▪ **Citation:** Usman, H., Ahmed, R. I., & Ali, S. S. (2022). Navigating the Gray Area: A Comprehensive Analysis of Cyber Warfare and its Relationship to the Law of Armed Conflict. *Global Legal Studies Review, VII*(III), 32-36. https://doi.org/10.31703/glsr.2022(VII-III).05

Hazrat Usman [*] Raja Ishtiaq Ahmed [†] Syed Suliman Ali [‡]

Navigating the Gray Area: A Comprehensive Analysis of Cyber Warfare and its Relationship to the Law of Armed Conflict

▪ **p- ISSN:** 2708-2458 ▪ **e- ISSN:** 2708-2466
▪ **Pages:** 32 – 36 ▪ **Vol.** VII, **No.** III (Summer 2022)
▪ **DOI:** 10.31703/glsr.2022(VII-III).05
▪ **URL:** http://dx.doi.org/10.31703/glsr.2022(VII-III).05

Abstract: *This scholarly research delves into the interplay between the realms of cyber hostilities and the norms governing the law of armed conflict. It commences by meticulously defining cyber warfare and expounding upon its multiple forms, including incursions into vital infrastructure, cyber espionage operations, and the deployment of malicious software. Subsequently, the study scrutinizes the legal paradigm that regulates the deployment of military force in the realm of cyberspace, encompassing the United Nations Charter and the Tallinn Manual. Additionally, the paper conducts a thorough examination of the difficulties encountered in the application of the law of armed conflict to the realm of cyber warfare, such as the complicated nature of attributing cyber-attacks and the absence of precise regulations for proportionality. Lastly, the paper proffers constructive recommendations aimed at resolving these challenges and identifies avenues for future research. In sum, the paper endeavors to furnish a comprehensive comprehension of the legal quandaries associated with cyber warfare and possible methods to address them.*

Key Words: Cyber Warfare, Armed Conflict, International Law, Distinction Principle, Proportionality Principle

Introduction

The exponential progression of technology in contemporary times has occasioned remarkable modifications in the way wars are waged. Amongst the most notable of these transformations is the advent of cyber warfare, which pertains to the utilization of cyber abilities to conduct military operations. Cyber warfare possesses the propensity to inflict substantial harm upon a state's military, economic, and societal foundation. Nevertheless, the legal framework governing the deployment of military force in the realm of cyberspace remains in a state of evolution. The LOAC provides the paradigm for the use of force in conventional warfare, yet its application to the realm of cyber warfare remains equivocal (Gisel, Rodenhäuser, & Dörmann, 2020). This scholarly study endeavors to scrutinize the interplay between cyber warfare and the LOAC and furnish a comprehensive comprehension of the legal quandaries associated with cyber warfare. The research question of this paper is: "How can the LOAC be applied to cyber warfare?" In order to answer this question, the study will commence by meticulously defining cyber warfare and expounding upon its multiple forms. Subsequently, the study will scrutinize the legal framework that regulates the deployment of military force in the realm of cyberspace, encompassing the United Nations Charter and the Tallinn Manual. Additionally, the paper will conduct a thorough examination of the difficulties encountered in the application of the LOAC to the realm of cyber warfare, such as the complicated nature of attributing cyber-attacks and the absence of precise regulations for proportionality. Lastly, the paper will proffer constructive recommendations aimed at resolving these challenges and identify avenues for future research.

The interplay between cyber warfare and the LOAC constitutes a significant area of research as it has

[*] Lecturer, Department of Law, Mohi Ud Din Islamic University, Nerian Sharif, Azad Jammu and Kashmir, Pakistan. Email: hazratusmanadvocate@gmail.com *(Corresponding Author)*
[†] Assistant Professor/Head of Department, Department of Law, Mohi Ud Din Islamic University, Nerian Sharif, Azad Jammu and Kashmir, Pakistan.
[‡] LLM, International Islamic University, Islamabad, Pakistan.

the potential to shape the future of warfare. As stated by the Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, "the rapidly evolving cyber domain has the potential to fundamentally alter the nature of armed conflict" (Schmitt, 2017). Thus, a better comprehension of the legal issues surrounding cyber warfare is imperative for the advancement of international law and the protection of states against cyber-attacks.

Definition and Forms of Cyber Warfare

Cyber warfare refers to the employment of cyber capabilities for the purpose of executing military operations. This encompasses an array of activities, including assaults on vital infrastructure, cyber espionage, and the deployment of malware. The term cyber warfare is frequently used synonymously with the expression cyber operations; however, the latter is a more inclusive term that encompasses non-aggressive activities such as cyber defense and cyber intelligence (Schmitt, 2017). One of the most notable forms of cyber warfare is the attack on a state's critical infrastructure. Critical infrastructure pertains to the systems and assets that are essential to the functioning of a society, including power grids, financial systems, and transportation networks (Aradau, 2010). These systems are frequently regulated by computer networks, rendering them susceptible to cyber-attacks. For instance, in 2015, a cyber-attack on Ukraine's power grid resulted in a widespread power outage (Case, 2016). This occurrence illustrates the potential for cyber-attacks to inflict substantial harm upon a state's infrastructure.

Cyber espionage represents a modality of cyber warfare and refers to the utilization of cyber capacities for the purpose of obtaining confidential information from a state or organization. A noteworthy instance of cyber espionage occurred in 2014, when a group of hackers, referred to as the "APT1" group, was discovered to have perpetrated the theft of substantial amounts of confidential information from various United States organizations, including the United States government (Mandiant, 2016). This occurrence serves as an illustration of the potential for cyber espionage to inflict significant harm to a state's security. The utilization of malware, another manifestation of cyber warfare, has the capacity to cause harm to a state's infrastructure or steal confidential information. Malware, as a category of software, is engineered with the intention of causing harm to a computer system (Seemma, Nandhini, & Sowmiya, 2018). One example of the implementation of malware is the Stuxnet malware, which was discovered in 2010 and designed to target and compromise the centrifuges employed in Iran's nuclear program (Baezner & Robin, 2017). This occurrence highlights the potential for malware to inflict significant harm on a state's infrastructure. Thus, cyber warfare encompasses a multitude of forms, ranging from attacks on critical infrastructure to cyber espionage and the use of malware, all of which have the potential to cause significant harm to a state's military, economic, and societal infrastructure. As such, it is imperative to comprehend the legal framework that governs the utilization of force in cyberspace, which will be the focus of the subsequent chapter.

Legal Framework Governing the Use of Force in Cyberspace

The current paradigm of legal administration that regulates the deployment of combative force in the virtual realm of cyberspace is still in its formative stage. The principal repository of global jurisprudence pertaining to the utilization of forceful means is embodied in the United Nations Charter (Charney, 2001). Article 2(4) of the UN Charter proscribes the implementation of any exertion of force that imperils the territorial coherence or sovereign autonomy of a state (Nations). Regrettably, the UN Charter does not offer a comprehensive and explicit account of the phenomenon of cyber warfare. The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, a compendium of insights proffered by an assemblage of worldwide legal scholars, serves as a source of guidance on the interpretation of international law as it pertains to operations within the domain of cyberspac (Schmitt, 2017) e. The Tallinn Manual asserts that the principles of discrimination and proportionality, being fundamental tenets of the LOAC, are also applicable to cyber operations. The principle of discrimination necessitates those military operations be focused on military objectives, while the principle of proportionality mandates that the harm inflicted by military operations must be commensurate with the military advantage accrued. The application of the LOAC to the realm of cyber warfare, however, is not a matter of simple resolution, owing to the challenge of attribution in cyber-attacks. Attribution refers to the identification of the entity responsible for a cyber-attack, a task that can be challenging given the potential for cyber-attacks to be executed via a diverse array of devices, such as personal computers and mobile phones, and to traverse numerous countries en route to their target, thereby complicating the determination of the origin and therefore the responsible party of a cyber-attack (Pascucci, 2017).

An additional obstacle to the imposition of the LOAC in the arena of cyber warfare is the absence of explicit regulations governing the principle of proportionality. The LOAC stipulates that the magnitude of damage inflicted by military operations must be commensurate with the military advantage derived therefrom. However, it can prove to be a daunting task to assess the extent of harm resulting from a cyber-attack and to quantify the military advantage procured (Pascucci, 2017). Hence, the legal framework that regulates the deployment of forceful means in cyberspace remains a work in progress and the application of the LOAC to cyber warfare is not a matter of simplistic resolution. Although the Tallinn Manual provides valuable perspectives for evaluating cyber-attacks, it should be noted that the recommendations it offers are not definitive or authoritative. The issue of whether a given cyber operation constitutes a violation of the LOAC remains subject to subjective interpretation (Denning, Blanken, Rothstein, & Lepore, 2015). The challenges of attribution and proportionality must be ameliorated to effectuate the effective application of the LOAC to cyber warfare. The subsequent chapter will examine these challenges in greater detail.

Challenges of Applying the Laws of War to Cyber Warfare

The implementation of the LOAC in the realm of cyber warfare is a matter of intricate complexity and requires the resolution of several hindrances. The occurrence of cyber warfare has become more widespread in recent times, with numerous nations augmenting their cyber proficiency and exploiting it as a strategic instrument. Nevertheless, the application of the LOAC to cyber warfare has proved to be an intricate and arduous task. This section will elaborate on some of the principal obstacles that have arisen in the implementation of the LOAC to cyber warfare and will scrutinize the endeavors that have been initiated to surmount these obstacles.

The implementation of the LOAC in the realm of cyber warfare is a complex and arduous task, with several obstructions that must be surmountable. One such challenge is the identification of when a cyber-attack constitutes an armed attack, as the LOAC defines an armed attack as a "hostile act committed by the armed forces of a State, purposed towards inducing injury to persons or damage to objects or creating a perilous scenario (Schmitt, 2012) ". However, attributing cyber-attacks to specific state or non-state actors can be a formidable challenge, making it hard to classify such attacks as armed attacks (Rid & Buchanan, 2015). The classification of what constitutes a "cyber weapon" is another daunting task, as international law does not have a clear definition for this term, which creates ambiguity between what is considered a cyber weapon and what is considered a dual-use item. This creates further difficulties in determining when the usage of a cyber weapon violates the LOAC (Rowe, 2007). Lastly, the application of the principles of distinction and proportionality within the realm of cyber warfare also poses a challenge, as the principle of distinction mandates that military targets be distinguishable from civilian targets, and the principle of proportionality necessitates that harm inflicted upon civilians be proportionate to the military advantage derived (Pascucci, 2017). However, it is often challenging to determine the target of a cyber-attack, as well as to calculate the harm inflicted and its proportionality to the military advantage gained (Hathaway, et al., 2012).

In light of these difficulties and obstacles, a number of endeavors have been launched to tackle them. One such instance is the release of the "Tallinn Manual on the International Law Applicable to Cyber Warfare" in 2013, which provides insightful directives on the implementation of the LOAC in the domain of cyber warfare (Schmitt, 2013). Additionally, the International Committee of the Red Cross (ICRC) has proffered a suite of interpretive guidelines on the implementation of the LOAC in relation to cyber warfare (Crawford, 2013). Consequently, the implementation of the LOAC in the arena of cyber warfare poses a complex and challenging task, owing to the challenges of determining the threshold at which cyber-attacks can be deemed an armed attack, the lack of a clear definition of the term "cyber weapon" and the difficulty in applying the principles of distinction and proportionality within the realm of cyber warfare. Nevertheless, the concerted efforts of the Tallinn Manual and the ICRC interpretive guidelines are noteworthy attempts at addressing these hurdles.

Recommendations and Future Research

The complexities and intricacies associated with the adaptation of the LOAC to the realm of cyber warfare necessitate the resolution of various hurdles, such as the intricacies of attributing cyber-attacks and the absence of unambiguous regulations for proportionality, in order to achieve an effective and practical application of the LOAC to the domain of cyber warfare (Buchan & Tsagourias, 2012). One possible solution to the challenge of attribution is the development of international norms and standards for incident response and information sharing. These

norms and standards could provide a framework for determining the origin of a cyber-attack and for sharing information about the attack. This would make it easier to attribute cyber-attacks and to determine who is responsible for the attack (Schmitt, 2017). Another possible solution is the development of clear rules for proportionality. These rules could provide guidance on how to calculate the level of harm caused by a cyber-attack and how to calculate the military advantage gained. This would make it easier to apply the principle of proportionality to cyber warfare (Schmitt, 2017).

To tackle the predicament of differentiating between cyber endeavors that target military objectives and those that focus on civilian objectives, a feasible strategy is to establish the differentiation between military and civilian objects within the purview of cyber operations. This can be achieved by formulating a definition of a military objective in the realm of cyber operations and proffering directives to differentiate a cyber operation that is directed towards a military or civilian objective (Schmitt, 2017).

Another crucial aspect that requires further examination is the tenet of "active defense" in cyberspace. This encompasses a comprehensive study of the lawful and ethical ramifications of active defense measures such as penetration assessment, intrusion detection, and intrusion mitigation, as well as the establishment of global norms and standards in this domain. Furthermore, further investigation is imperative to deal with the difficulties in the application of LOAC to newfangled technologies, such as artificial intelligence and quantum computing, that could potentially be utilized in cyber operations.

In conclusion, there are numerous challenges that necessitate resolution in order to apply LOAC to cyber warfare with effectiveness. The establishment of international norms and standards for incident response and information dissemination, the creation of explicit rules for proportionality, and the clarification of the distinction between military and civilian objects in the cyber context are potential answers to these challenges. Moreover, additional research is imperative on the subject of active defense in cyberspace and the utilization of emerging technologies in cyber operations.

Conclusion

This scholarly treatise has meticulously scrutinized the conjunction of cyber hostilities and the LOAC. The analysis commenced by defining the concept of cyber warfare and delving into its various manifestations, such as incursions into critical infrastructure, cyber espionage, and the deployment of malware. The paper then probed the legal milieu that governs the employment of force in the cyberspace domain, encompassing the United Nations Charter and the Tallinn Manual 2.0 on the International Law Relevant to Cyber Operations. The paper also analyzed the intricacies associated with the application of LOAC to cyber warfare, including the intricate challenge of attributing cyber-attacks and the paucity of unambiguous rules of proportionality. The paper proffered several potential remedies to these difficulties, including the formulation of global norms and standards for incident response and information exchange, the creation of clear rules of proportionality, and the clarification of the differentiation between military and civilian objects within the context of cyber operations. Additionally, the paper advocated for further research into the area of active defense in cyberspace and the exploitation of emerging technologies in cyber warfare. In essence, the paper aimed to provide an in-depth appreciation of the legal quagmires surrounding cyber hostilities and potential ways to address them. The junction of cyber hostilities and the LOAC is a critical area of study, as it holds the potential to shape the future of warfare. As the utilization of cyber operations in warfare continues to escalate, the legal framework governing their employment must be refined and comprehended. As Schmitt (2017) astutely posits, "the rapidly evolving cyber domain has the capability to fundamentally transform the nature of armed conflict" (Schmitt, 2017)", thus, an enhanced understanding of the legal intricacies surrounding cyber hostilities is crucial for the advancement of international law and the safeguarding of states against cyber-attacks.

References

Aradau, C. (2010). Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue, 41*(5), 491–514. https://www.jstor.org/stable/26301166

Baezner, M. & Robin, P. (2017). *Stuxnet, Zurich*: ETH.

Buchan, R., & Tsagourias, N. (2012). Cyber War and International Law. *Journal of Conflict and Security Law, 17*(2), 183–186. https://doi.org/10.1093/jcsl/krs016

Case, D. U. (2016). *Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (E-ISAC)*, 388, 1–29.

Charney, J. I. (2001). The use of force against terrorism and international law. *American Journal of International Law, 95*(4), 835–839.

Crawford, E. (2013). Virtual Backgrounds: Direct Participation in Cyber Warfare. *ISJLP, 9*(1), 1–19.

Denning, D. E., Blanken, L., Rothstein, H. & Lepore, J. (2015). *Assessing cyber war*: Assessing War, 266–284.

Falliere, N., Murchu, L. O. & Chien, E. (2011). W32. stuxnet dossier. White paper, symantec corp., *security response, 5*(6), 1–69. https://www.wired.com/images_blogs/threatlevel/2010/11/w32_stuxnet_dossier.pdf

Gisel, L., Rodenhäuser, T. & Dörmann, K., 2020. Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts. *International Review of the Red Cross, 102*(913), 287–334.

Hathaway, O. A. et al. (2012). The law of cyber-attack. *California law review, 100*(817), 817–885.

Mandiant, A.P.T. (2016). *Exposing One of China's Cyber Espionage Units, Alexandria*: VA: Mandiant 2013.

Nations, U. (n.d). *Charter of the United Nations, 1945*, 1 UNTS XVI. https://www.un.org/en/about-us/un-charter

Pascucci, P. (2017). Distinction and Proportionality in Cyberwar: Virtual Problems with a Real Solution. *Minnesota Journal of International Law, 26*, 419–460. https://scholarship.law.umn.edu/mjil/257

Rid, T., & Buchanan, B. (2014). Attributing Cyber Attacks. *Journal of Strategic Studies, 38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Rowe, N. C. (2007). War Crimes from Cyber-weapons. *Journal of Information Warfare, 6*(3), 15–25. https://www.jstor.org/stable/26503486

Schmitt, M. N. (2012). *"Attack" as a term of art in international law: The cyber operations context*. Tallinn, NATO CCD COE Publications.

Schmitt, M. N. (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare. Ist ed.* Cambridge: Cambridge University Press.

Schmitt, M. N. (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations. 2017 ed. Cambridge:* Cambridge University Press.

Seemma, P. S., Nandhini, S. & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125–128.