as the comprehension of military objectives in the cyber realm. The final section of the paper presents the conclusion and provides a list of suggestions.[3]

Specificity of Cyber Space

Cyberspace can be defined as a worldwide interconnected network of digital information and communication infrastructures, encompassing many components such as the internet, telecommunications networks, computer systems, and the information contained inside them. The cyber space, unlike other forms of combat such as land, air, sea, and space, is regulated by the laws of human technology rather than the natural laws. In natural mediums, the problem lies in uncovering the laws of nature to determine cause and effect relationships. However, in cyber mediums, the expertise regarding established rules is always being challenged by new inventions.

The cyberspace is the domain where human mind develops both the framework and the rules. Establishing cause-effect relationships in natural mediums such as land, sea, air, and space is more straightforward compared to cyberspace. Therefore, anonymity is a prevalent characteristic in the realm of cyberspace, and determining the precise origin of any given activity is consistently challenging. Furthermore, the concurrent utilization of physical infrastructures such as cables and satellites by multiple parties facilitates the execution of cyber activities. Therefore, it will be challenging to categorize the utilization of these infrastructures at any certain moment.

Currently, computer systems worldwide are highly susceptible to cyber-attacks. There are numerous factors contributing to its vulnerabilities. Firstly, this approach is highly cost-effective and requires less physical exertion to get the intended outcomes. Even in the absence of direct combat resulting in casualties, the adversary's ability to maintain a state of war might be diminished to achieve the intended outcome. Furthermore, the intricate nature of cyber operations renders them highly sought-after targets at all times. The perpetrator or assailant can simply achieve the intended outcome by possessing knowledge of one or a few vulnerabilities inside the entire system.[4]

Furthermore, the cyber medium offers the attacker advantages in terms of the challenges associated with establishing identification and attribution. The cyberspace is a realm of anonymity that is perpetually perplexed by the exact origin of the disputed cyber activity. The fourth factor is the geographical accessibility to target any region of the world from any location. This technology enables soldiers to engage in warfare remotely, while cyber attackers tend to exhibit a higher degree of emotional detachment from the consequences of their actions. There are several key factors that contribute to the increasing popularity of cyber media as a preferred framework for warfare objectives. Some researchers have referred to cyber space as the fifth domain of combat, following land, water, air, and space.[5]

The imperative for states to establish a robust and dependable cyber security framework is currently the most pressing issue at hand. Nevertheless, the cyber security problem is more formidable during times of war compared to times of peace. The war allows for the execution of military operations targeting the adversary's cyber security, as long as it has been designated as a military goal. Nevertheless, cyber security attacks during times of peace encompass matters pertaining to culpability, jurisdiction, and evidentiary support, but the difficulties surrounding cyber security attacks during times of conflict are distinct in nature. They primarily entail assessing the characteristics of military operations, the scope of the attack, and evaluating the results within the context of International Humanitarian Law (IHL). The subsequent sections will provide additional elaboration on these problems.

Attack in the Cyber Space

Prior to proceeding, it is essential to examine the definition of the term 'attack' inside the realm of cyberspace.

The primary objective of this analysis is to examine the concept of attack within the framework of International Humanitarian Law (IHL) and assess its applicability in describing activities occurring in the realm of cyberspace. It is crucial because the majority of the protections provided by IHL are specifically aimed at preventing attacks. It will enhance one's comprehension of the specific operations that will be subject to the regulation of International Humanitarian Law (IHL).

According to Article 49 of the Additional Protocol I, the term "attack" is defined as "acts of violence directed towards the adversary, regardless of whether they are made in offense or defense." The term 'acts of violence' has generated significant debate over the non-kinetic characteristics of cyber-attacks. Cyber-attacks refer to deliberate activities executed via computer networks with the intention of disrupting, denying, degrading, or destroying information within computers and computer networks. Additionally, these assaults can also result in damage to the computer network itself.

Nevertheless, the definition of attack in International Humanitarian Law (IHL) has not always been limited to the kinetic aspect and inherent violence of the object. The illustration of chemical and biological weapons holds significant relevance in this context. These weapons are non-kinetic and do not possess inherent kinetic properties. However, their use has long been acknowledged as an act of aggression due to their destructive consequences. Similarly, the cyber-attacks might be referred to as attacks based on their consequences. Nevertheless, this methodology gives rise to two inquiries pertaining to the potential consequences of the cyber-attacks. The consequences of cyber-attacks might vary, ranging from violent to non-violent outcomes. They have the potential to inflict destruction, harm (violent consequence), or just neutralize (non-violent result) the operations of some systems. Therefore, the question arises as to which specific consequences of cyber operations can be classified as attacks. There are primarily two types of methodologies that support each position. [6]

In 2002, Michael N. Schmitt put out the argument that cyber activities can only be classified as attacks under International Humanitarian Law (IHL) if they result in a violent end. He has stated that the principle of distinction outlined in article 48 of the Additional Protocol I does not apply to all types of military operations. Therefore, certain types of military operations, such as psychological operations against civilians, may fall outside the scope of this principle. The speaker emphasized that Article 48 exclusively outlaws the act of attacking civilians and civilian property, without imposing any restrictions on targeting them in different ways that do not meet the criteria for an attack.[7]

By delineating these criteria, he provided a more precise definition of assaults as actions that must result in violent outcomes. Consequently, he categorizes any cyber operations lacking such results as attacks. He believed that all other cyber operations are not prohibited and can be employed without triggering any inquiry into International Humanitarian Law (IHL). The author additionally referred to it as a permissive approach, perhaps implying that it allows for cyber targeting activities that do not result in violent outcomes. Knut Dorman advocated for the second approach, asserting that under International Humanitarian Law (IHL), an attack would encompass not only the violent outcome but also any act of neutralizing the object. The individual formulated their case regarding the concept of military objectives as outlined in article 52(2) of Additional Protocol I. A military goal refers to a target that, under the prevailing circumstances, provides a clear military advantage by its whole or partial destruction, capture, or neutralization.

Cordula Droege argues that military activities that may not be explicitly classified as attacks are still subject to scrutiny under International Humanitarian Law (IHL). However, Droege highlights a fundamental issue with Melzer's thesis, which is its failure to address the precise definition of hostilities. Moreover, in her explanation of the attack idea, she determined that an attack should also include actions that temporarily interrupt the operation of items without causing physical harm or destruction.

According to Rule 30 of the Tallinn Manual, cyber-attacks are defined as cyberoperations, regardless of whether they are offensive or defensive in nature, that are reasonably anticipated to result in harm or fatality to individuals or harm or destruction to things.[8]

Currently, experts widely agree that any disruptions to functionality of a significant level should be considered as harm and hence fall under the investigation of International Humanitarian Law (IHL) if they occur in connection with an armed conflict. The existing body of literature pertaining to the topic has progressed beyond the initial dispute between Knut Dormann and Michael N. Schmitt over the necessity of violent repercussions in any cyber activity. Nevertheless, there is a lack of consensus regarding the degree of functionality impairment, and there are attempts to quantify this threshold in relation to the efforts required to restore the previous functioning.

Therefore, the primary purpose of the functionality test is to assess the suitability of International Humanitarian Law (IHL) in relation to the specific technological requirements necessary for the restoration of the original function. This phenomenon may potentially exacerbate challenges in the advancement of novel technology, as certain technologically proficient nations may attain functionality without resorting to extreme measures, while others may require arduous endeavors to restore performance. Due to the complexity of cyber operations, accurately assessing the necessary efforts to restore functioning and determining whether specific cyber operations would be subject to IHL scrutiny would be a challenging undertaking. Therefore, even the functionality is susceptible to further challenges in comprehension. [9]

2. Conclusion

The current reality of cyber threats poses a significant risk to the cybersecurity of any nation. The aforementioned threat is amplified during periods of armed conflict due to the fact that armed conflicts provide an opportunity for the legitimate application of force against military targets. International Humanitarian Law (IHL) governs the circumstances surrounding armed conflict, and this study aims to examine the relevance of IHL in the context of cyber warfare. The field of cyber warfare has numerous obstacles, including the need to comprehend cyber-attacks, the principles of differentiation and proportionality, and other related concepts. There exist several areas that present challenges when attempting to apply the established norms of International Humanitarian Law (IHL) to the context of cyber warfare. The following areas might be briefly noted as prerequisites for combatants to differentiate themselves, the necessity of publicly carrying weapons during hostilities or before preparations, the assessment of proportionality, and the definition of military objectives, among others. The presence of difficult areas of application does not preclude the applicability of International Humanitarian Law (IHL) to the given circumstance.

International Humanitarian Law (IHL) will consistently retain its applicability in the context of armed conflict, and any cyber-attack that is connected to the continuing armed conflict will consistently fall under the purview of IHL. Even in difficult circumstances, where the direct implementation of International Humanitarian Law (IHL) is not guaranteed due to definitional and technological difficulties, the safeguard provided by the Martens Clause shall always be applied. In situations where the direct applicability of principles of International Humanitarian Law (IHL) is uncertain, the Martens clause offers protection to persons based on the values of humanity and public conscience.

Nevertheless, it is imperative to enhance international legal reasoning in order to address the ambiguous aspects of applying specific International Humanitarian Law (IHL) standards to the context of cyber warfare. There is little question that placing excessive emphasis on established international humanitarian law (IHL) conventions and treaties may lead to an excessive extension of these norms to a new reality, perhaps resulting in the emergence of inconsistencies in their application. Cyber warfare is undeniably a form of combat that utilizes novel mediums, strategies, and tools. It is challenging to assert that throughout the negotiations of the Geneva Conventions and the Additional Protocols, the actualities of cyber warfare were not even conceived. Hence, it is imperative to examine the distinct International Humanitarian Law (IHL) concerns brought to the forefront by cyber warfare.

The Tallinn Manual represents an endeavor in this regard; yet, it falls short in adequately addressing all pertinent concerns. There is a question over whether cyber warfare can be conducted in accordance with the norms of International Humanitarian Law (IHL). This inquiry pertains to the inherent feasibility of engaging in conflict using cyber methods in accordance with the standards of International Humanitarian Law (IHL). This line of reasoning is significant because if there are inherent difficulties in accurately applying principles of International Humanitarian Law (IHL), it is more appropriate to view cyber warfare not as a method or approach to warfare, but as a weapon that can be prohibited or regulated under specific conventions on weapons, especially a new one. This field of research is quite nascent and has yet to establish its own position within the scholarly conversation. The aforementioned factors represent significant concerns that have the potential to impact the advancement of this field and consequently enhance the regulation of cyber warfare.

3. References

1. Nils Melzer, 'Cyber Warfare and International Law' UNIDIR Resources 4 (2011), available at: https://unidir.org/sites/default/files/publication/pdfs/cyberwarfare-and-internatio nal-law-382.pdf (last accessed on 23 August 2023).
2. Oona A Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel, 'The Law of Cyber Attack' 100 (4) California Law Review 821 (2012).
3. Cordula Droege, 'Get Off My Cloud: Cyber Warfare, International Law and the Protection of Civilians' 94 (886) International Review of the Red Cross 538 (2012).
4. Jack Goldsmith, 'How Cyber Changes the Laws of War' 24(1) EJIL, 130 (2013)
5. Michael Grevais, 'Cyber Attacks and the Laws of War' 30(2) Berkely Journal of International Law 532 (2012).
6. Additional Protocol I to the Geneva Convention of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) of 8 June 1977. See articles, 12 (1), 41 (1), 44(3) 51 (2), 52 (1).
7. Knut Dormann, 'Applicability of the Additional Protocols to the Computer Network Attacks' (2004) 4, available at:
8. https://www.icrc.org/en/doc/assets/files/other/applicabilityofihltocna.pdf (last visited on Aug. 23, 2023).
9. Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare106 (Cambridge University Press, Cambridge, 1st ed., 2013).
10. Robert Kolb and Richard Hyde An Introduction to the International Law of Armed Conflict, 125 (Hart Publishing 2008).
11. T. M. Kulkarni and A. O. Mulani (2024). Deep Learning Based FaceMask Detection: An Approach to Reduce Pandemic Spreads. African Journal of Biological Sciences (South Africa). 6(6), 783-795.
12. Birajadar Ganesh Basawaraj, Altaf Osman Mulani, Osamah Ibrahim Khalaf, Nasren Farhah, Pravin G. Gawande, Kinage Kishor; Abdullah Hamad Abdulsattar (2024). Epilepsy Identification using Hybrid CoPrO-DCNN Classifier. International Journal of Computing and Digital Systems. 16(1).
13. Kolhe, V. A., Pawar, S. Y., Gohari, S., Mulani, A. O., Sundari, M. S., Kiradoo, G., & Sunil, J. (2024). Computational and experimental analyses of pressure drop in curved tube structural sections of Coriolis mass flow metre for laminar flow region. Ships and Offshore Structures, 1-10.
14. Mulani, A. O., Birajadar, G., Ivković, N., Salah, B., & Darlis, A. R. (2023). Deep learning based detection of dermatological diseases using convolutional neural networks and decision trees. Traitement du Signal, 40(6), 2819-2825.
15. Mane, P. B., & Mulani, A. O. (2019). High throughput and area efficient FPGA implementation of AES algorithm. International Journal of Engineering and Advanced Technology, 8(4).
16. Dr.Sapna Sukrut Deo et al. (2019). JUDICIAL REFORM: COMBATTING DELAYED JUSTICE. International Journal of Advanced Science and Technology, 28(15), 340 - 343.
17. Dr. Sapna Sukrut Deo, Prof. Dr. Pooja Prashant Narwadkar, Dr. Madhura Kalamkar, Dr. Aishwarya Yadav and Mr. Jatin Sethi (2024), Affecting computing for social justice. African Journal of Biological Sciences (South Africa). 6(6), 1610-1614.

18. Dr.Sapna Sukrut Deo et al. (2019). RIGHT TO PRIVACY BETWEEN HUSBAND AND WIFE. International Journal of Advanced Science and Technology, 28(15), 337 - 339.
19. Sarda, M., Deshpande, B., Deo, S., & Karanjkar, R. (2018). "A comparative study on Maslow's theory and Indian Ashrama system". International Journal of Innovative Technology and Exploring Engineering, 8(2), 48-50.
20. Deo, S., & Deo, S. (2019). "Cybersquatting: Threat to domain name". International Journal of Innovative Technology and Exploring Engineering, 8(6), 1432-1434.
21. Deo, S., & Deo, D. S. (2019). "Domain name and its protection in India". International Journal of Recent Technology and Engineering.