https://doi.org/10.62585/pjcj.v4i1.36

Volume and Issues Obtainable at Centeriir.org
Pakistan Journal of Criminal Justice
ISSN: 2958-9363 ISSN (E): 2958-9371
Volume 4, No.1, 2024

Journal Homepage:https://journals.centeriir.org/index.php/pjcl

Common Article 3 and Asymmetric Warfare in the Context of Cyber Operations

Muhammad Asif Safdar [1] Dr. Faiz Bakhsh[2] Saadat Ali Nadeem[3] Prof. Dr. Rao Imran Habib[4]

[1]Assistant Professor, University Gillani Law College, Bahauddin Zakariya University Multan. E-Mail: Asif.Safdar@Bzu.edu.pk
[2]Assistant Professor, University Gillani Law College, Bahauddin Zakariya University Multan. faizmalik@bzu.edu.pk
[3]Ph.D Law Scholar, Department of Law, The Islamia University of Bahawalpur. E-Mail: miansaadatali@yahoo.com
[4]Dean Faculty of Law, The Islamia University of Bahawalpur, Bahawalpur. E-Mail: Imran.habib@iub.edu.pk

ABSTRACT

International Humanitarian Law (IHL) serves as the crucial framework governing armed conflicts, seeking to humanize warfare and regulate the conduct of hostilities, whether at the international or non-international level. While the rules outlined in Common Article 3 (CA3) and Additional Protocol II (APII) pertain specifically to non-international armed conflicts (NIAC), customary international law also plays a significant role. The landscape of armed conflicts has evolved, particularly with the rise of asymmetric warfare, where adversaries may possess disparate weaponry, arsenal, or digital prowess capabilities. In the contemporary era marked by rapid digitalization, the emergence of cyber warfare introduces new challenges to IHL. Defining cyber operations within the context of armed conflicts remains an ongoing process, raising questions about the applicability and extent of IHL to cyber-attacks and establishing clear thresholds for compliance. The transformative nature of cyber warfare introduces complexities in determining the initiation, duration, and conclusion of armed conflicts. This article also explores the challenges posed by attributing cyber attacks and identifying responsible actors, crucial aspects for ensuring accountability under IHL. By examining the nuanced intersections of cyber operations and armed conflicts, the research aims to contribute to a comprehensive understanding of how IHL can effectively adapt to and govern these emerging forms of warfare in the contemporary digital age.

Article History: Received: September 12, 2023: Accepted: December 22, 2023: Published: January 02, 2024
Keywords: IHL, CA3,Cyber Warfare, Cyber Operations, Tallinn Manual , IAC , NIAC, GCs APII

Corresponding Author's Email: Asif.Safdar@Bzu.edu.pk
How To Cite: Muhammad Asif Safdar, Dr. Faiz Bakhsh, Saadat Ali Nadeem, & Prof. Dr. Rao Imran Habib. (2024). Common Article 3 and Asymmetric Warfare in the Context of Cyber Operations. *Pakistan Journal of Criminal Justice*, *4*(1), 15-23.

https://doi.org/10.62585/pjcj.v4i1.36

1. Introduction

In the rapidly evolving landscape of modern warfare, the intersection of technology and conflict has given rise to a new battleground – the realm of cyber warfare. As nations harness the power of digital capabilities, the applicability of established legal frameworks, such as Common Article 3 (CA3) of the Geneva Conventions, becomes paramount in understanding the intricacies of this emerging domain. This article delves into the nuanced relationship between CA3 and the asymmetric nature of cyber warfare, exploring how the principles of the law of armed conflict (LOAC) and the laws of war are adapting to the challenges posed by cyber actions within the context of armed conflict.

For the purposes of this exploration, "cyber warfare" refers to the spectrum of cyber actions that are not only performed within the theater of armed conflict but also those that, by their nature and impact, rise to the level of armed conflict. As we navigate this intricate terrain, we aim to shed light on the legal contours that govern cyber warfare, emphasizing the need for a comprehensive understanding of CA3 and its relevance in addressing the complexities posed by the asymmetric dynamics inherent in this evolving form of conflict. Such cyber operations, which include the development and transmission of computer code from a number of computers to target computers, may be aimed at infiltrating a computer system in order to collect, shipping, destroy, shift, or encrypt data, or at triggering, altering, or otherwise manipulating processes regulated by the infiltrated system. While such operations are directed at computers rather than people, they have the potential to inflict great human misery (Ben & Diamond, 2023).

During armed conflicts, there is a concern that cyber operations may be employed to disrupt essential infrastructure, thereby impeding the provision of critical services and resources to civilians. Critical infrastructure, including power plants, nuclear facilities, dams, water purification, and supply systems, refineries for petroleum, gas and oil pipelines, financial institutions, hospital systems, railways, and air traffic control, heavily depend on vulnerable computer systems that can be infiltrated and manipulated through cyber operations. The interconnectedness and interdependence of civilian and military computer infrastructure pose an elevated risk of harm to people and civilian objects in cyber warfare. This is due to the challenge of distinguishing between these two entities. Attacking a military computer system increases the probability of causing harm to civilian computer systems (Droege, 2012).

These services are crucial for certain civil functions, such as water and electricity supply, as well as property transfers. The existence of these risks underscores the humanitarian necessity of legislation to regulate and restrict cyber warfare. Despite efforts to enhance clarity, numerous questions persist regarding the application of existing legal frameworks to this relatively new and still poorly understood phenomenon. This article does not aim to provide comprehensive answers to all of these questions. This analysis will focus solely on the application of international humanitarian law in relation to cyber warfare, without attempting to cover all the associated legal issues (Schmitt, 2013).

Furthermore, despite focusing solely on the challenges that cyber warfare presents to international human rights law, several significant inquiries remain unresolved. This article aims to outline the key questions and challenges that need to be addressed in order for international humanitarian law to effectively uphold human dignity and prevent unnecessary human suffering in the context of emerging forms of warfare. It refrains from offering definitive answers, as the reasons for this limitation will be discussed. The article will begin by discussing the challenge of applying traditional rules of international humanitarian law to conflicts involving new techniques and methods of warfare, with a specific focus on cyber operations. The limited transparency and information surrounding cyber operations pose additional challenges to the implementation of international humanitarian law (Khan & Bhuian, 2019)

This article will discuss the challenges in determining the occurrence of cyber operations during armed conflicts. International humanitarian law exclusively applies during armed conflicts. After confirming the

presence of armed conflict, it becomes crucial to ascertain the interpretation and application of international humanitarian law rules to cyber operations. This article examines the conditions that lead to the application of international humanitarian law in cyber operations and explores the application of principles such as distinction, proportionality, and the duty to take preventive measures in the context of cyber warfare (Watson, 1995).

In this article, the author intends to chalk out an adhesive framework for the applicability of CA3 in the asymmetric nature of cyber operation scenarios. It will further elaborate on the concrete definition of the notion of the armed conflict and NIAC to determine whether cyber warfare may amount to an armed conflict. That is why this article is very significant in terms of its finding out the cyber warfare and the date is subject to IHL if it causes physical damage or not. It further indicates the version of the World, ICRC, and Pakistan regarding IHL and its cognizance over cyber warfare.

2. Research Methodology

The present study will benefit from conducting a doctrinal analysis. This study will adopt a black letter approach, prioritizing the interpretation and application of legal statutes rather than examining their practical implementation. The researcher will conduct an in-depth examination of the CA3 asymmetry and its sources, focusing on providing both descriptive and explanatory insights. The study will employ a qualitative research design, utilizing non-numerical data to comprehensively understand cyber operations and IHL. This approach focuses on obtaining in-depth insights rather than providing a superficial description based on a large population sample. The chosen research philosophy is interpretivism, which emphasizes the researcher's subjective experiences, the construction of theory through shared meanings, and the interactions and relationships between them.

3. Research Question

- This article focuses on one pivotal question: Is CA3 applicable to cyber warfare and its operations or not?
- Does cyber warfare amount to asymmetric warfare or not?

4. IHL APPLICABILITY IN CYBER OPERATIONS

To ascertain whether a specific cyber operation falls under the jurisdiction of IHL, it is essential to establish if the operation is linked to CA3 and exclusively applies within the framework of armed conflicts. Establishing the applicability of IHL in relation to cyber operations during an ongoing armed conflict is not straightforward. Complicating factors may arise, making it less self-evident (Bakhsh et al, 2021).

Establishing a definitive relationship between the operations and an armed conflict may not always be feasible. Given the anonymity often associated with cyber operations, it is not necessary to attribute these operations to a specific party involved in an armed conflict. The applicability of IHL remains uncertain as long as there is doubt regarding its connection to the armed conflict. Cases where cyber warfare occurs independently of other forms of hostilities would be particularly problematic. In these circumstances, a further inquiry arises regarding the potential classification of cyber operations as armed conflicts (Briggs, 1985).

The operations involve the employing of armed forces against another state. The issue of attribution remains challenging within the realm of cyber warfare. The adoption of suitable legal presumptions has been proposed as a potential solution to alleviate this challenge. A state would bear responsibility for cyber operations beginning from its government facilities unless proven otherwise (Rahman, 2016).

States have many times affirmed that international law does apply to cyberspace. At the UN GGE in 2017, states disagreed: the EU, France, the US, and Australia confirmed the applicability of IHL. However, their positions have met with considerable opposition from countries such as Iran, China, Russia and Cuba, which argue that the application of IHL would lead to an unnecessary militarization of

cyberspace (Amann, 1996). This led to the withdrawal of Cuba, China and Russia from the negotiations and the subsequent failure to adopt a consensus-based final report. Russia completely rejects ICT as a recognized "weapon" at the global level (Mundis, 2001).

5. CA3 and Asymmetric Warfare In the Domain of Cyber Warfare

CA3 is the small treaty within the GCs that entails protections during internal and domestic violence and wars. For the applicability of the CA3 there is only one condition there has to be a NIAC contrary to the involvement of the states. Interestingly, another intermixed phenomenon exists simultaneously with NIAC, which is AW in every NIAC. Because on the one side, there are rebels and on the other hand there is a host state. Due to this huge difference, unconventional war occurs in contrast with the rules of IHL as IHL mostly deals with the Conventional rules of IHL, particularly in the cases of IACs.But with the recent advancements in the digital world, cyber-attacks and cyber operations are increasingly taking place nationally and globally. The present articles deals with such attacks at the national level which is a more complex area already (Sassòli & Olson, 2000).

The Ca3 deals with the NIAC and the NIAC entail the idea of armed conflict in itself . But most of the NIACs are of the nature of AW because of the drastic changes and revolutionary advancement o technology, digitalization and artificial intelligence. In such complex scenario If there is a cyber-attack within the state and amongst the non-state actors and rebels, what would be the impact o this on IHL and does IHL framework regulate such a chaotic state of affairs or not? (Poisel, 2009).

6. Applying the Principle of Proportionality in Cyberspace

Principle of proportionality - e.g. computer virus that uncontrollably spreads and destroys a network shared by both civilian and military in hope that it eventually hits something military would be an indiscriminate attack (Jenks, 2013).

The primary concern in applying this principle to cyber warfare is determining whether the term "damage" encompasses the loss of functionality. Given the potential gravity of the consequences resulting from the disruption of civil infrastructure functionality, it is justifiable to include the assessment of such damage in the determination of proportionality. However, it is necessary to further specify the specific types of impairments that are considered appropriate for classification within this category (Junod, 1983).

A challenge in implementing the principle of proportionality is assessing whether the expected harm to civilian objects is excessive compared to the anticipated military benefit. The assessment of balancing potential harm to civilians or civilian objects with anticipated military benefits is consistently challenging. However, in the context of cyber warfare, these challenges are further complicated due to the inherent difficulty in accurately predicting the extent of unintended damage that may occur. The limited understanding of the impact of cyber operations is due to their recent emergence and the complex interconnectedness of cyberspace, which hinders the ability to anticipate all potential effects (Schmitt, 2014).

7. Applying the Principle of Distinction in Cyberspace

Principle of distinction - e.g., includes a prohibition on cyber attack targeting a pacemaker of a civilian or a networked insulin pump and prohibits cyber attacks on networks of a water treatment facility that provided services to only civilian populations. Therefore, it cannot be targeted for an attack. The challenge in implementing these rules in the context of cyber warfare arises from the dual-use nature of most cyberinfrastructure, which serves both civilian and military functions (Michael & Schmitt, 2011)

8. Does Cyber Warfare Fall within the Confines of Armed Conflict?

Cyber operations conducted during armed conflicts are bound by IHL specifically the rules regulating the conduct of hostilities. Implementing these rules to computer code deployment in cyberspace, rather than

physical force in the real world, is a complex task. The initial challenge lies in identifying the specific cyber operations that would fall under the purview of conduct of hostilities regulations. The relevance of this question lies in the potential of cyber operations to significantly disrupt critical infrastructure without resorting to physical destruction commonly associated with conventional warfare. In relation to cyber operations falling under the conduct of hostilities, it is important to examine how the applicable rules, particularly the principles of distinction, proportionality, and precaution, should be modified and implemented in the context of cyber warfare (Chayes, 1985).

9. Tallinn Manual and Cyber Attack (physical damage)

The Tallinn Manual is a comprehensive document that outlines that the actual and physical damage amounts to the cyber-attacks if it happens then laws germane to cyber warfare. It also provides a list of ninety-five "black rules" that govern these types of conflicts. The covered topics encompass sovereignty, responsibility for states, jus ad bellum, IHL, and the law of neutrality. The actual damage entails death , injury, and destruction (Schmitt, 2013).

10. Data is Object or not.

States view: - According to the Danish Military Manual, digital data are generally not considered to be objects. The Norwegian military manual assumes that data is considered as objects and can only be directly targeted if they meet the criteria of being legitimate targets. Please rewrite the user's text to be academic and concise. France has taken a moderate stance by asserting that material data, including civil, bank, and medical data, should be safeguarded based on the principle of distinction, considering the prevailing state of digital reliance. Peru's stance on operations against data is based on the concept of "military objective," implying that certain data systems may be exempt from attacks if such attacks do not provide a legitimate military advantage. However, no explicit position is taken on this matter. Please rewrite the user's text to be academic and concise. Chile suggests examining the consequences of data attacks and asserts that the principle of distinction should be considered in the realm of cyber operations. It is recommended that states abstain from targeting data if doing so could harm civilians (Meron, 1995). The question of whether civilian data can be considered civilian objects is still unresolved. However, the assertion that the deletion or manipulation of vital civilian data should not be prohibited appears to contradict the goals and intentions of IHL paper with digital files. The files should be replaced. Not diminish the legal protection afforded by IHL.

11. Pakistani Viewpoint

In the complex landscape of Pakistan, where gender discrimination and sexual harassment persist as societal challenges, the state has not only grappled with these internal issues but has also been a victim of cyber espionage and hacking on numerous occasions (Jamshed, 2021). Despite facing the threat of cyber attacks, the nation currently lacks robust and effective systems to protect against such acts, highlighting a critical vulnerability in its cybersecurity infrastructure. Therefore, it should proactively try to deal with cyber threats and establish cyber defense mechanisms by first identifying cyber security loopholes. Pakistan is bound by existing IHL with respect to cyber warfare and must adhere to those rules in establishing such a mechanism. However, where such regulations are inadequate, local cyber laws are relevant to determining state practice and may be modeled accordingly.as well as civilian objects and military targets. Furthermore, the use of any type of cyber weapon that causes indiscriminate harm is illegal under IHL and critical civilian infrastructure and civilian populations will be protected during cyber conflict (Hans et al, 1996). Pakistan believes that due to the interconnected nature of the Internet and related infrastructure, the existing framework of IHL needs to be modified to accommodate the needs of modern warfare so as to preserve the core principles of IHL namely discrimination, proportionality and precaution.

12. ICRC Viewpoint

Cyber operations are now integrated into armed conflicts, and there is a growing acknowledgment within the international community that the utilization of iCT in future state-to-state conflicts is increasingly probable (Henckaerts & Doswald, 2006). The ICRC has expressed its apprehension regarding the potential humanitarian consequences of cyber operations. It has previously identified specific areas of concern in this regard. In March 2021, states acknowledged that cyber operations have the potential to significantly impact civilian infrastructure, leading to severe humanitarian consequences.

The ICRC calls on States to enhance clarity regarding the constraints imposed on cyber operations by the current rules of IHL. The ICRC acknowledges that IHL places restrictions on cyber operations during armed conflict, similar to other weapons and methods of warfare employed by combatants, regardless of their novelty. This perspective is widely held by various states.

The application of IHL, particularly its principles of humanity, necessity, proportionality, and distinction, to cyber operations is currently of great importance for states (Fleck, 2006). This significance has been highlighted in a 2021 report by the Group of Governmental Experts mandated by the United Nations.

13. Conclusion

IHL has some serious issues that need to be resolved, such as the idea of the armed conflict is unclear and defined. At the same time if this is not the settled then CA3 concept and its endorsement will also be in vain. Most of the NIAC are of asymmetric nature as they entail unevenness and disparities between the adversaries. In such a scenario there is an ongoing debate on whether CW amounts to an armed conflict. So the answer to this question is complicated. Cyber warfare operates within a legal framework. Cyber operations are subject to legal regulations, particularly when they are associated with or occur during armed conflict, in which case they are governed by (IHL). Although it is widely accepted that IHL is applicable to cyber warfare, numerous unresolved questions remain regarding its implementation. The secrecy surrounding cyber operations and their distinct methods and means of warfare make it challenging to determine if they occur within armed conflict and are connected to it.

Although the applicability of IHL rules to the conduct of hostilities is widely accepted, there remains uncertainty regarding which specific cyber operations will be governed by these rules. The interpretation of long-established rules in relation to this new form of warfare lacks clarity. From a humanitarian standpoint, it is crucial to address these inquiries and ensure the effective implementation of IHL to safeguard civilians and civilian infrastructure against the detrimental impacts of cyber warfare. The task at hand necessitates a meticulous analysis of current regulations, taking into account the fundamental humanitarian objectives of IHL. It may also entail the formulation of additional, stricter regulations to safeguard humanitarian principles from being compromised.

Funding

This article was not supported by any funding from public, commercial, or not-for-profit sectors.

Conflict of Interest/ Disclosures

The authors have disclosed that there are no potential conflicts of interest concerning the research, authorship, and/or publication of this article.

References

Amann, D. M. (1999). Prosecutor v. Akayesu. Case ICTR-96-4-T. *American Journal of International Law*, 195-199.

Bakhsh, F., Anwar, M. F., Rafiq, W., & Jamshed, J. (2023). Adjustment of Due Diligence Doctrine in International Humanitarian Law: Constructing an Unobstructed Road. *Review of Education, Administration & Law*, *6*(1), 31-39.

Ben-Naftali, O., & Diamond, E. (2023). No Place for Palestinians: The Israeli High Court of Justice Fades out of the Global Community of Courts-The Farcical Tragedy of the 2022 Judgment of Masafer Yatta. *BU Int'l LJ*, *41*, 47.

Briggs, H. W. (1985). Nicaragua v. United States: Jurisdiction and Admissibility. *American Journal of International Law*, *79*(2), 373-378.

Chayes, A. (1985). Nicaragua, the United States, and the World Court. *Colum. L. Rev.*, *85*, 1445.

Droege, C. (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. *International review of the Red Cross*, *94*(886), 533-578.

Fleck, D. (2006). International accountability for violations of the ius in bello: the impact of the ICRC Study on Customary International Humanitarian Law. *Journal of Conflict and Security Law*, *11*(2), 179-199.

Han, H., Haque, I., Harland, C., Hathaway, J., Hendell, G. B., Hendley, K., ... & Rubin, A. 644 ASIL Proceedings, 1996.

Henckaerts, J. M., & Doswald-Beck, L. (2006). Droit international humanitaire coutumier.

Jamshed, J. (2021). Gender discrimination and sexual harassment in the legal profession: A perspective from patriarchal society. *Women & Criminal Justice*, 1-13.

Jenks, C. (2013). Prosecutor V. Perišić (ICTY). *International Legal Materials*, *52*(5), 1065-1116.

Junod, S. (1983). Additional Protocol II: history and scope. *Am. UL Rev.*, *33*, 29.

Khan, B. U., & Bhuian, M. N. (2019). The Development of the Geneva Conventions. In *Revisiting the Geneva Conventions: 1949-2019* (pp. 12-39). Brill Nijhoff.

Meron, T. (1995). Extraterritoriality of human rights treaties. *American Journal of International Law*, *89*(1), 78-82.

Mundis, D. A. (2001). ICTY (Appeals Chamber): Prosecutor v. Delalić (" Čelebići Case"). *International Legal Materials*, *40*(3), 626-725..

Pictet, J. S. (1952). Geneva convention. *International Committee of the red cross*.

Poisel, T. J. (2009). Prosecutor v Boskoski:(ICTY, Trial Chamber, Case No IT-04-82-T, 10 July 2008). *Australian International Law Journal*, *16*, 259-270.

Rahman, M. H. (2016). How To Approach A Problem Question On International Humanitarian Law (IHL): A Sample Answer. *Available at SSRN 4077265*.

Sassòli, M., & Olson, L. M. (2000). The judgment of the ICTY Appeals Chamber on the merits in the Tadic case. *International review of the Red Cross*, *82*(839), 733-769.

Schmitt, M. N. (2014). The law of cyber warfare: Quo Vadis. *Stan. L. & Pol'y Rev.*, *25*, 269.

Schmitt, M. N. (Ed.). (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge University Press.

Watson, G. R. (1995). The Humanitarian Law of the Yugoslavia War Crimes Tribunal: Jurisdiction in Prosecutor v. Tadic. *Va. J. Int'l L.*, *36*, 687..

Zegveld, L. (1998). The Inter-American Commission on Human Rights and international humanitarian law: A comment on the Tablada case. *International Review of the Red Cross (1961-1997)*, *38*(324), 505-511.