NAVIGATING LEGAL FRONTIERS IN CYBER WARFARE: INSIGHTS FROM THE RUSSIA-UKRAINE CONFLICT

Ahmad Khalil,* Mohammad Bitar,** S. Anandha Krishna Raj***

Abstract: *Cyberspaces can be significantly influenced by simple tools and tactics, and offer cost-effective solutions for states to achieve their objectives. However, it can also be used for conducting cyberwarfare, and its effects remain in gray areas. The spectrum of cyberwarfare activities ranges from minor web disruptions to crippling attacks on critical national infrastructures. Nevertheless, cyberattacks present a unique challenge in applying well-established humanitarian legal principles, particularly regarding the distinction between civilian and military targets. This is because of the interconnectedness and shared infrastructure of cyberspace between civilian and military entities, which blurs the lines between combatants and civilian populations. This article seeks to shift the general perception of the problems associated with this manner of conducting hostilities by building on the learning of the Russian-Ukrainian conflict. Furthermore, the authors examine the cyber activities that occurred during the conflict and the legal and ethical challenges that arise from classifying these activities and applying international law. They try to distinguish cyber activities as an act of force or armed attack, with a focus on determining the criteria that played a role in this classification, in light of Articles 2 (4) and 51 of the UN Charter. With reference to the United Nations (UN) Charter and the principles of self-defence, the concept of attack is scrutinised. Furthermore, the article addresses the principles of distinction and proportionality in relation to qualified cyber activities as an armed attack in the same conflict, emphasising the importance of the principle of proportionality in assessing cyber warfare.*

Keywords: *Cyberwarfare, International humanitarian law, Use of force, Armed attack, Distinction, Proportionality, Russia-Ukraine conflict*

INTRODUCTION

The emergence of cyberwarfare presents a paradigm shift in modern warfare dynamics, leveraging sophisticated computer technologies to potentially redefine military strategies.[1] Through cyberspace, armed forces can unleash havoc, causing harm, loss of life, and widespread devastation.[2] This spectrum of cyberwarfare activities ranges from minor web disruptions to crippling assaults on critical national infrastructure. While minor disruptions like defacing government websites may seem inconsequential, the threat of disseminating false information to military leaders or launching coordinated attacks on vital systems such as electricity, water, communication, transportation, and fuel networks poses grave risks to both military personnel and civilians. Moreover, the infiltration of state information networks and the covert acquisition of classified data, known as cyber espionage, are

* Mr. Ahmad Khalil, Research scholar, Vellore Institute of Technology, VIT University, School of law, Chennai, Tamil Nadu, India. ORCID: 0009-0007-0615-9812.
** Mr. Mohammad Bitar, Research scholar, VIT-AP University, School of Law, Amravati, Andhra Pradesh, India. ORCID: 0000-0003-4686-7411.
*** Dr. S. Anandha Krishna Raj, Associate Professor, Vellore Institute of Technology, VIT University, School of law, Chennai, Tamil Nadu, India. ORCID: 0009-0001-0177-1689.
[1] BARKHAM, J. Information Warfare and International Law on the Use of Force. *NYUJ Int'l L. & Pol.* 2001, Vol. 34, p. 57.
[2] BROWN, D. A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. *Harv. Int'l L.* 2006, Vol. 47, p. 179.

facilitated by the increasing reliance of government agencies on electronic communication channels.

The concept of cyber warfare, while widely understood in abstract terms, remains challenging to define within military and civilian contexts. While it may not be conventional warfare, it's evident that various actors, including states, engage in cyber activities for intelligence, military, and economic purposes, often without public disclosure of their actions.[3] Despite limited public information, certain attacks, potentially state-sponsored, have disrupted communications, targeted nuclear research, national media, and industries, while others aimed at corporate espionage to bridge military capability gaps.

Changing this sentence to: Example the "Machete" campaign illustrates how relatively simple tools and tactics can achieve significant impact in cyberspace, offering states a cost-effective means to pursue their objectives.[4] These instances highlight the evolving landscape of cyber warfare and the increasing role of state-influenced actors in shaping geopolitical events. With a defined understanding of cyberattacks in place, attention turns to the technical environment where these operations unfold.

The legal frameworks delineating the terms 'cyberattack' and 'cyber warfare' encompass various sources, one of which is the Tallinn Manual on International Law Applicable to Cyber Warfare. This source defines a cyberattack as "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects".[5] This definition excludes cyber operations not anticipated to result in injury, death, or destruction, typically falling outside the scope of *jus ad bellum* owing to their failure to meet the conventional severity thresholds associated with the application of force.

The distinctive features of cyber warfare, often referred to as 'information warfare', pose notable challenges for both jus ad bellum (the law governing the justification for the use of force) and jus in bello (the law regulating conduct during war).[6] Despite the potential for cyberwarfare to be highly destructive, it currently exists in legal gray areas.

The utilisation of cyber warfare techniques in asymmetrical warfare emphasises the importance of establishing a universally recognised and respected code of conduct.[7] Consequently, the distinction between different cyber activities and their classification as either a use of force or an armed attack, as well as the correlative right to self-defence, has emerged as a critical factor in international law.[8]

---

[3] RID, T. Cyber war will not take place. *Journal of strategic studies*. 2012, Vol. 35, No.1, pp. 5–32.

[4] This reference to be changed to: Besenyő, J. Low-cost attacks, unnoticeable plots? Overview on the economical character of current terrorism. Strategic Impact. 2017, Vol. 63, pp. 83–100.

[5] SCHMITT, M. N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press. 2013 p. 42.

[6] BARKHAM, J. *Information Warfare and International Law on the Use of Force*. p. 57.

[7] BROWN, D. *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*.

[8] JENSEN, E. T. Computer attacks on critical national infrastructure: A use of force invoking the right of self-defense. *Stan. J. Int'l L.* 2002, Vol. 38, p. 207.

I. THE NUANCED DISTINCTIONS BETWEEN CYBER ACTIVITIES

When examining the complex domain of international law concerning cyber activities, it is crucial to differentiate between cyberattacks, cyber-intrusions, and cyber-espionage. These distinctions are of paramount importance in determining whether an action constitutes a use of force or an armed attack, concepts governed by the UN Charter, and laws that pertain to armed conflict.

An effects-based interpretation of "force" or "armed attack" concerning cyber activities is often preferred, focusing on the consequential effects rather than the action itself.[9] Under this approach, certain activities such as cyber espionage or intelligence collection may not be considered prohibited force since they do not result in direct or indirect destructive consequences akin to a military attack.[10] This perspective underscores the complexity of developing clear legal positions on illicit force in cyberspace, particularly due to divergent policy priorities among key stakeholders in various agencies. These priorities range from safeguarding military capabilities, intelligence gathering, protecting civilian infrastructure, to transnational law enforcement. Such diversity in objectives complicates the consensus on legal boundaries and the pursuit of clarity in this domain.

However, the espionage through cyber exploitation may be highly invasive, it does not necessarily amount to a use of force unless there is non-consensual physical penetration of the target state's territory.[11] Moreover, the presumptive legitimacy of cyber operations is another aspect to consider. International law tends to be prohibitive, implying that acts not expressly forbidden are presumptively legitimate.[12] Activities like propaganda, psychological warfare, or espionage, when conducted through cyber means, are generally deemed legitimate unless explicitly prohibited.

Moving from the nuanced differentiations among cyber activities, attention now turns to elucidating actions that meet the criteria for a use of force or an armed attack within the domain of cyber warfare.

II. RESTRICTIONS ON THE APPLICATION OF FORCE AND THE CONCEPT OF SELF-DEFENCE

In his article "Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense", Eric Talbot Jensen explores complex questions surrounding the interpretation of the term "force" within the context of international law. Published in the esteemed Stanford Journal of International Law in 2002,[13] Jensen's work delves into whether the term "force" is limited to armed force or extends to encompass economic and political coercion. This discussion references the principles outlined in the Vienna Con-

[9] WAXMAN, M. C. Cyber Attacks as "Force" under UN Charter Article 2 (4). *Int'l L. Stud.* 2011, Vol. 87, p. 48.
[10] KURU, H. Prohibition of use of force and cyber operations as "force". *Journal of Learning and Teaching in Digital Age*. 2017, Vol. 2, No. 2, pp. 46–53.
[11] BROWN, G., POELLET, K. The customary international law of cyberspace. *Strategic Studies Quarterly*. 2012, Vol. 6, No. 3, pp. 126–145.
[12] KURU, H. *Prohibition of use of force and cyber operations as "force"*.
[13] JENSEN, E. T. Computer attacks on critical national infrastructure: A use of force invoking the right of self-defense. *Stan. J. Int'l L.* 2002, Vol. 38 p. 207.

vention on the Law of Treaties 1969 (VCLT), which provides guidelines for interpreting treaties. According to Article 31 of the VCLT, terms within a treaty should be understood in an ordinary sense, considering the treaty's purpose and objectives.[14] Some argue that since Article 2(4) of the UN Charter does not qualify the term "force", and given the Charter's emphasis on maintaining international peace and security, the prohibition should apply to all forms of force, including economic and political coercion.[15] However, opposing views suggest that considering the UN Charter's primary aim of limiting the use of armed force, the term "force" should specifically refer to armed force.

Additionally, the interpretation of the term "force" in Article 2(4) intersects with the definition of "armed attack", a pivotal aspect for delineating the parameters of self-defence as outlined in Article 51 of the UN Charter. The International Court of Justice (ICJ) has confronted this issue in landmark cases such as Nicaragua[16] and Oil Platforms.[17] In these instances, the ICJ introduced the "scale and effects" test to discern the difference between an armed attack and lesser use of force. According to this test, an armed attack, when identified, triggers the right to self-defence under Article 51, while instances of lesser force may not warrant such a response. This distinction underscores the significance of the severity necessary to justify invoking the right to self-defense, highlighting the requisite gravity in the application of force.[18]

Furthermore, some scholars advocated for an effects-based approach to defining "armed force," which considers the impact on life and property rather than solely focusing on kinetic force.[19] This interpretation is particularly relevant in modern contexts like cyber warfare, where traditional notions of force may not apply directly.

Ultimately, while there is textual support within the UN Charter for both broad and narrow interpretations of Article 2(4), the generally accepted view, supported by preparatory materials and ICJ jurisprudence,[20] is that the prohibition primarily concerns armed force. However, ongoing developments in international law, especially regarding the nature of force in the modern world, continue to shape interpretations of Article 2(4) and its implications for international relations and security.

II.1 Cyberattack as a use of force

Rule 10 of the Tallinn Manual stipulates that any cyber operation that infringes upon a state's territorial integrity or political independence, or contravenes UN provisions, is prohibited.[21] The debate surrounding the use of cyber force centres on whether an action by a state or non-state actor breaches this prohibition. In the "Case Concerning Military and Paramilitary Activities in and Against Nicaragua", ICJ did not interpret the use of force

[14] AUST, A. *Modern treaty law and practice*. Cambridge: Cambridge University Press, 2013, p. 235.
[15] TUNKIN, G. I. *Law and force in the international System*. Moscow: Progress Publishers Moscow, 1985, p. 338.
[16] Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America); *Merits, ICJ*, 27 June 1986.
[17] Case Concerning Oil Platforms (Islamic Republic of Iran v. U.S.), Judgment, 2003 *ICJ,* 161, 51.
[18] DINSTEIN, Y. *War, aggression and self-defence*. Cambridge: Cambridge University Press, 2017, p. 209.
[19] BROWNLIE, I. *International law and the use of force by states*. Oxford: Oxford University Press,1963, p. 362.
[20] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States of America). *ICJ Rep,* 1986, para 202.
[21] SCHMITT, M. N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. 2013, pp. 42–43.

strictly. Instead, it deemed that providing support to the contras through arming and training could be considered as involving force, whereas mere financial aid did not constitute force.[22] Additionally, the ICJ determined that offering rebels with weapons, logistical support, or other forms of assistance could amount to force or threaten it. As a result, non-destructive cyber activities, like providing malicious software or training for its use in rebels, may be considered as force.[23] Rule 11 of the Tallinn Manual sets out criteria for determining whether an act is forceful. According to this rule, a cyber operation is considered a use of force if its scale and effects are comparable to those of non-cyber operations that amount to force.[24] The Tallinn Manual employs an effect-oriented approach, examining seven factors: severity, immediacy, diversity, invasiveness, measurability, presumptive legitimacy, and state responsibility, as summarised by Priyanka. Dev.[25]

II.2 CYBERATTACK AS AN ARMED ATTACK

Article 51 of the UN Charter stands as the foundational principle affirming a country's inherent entitlement to defend itself in the face of an "armed attack." However, the exact definition and scope of what constitutes such an attack have long been subjects of interpretation and qualification. Prior to the 9/11 events, an armed attack was typically viewed as constituting the substantial deployment of military power by state entities across international boundaries, which gave rise to significant repercussions.[26]

The scene underwent a significant transformation following the 9/11 incidents, leading to a more recent interpretation that recognised the potential for non-state actors to employ unconventional methods of force as armed attacks. This change was evidenced when France invoked the common defence clause of Article 42(7) of the Treaty on the Functioning of the EU, citing Article 51 of the UN Charter, in response to the Bataclan terrorist attacks in Paris.[27] This event further strengthened the evolving understanding of armed attacks to include acts perpetrated by non-state actors.

Furthermore, the advent of cyber warfare has added layers of complexity to the debate. The question of whether and when digital actions in cyberspace can constitute armed attacks, especially when not accompanied by conventional military force, remains unresolved. Despite contributions from scholars, international organizations, coalitions, and states, a definitive conclusion has yet to be reached.

This perspective, supported by both the Tallinn Manual and the International Group of Experts, highlights the evaluation of armed attacks based on their outcomes.[28]

---

[22] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), *I.C.J.* 1986, para. 195.
[23] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), *I.C.J.* 1986, para. 195.
[24] SCHMITT, M. N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press. 2013, p. 45.
[25] DEV, P. R. Use of force and armed attack thresholds in cyber conflict: The looming definitional gaps and the growing need for formal UN response. *Tex. Int'l LJ.* 2015, Vol. 50, p. 389.
[26] GILL, T. D. *Legal basis of the right of self-defence under the UN Charter and under customary international law.* Oxford: Oxford University Press, 2010, pp. 216–217.
[27] DUCHEINE, P. A. L., BODDENS HOSANG, J. F. R. *Implementing Article 42.7 of the Treaty on European Union: Legal Foundations for Mutual Defence in the Face of Modern Threats*. Amsterdam: Amsterdam Law School Research Paper, 2020.
[28] RÜDIGER, W.,VON BOGDANDY, A., LACHENMANN, F. *The Max Planck Encyclopedia of Public International Law*. Oxford: Oxford University Press, 2012, p. 21.

In the field of cyber warfare, entities that are organised for cyber warfare have the capability to launch attacks on states that could potentially meet the criteria for an armed attack. If such cyber assault results in harm to individuals or property, it triggers the targeted state's right to self-defence. This right is invoked when the state that hosts the cyberattacks shows either an unwillingness or an inability to prevent these actions.[29]

The practical implications of the preceding discussion on the interpretation of cyberattacks that constitute the use of force and armed attack, as well as the evolving landscape of cyber warfare, are exemplified in notable cases such as the Stuxnet and Aramco incidents. These cases illuminate the complexities of applying international legal principles to modern cyber threats and underscore the necessity for comprehensive frameworks to effectively address them. Later in this article, we'll delve into the legal intricacies surrounding the large-scale Russian cyberattacks on Ukraine, which pose unique challenges in determining their legal implications.

III. SIGNIFICANT CYBER INCIDENTS

The Stuxnet cyberattack on Iran's Natanz nuclear facility in 2010 presents a complex scenario that intersects with international legal principles regarding the use of force and cyber warfare. Stuxnet, a sophisticated malware virus, targeted the centrifuges used for uranium enrichment at Natanz, aiming to disrupt Iran's nuclear program. By covertly manipulating the rotor speeds of the centrifuges, Stuxnet caused physical damage to the equipment, rendering them inoperable. This deliberate act of sabotage resulted in significant setbacks to Iran's uranium enrichment efforts.[30]

The Stuxnet attack prompts significant enquiries regarding the application of international law, particularly concerning the prohibition of the use of force, as outlined in Article 2(4) of the UN Charter. Functioning as an effect-based prohibition, Article 2(4) evaluates the consequences of an action, rather than its means. Hence, the assessment of whether the Stuxnet attack constituted an illegal use of force depends on the degree of physical damage caused.

While Iranian officials downplayed the impact of Stuxnet, claiming it only caused minor disruptions,[31] other reports suggest that the damage was far more severe[32]. The Institute for Science and International Security asserts that Stuxnet's manipulation of centrifuge speeds induced excessive vibrations, leading to the destruction of a significant number of centrifuges at Natanz.[33] This physical destruction of property, if proven, would constitute a violation of Article 2(4) of the UN Charter. Furthermore, the Stuxnet attack repre-

[29] DEEKS, A. S. Unwilling or unable: toward a normative framework for extraterritorial self-defense. *Va. J. Int'l L.* 2011, Vol. 52, p. 483.

[30] Creators, What Stuxnet'S. To Kill a Centrifuge. 2013.

[31] NAKASHIMA, E., WARRICK, J. Stuxnet was work of US and Israeli experts, officials say. In: *The Washington Post* [online]. 2. 6. 2012 [2024-04-29]. Available at: <https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html>.

[32] Albright, David, Paul Brannan, and Christina Walrond. "Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant?". Institute for Science and International Security, 2010.

[33] ALBRIGHT, D., BRANNAN, P., WALROND, C. Did Stuxnet take out 1,000 centrifuges at the Natanz enrichment plant? In: *Institute for Science and International Security* [online]. 22. 12. 2010 [2024-04-29]. Available at: <https://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/>.

sents a significant escalation in cyber warfare, as it targeted critical infrastructure of a sovereign state. Unlike previous cyber incidents, which primarily targeted information systems without causing physical harm,[34] Stuxnet directly impacted a nation's industrial capabilities. This raises legal questions regarding the classification of cyberattacks and their implications under international law.

Similarly, the Shamoon virus, unleashed on Saudi Aramco's network in 2012, revealed its highly destructive nature as it rendered over 30,000 computers unusable by erasing data and replacing it with an image of a burning American flag.[35] The operations carried out by Shamoon caused severe disruption to Aramco's operations, resulting in the shutdown of internal corporate networks and extensive damage to crucial files such as documents and spreadsheets. The principle of noninterference, which is a customary rule, prohibits this type of interference. The consequences of interference, whether through the use of force or armed attack, can be severe and may result in physical harm. Therefore, such actions invoke the right to self-defence, which is enshrined in Article 51 of the UN Charter.

The Stuxnet and Aramco incidents illustrate the pressing need for comprehensive legal frameworks to address cyber threats and regulate state behaviour in the online realm. Defining terms, such as cyberattacks and "cyberattack" and "cyber warfare" with precision, is crucial for evaluating the legality and proportionality of state reactions to cyber incidents. The Tallinn Manual provides a definition that emphasises the significance of the impact on individuals or objects as the primary determinant.

The recent cyber warfare against Ukraine during the Russian-Ukrainian conflict adds another layer to the discussion. Unlike the Stuxnet and Aramco incidents, where material damage was evident, assessing the impact on Ukraine necessitates a nuanced examination due to the less clear material damage inflicted. Determining whether these actions constitute the use of force and an armed attack will require careful consideration of the evolving landscape of cyber warfare and its implications under international law.

IV. THE PRINCIPLE OF DISTINCTION IN CYBER WARFARE

The use of cyber weapons should not violate the principles of distinction and proportionality, similar to other weapons. However, cyberspace is an amorphous domain by nature, and identifying perpetrators of cyberattacks is challenging.[36] These characteristics of cyber warfare present difficulties in applying the norms of jus in bello to the virtual realm.

IV.1 The Distinction in context of human targets

International humanitarian law (IHL) has long served as a framework for mitigating civilian harm during armed conflict. IHL offers clear definitions: combatants directly involved in hostilities are considered legitimate military targets Article 43 of Additional Protocol I

[34] Ibid.
[35] AL-RAWI, A. *Cyberwars in the Middle East.* New Brunswick: Rutgers University Press, 2021.
[36] BIJU, J. M., GOPAL, N., PRAKASH, A. J. Cyber-attacks and its different types. *International Research Journal of Engineering and Technology.* 2019, Vol. 6, No. 3, p. 4849.

1977 (API) to Geneva Conventions 1949, while civilians generally enjoy protection from attack (Article 50(1)) of API.[37] However, the rise of cyberspace as a battleground throws a wrench into these clear-cut distinctions.

Operating the complex IT systems that underpin cyberwarfare often necessitates civilian involvement. This blurs the line between those directly fighting and those providing crucial technological support. Programmers, network specialists, and even everyday citizens maintaining critical infrastructure can all be unwittingly drawn into the conflict. The International Committee of the Red Cross (ICRC) attempted to address this grey area with the concept of "continuous combat function." This concept suggests that civilians engaged in activities directly preparing, executing, or commanding hostile acts could lose their protected status.[38] However, such attempts at clarification only create further ambiguity. The difficulty lies in pinpointing the exact threshold of "direct participation" that strips away civilian protections.[39] Is creating malware considered direct participation? What about maintaining a server used for cyberattacks? These questions remain hotly debated within the international community.

The very nature of cyberspace poses additional challenges to applying traditional IHL frameworks. The requirement for combatants to wear distinctive uniforms (Article 44(3) of the Geneva Conventions) is rendered irrelevant in this anonymous environment.[40] Cyberattacks can be launched from anywhere in the world, often exploiting civilian networks as a springboard. This makes it extremely difficult to identify attackers and distinguish them from legitimate targets.[41] The traditional concept of carrying arms openly becomes obsolete when the weapon itself is digital code that can be easily replicated and deployed from anywhere.

These complexities and the inherent anonymity of cyberspace pose significant challenges to applying the principle of distinction, a cornerstone of IHL. This principle emphasizes the importance of differentiating between combatants and civilians during warfare to minimize civilian casualties[42]. The inability to effectively differentiate between the two in cyberspace creates a situation where civilians are potentially more vulnerable to attack. Additionally, the lack of clear lines between combatants and civilians makes it difficult to hold attackers accountable for violations of IHL. This, in turn, fosters an environment where cyberattacks can be launched with a greater degree of impunity.

IV.2 The Distinction in context of non-human target

Cyberspace presents a unique challenge when it comes to applying established humanitarian legal principles, particularly in regards to distinguishing between civilian and mili-

[37] Additional protocol I of GCs, Article 50(1).
[38] MELZER, N. Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law. *ICRC.* 2009, p. 43.
[39] WATTS, S. Combatant status and computer network attack. *Va. J. Int'l L.* 2009, Vol. 50, p. 391.
[40] MELZER, N. Interpretive guidance on the notion of direct participation in hostilities under international humanitarian law. *ICRC. 2009,* p. 96.
[41] HATHAWAY, O. A., CROOTOF, R., LEVITZ, P., NIX, H. The law of cyber-attack. *Calif. L. Rev.* 2012, Vol. 100, p. 817.
[42] Bitar, M., Chakka, B. Drone attacks during armed conflict: quest for legality and regulation. International Journal of Intellectual Property Management. 2023 Vol.13, p. 397.

tary objects.[43] This arises from the intertwining and common infrastructure utilized by both civilian and military sectors in cyberspace, creating ambiguity regarding who constitutes combatants and civilians. The majority of cyberspace infrastructure is composed of civilian objects, such as computers, operating systems, and applications, which military organizations also utilize. This interconnection makes it difficult to identify clear-cut military objectives in cyberspace, as both civilian and military installations are intertwined. As a result, applying Article 52(2) of API in cyberspace could potentially classify civilian cyber assets as legitimate military objectives. The destruction or neutralization of these assets could provide a military advantage,[44] leading to the risk of civilian networks being targeted in cyberattacks,[45] which could have serious consequences in societies heavily reliant on cyberspace for critical functions such as healthcare, finance, and transportation. Cyberattacks also complicate matters further by affecting both military and civilian systems indiscriminately. Malicious code, once released, can spread to unprotected civilian computers and even vital infrastructure like medical facilities. The resilient nature of cyberspace makes it challenging to distinguish between military and civilian targets, as data packets can find alternate routes.[46]

In the digital realm, even objects primarily intended for civilian use can be considered military targets due to their dual-use nature. Although some cyberattacks may focus solely on military objectives, the interdependency of cyberspace often leads to unintentional harm to civilian systems. The far-reaching consequences of cyberattacks, as exemplified by the Stuxnet attack on Iran's nuclear facility, highlight the pressing need for legal frameworks that can adequately address the intricacies of cyber warfare.

Considering the principle of distinction, the determination of what constitutes damage to civilian objects in cyber warfare is crucial. Assessing the impact of disruptions to functionality on civilian infrastructure becomes paramount in applying the principle of proportionality. However, clarifying the scope of such disruptions and balancing them against anticipated military advantage presents significant challenges, particularly given the novelty and complexity of cyber operations.

V. THE PRINCIPLE OF PROPORTIONALITY IN CYBER WARFARE

The concept of proportionality in armed conflict stipulates that parties should not carry out cyberattacks on military targets if the potential harm to civilians exceeds the military advantage gained. This principle plays a vital role in safeguarding civilians and critical infrastructure, given the interconnected nature of civilian and military networks in the digital age. Recognized as customary international law[47] and enshrined in the Article 51(5) (b)

[43] Taddeo Mariarosaria - Ludovica Glorioso (eds.). Ethics and policies for cyber operations: A NATO cooperative cyber defence centre of excellence initiative. *Springer.* 2016, Vol. 124, p. 35.
[44] GEIß, R., LAHMANN, H. Cyber warfare: Applying the principle of distinction in an interconnected space. *Israel Law Review*. 2012, Vol. 45, No. 3, p. 383.
[45] KODAR, E. Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I. *ENDC Proceedings*. 2012, Vol. 12, p. 115.
[46] GEIß, R., LAHMANN, H. *Cyber warfare: Applying the principle of distinction in an interconnected space*. p. 386.
[47] ICRC, Study on Customary International Humanitarian Law, 2005, Rule 14.

of API, the principle restricts civilian harm during attacks on military objectives, while balancing the principles of humanity and necessity.

While the UN Group of Governmental Experts acknowledges proportionality as a well-established legal principle regarding the use of ICTs in conflict, more research is needed to fully understand its practical application.[48] The principle is reinforced by the precautions in attack, which require attackers to evaluate and, if necessary, call off disproportionate attacks.[49] Legal attacks on military targets must adhere to both proportionality and precautions, ensuring that civilian harm is minimized.

Civilian harm in cyber operations can encompass loss of life, injury, and damage to objects. Unlike kinetic operations, cyberattacks can cause various types of harm, such as disabling systems without causing physical damage but with widespread effects due to cyberspace's interconnectedness. The assessment of civilian harm considers both direct consequences, such as immediate damage to targeted systems,[50] and indirect effects, such as reverberating impacts on infrastructure and individuals. This assessment also takes into account harm incurred during transit and the consequences of impairing objects used for both civilian and military purposes, such as elements of the power grid. The principle of proportionality prohibits launching an attack if the expected harm to civilians or civilian property outweighs the anticipated military advantage gained.[51]

The evaluation of potential threats during a cyberattack is guided by the perspective of a "competent commander," an individual with military training and experience who, acting in good faith, takes into account information from multiple sources, including technical experts. It is generally acknowledged that in the context of military cyber activities, these sources ought to possess relevant technical knowledge.[52]

A key question arises when considering incidental harm: should the loss of functionality of civilian computers, systems, or networks be taken into account when applying the principle of proportionality? The ICRC maintains that any harm that affects the protection of civilian objects from direct attack, including instances where these objects are rendered inoperable, must be considered.[53]

The necessary harm to civilians must be weighed against the anticipated "concrete and direct military advantage".[54] It is essential to exclude any advantages that are not truly military in nature, such as those that are political, psychological, economic, financial, social, or moral.[55] For instance, disrupting government propaganda or undermining civilian morale would not be seen as providing a concrete and direct military advantage.

---

[48] UN. Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. July 2021, para. 71.
[49] ICRC. note 45, Rules 18 and 19, Articles 57(2)(a)(iii) and 57(2)(b) of AP I.
[50] Michael N. Schmitt (ed.). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge: Cambridge University Press. Commentary on Rule 113. 2017, para. 3.
[51] ICRC. Avoiding Civilian Harm from Military Cyber Operations during Armed Conflicts. 2021, p. 19.
[52] ICRC. International expert meeting report: The principle of proportionality. 2018, p. 49.
[53] ICRC. ICRC Position Paper: International humanitarian law and cyber operations during armed conflicts. 2020, pp. 7–8.
[54] ICRC. note 49, p. 12.
[55] Khalil, A., Raj, S. A. K. Assessing the Legality of Autonomous Weapon Systems: An In-depth Examination of International Humanitarian Law Principles. LAW REFORM. 2023 Vol. 19, p. 372.

The term "concrete" demands that only real and quantifiable advantages be considered, excluding speculative or hypothetical benefits. Those responsible for planning and authorizing a cyberattack must have a reasonable certainty that the attack will lead to a tangible advantage.[56]

The term "direct" necessitates a clear causal link between the cyberattack and the anticipated military benefit, without any intervening factors or entities. Indirect or distant advantages, as well as those that may only manifest in the long run, should be discounted.

When a cyber operation is integrated into a coordinated military campaign alongside kinetic strikes targeting the same military objective, the assessment of military advantage should consider the entire operation rather than each action in isolation. Nevertheless, it's essential to acknowledge that the operation has specific boundaries and should not be conflated with the broader war effort.[57]

Even when more precise weapons or tactics aren't available, all parties engaged in armed conflicts must still abide by the principle of proportionality. To uphold this principle, it's crucial to prioritize the paramount duty of minimizing harm to civilians and civilian infrastructure to the greatest extent feasible.

While certain states have outlined fundamental protocols for evaluating adherence to the principle of proportionality, such as "collateral damage estimation methodologies," the detailed execution, especially concerning military cyber capabilities, is frequently undisclosed. Consequently, states conducting cyber operations during armed conflicts should utilize existing procedures established for kinetic operations as a foundational framework and modify them to account for the distinct characteristics and obstacles of cyber operations.

VI. LESSONS FROM RUSSIA-UKRAINE CONFLICT:

Throughout the Russian invasion of Ukraine, cyberattacks and operations have been meticulously designed to target data and systems, disrupt critical infrastructure and services, manipulate the information domain, collect vast amounts of data, engage in intelligence activities, and carry out influence operations.[58]

Cyber activities during the conflict involved the use of wiper malware, exemplified by the attack on Ukrainian government entities and various sectors. Additionally, the recent resurgence of the 'CaddyWiper' malware, identified by the Computer Emergency Response Team of Ukraine (CERT-UA) in January 2023, targeted Ukraine's National Information Agency 'Ukrinform'.[59]

---

[56] Tallinn Manual 2.0, commentary on Rule 113, para. 9.

[57] SCHULZE, M. Cyber in war: Assessing the strategic, tactical, and operational utility of military cyber operations. 2020 12th International Conference on Cyber Conflict (CyCon). *IEEE*. 2020, Vol. 1300, pp. 183–197.

[58] Defending Ukraine: Early Lessons from the Cyber War. In: *Microsoft* [online]. [2024-04-29]. Available at: <https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK>.

[59] Ibid.

Distributed Denial of Service (DDoS) attacks have notably become the predominant form of cyberattack during this conflict, significantly affecting both the public and financial sectors. Data from the Cyber Peace Institute indicates that DDoS attacks constituted 87% of all recorded cyberattacks between January and March 2023. These assaults primarily focused on the financial, public, and Information and Communication Technology (ICT) sectors.[60]

One such attack involved the targeting of energy infrastructure, particularly during winter months.[61] For instance, DTEK, Ukraine's largest private energy company, faced hacking attempts aimed at disrupting its technological operations. Additionally, its thermal power plant was subjected to an attack.[62]

The severe and unsettling repercussions of cyber warfare in Ukraine are exacerbated by the significant involvement of non-state actors and unofficial entities. These include state-sponsored hackers and patriotic enthusiasts or volunteers, operating within a sphere that traditionally involves interactions between sovereign states.[63]

On the 24th of February 2022 just prior to the initiation of the kinetic invasion, a cyberattack was launched against the American commercial internet provider (Viasat) in Ukraine. The utilisation of a novel type of malware, termed "AcidRain", which was designed to remotely assess vulnerable modems and routers, is a characteristic feature of the attack. Although it is believed that the primary target was the Ukrainian army as a consequence of this attack, tens of thousands of modems connected to the satellite network were rendered inoperable, resulting in outages for thousands of Ukrainian customers, impacting wind farms and affecting Internet users in Central Europe.[64] Viasat has said that "tens of thousands of terminals have been damaged, made inoperable and cannot be repaired".[65]

Although a lots of cyberattacks attributed to entities allegedly connected to Russia have occurred during the conflict, the Viasat satellite incident was the largest. UK's Foreign Secretary Liz Truss said based on the damaged resulted: "This is clear and shocking evidence of a deliberate and malicious attack by Russia against Ukraine which had significant consequences on ordinary people and businesses in Ukraine and across Europe".[66]

As per Sentinel One, a cybersecurity firm, the wiper malware employed in the attack exhibited developmental resemblances to the "VPNFilter" malware. Initially, the FBI

[60] JONES, D. Viasat network cyberattack linked to newly discovered Russian wiper. *Cybersecurity Dive*. 2022.

[61] ESCU. Cyber, Artillery, Propaganda: Comprehensive Analysis of Russian Warfare Dimensions. In: *Economic Security Council of Ukraine* [online]. [2023-01-17]. Available at: <https://nsarchive.gwu.edu/sites/default/files/documents/rr9q9n-glu5j/2023-01-17-Ukraine-ESCU-Cyber-Artiller-Propaganda-Comprehensive-Analysis-of-Russian-Warfare-Dimensions-ESCU.pdf>.

[62] Russian Hackers Blamed for Cyber Attack on Ukrainian Energy Firm DTEK Group. In: *Cyberdaily* [online]. 8. 7. 2022 [2024-04-29]. Available at: <https://www.cyberdaily.au/critical-infrastructure/8008-russian-hackers-blamed-for-cyber-attack-on-ukrainianenergy-firm-dtek-group>.

[63] Duguin, Stéphane and Pavlova, Pavlina. "The role of cyber in the Russian war against Ukraine: Its impact and the consequences for the future of armed conflict". Directorate-General For External Policies Policy Department. 2023

[64] VALLANCE, C. UK blames Russia for satellite internet hack at start of war. In: *BBC* [online]. 10. 5. 2022 [2024-04-29]. Available at: <https://www.bbc.com/news/technology-61396331>.

[65] UK Government. Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. In: *gov.uk* [online]. 10. 5. 2022 [2024-04-29]. Available at: <https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion>.

[66] UK Government, note 61.

attributed "VPNFilter" to the APT28 group (also recognized as "Fancy Bear") in 2018.[67] Later investigations associated it with the Sandworm group.

Google's Threat Analysis Group (TAG), which is responsible for detecting state-sponsored, espionage-oriented threats, elevated the Russian group known as Sandworm to the level of an Advanced Persistent Threat (APT), assigning it a new code name, APT44. In a recent report, TAG stated that APT44 has been a versatile tool for Russia, capable of serving its diverse interests, and has played a critical role in Russia's war against Ukraine.[68]

According to researchers, APT44's repeated utilisation of network attack techniques in political and military contexts has resulted in its classification as a significant and persistent threat to both global governments and critical infrastructure providers, particularly in areas where Russian national interests intersect.[69]

According to the UN Charter, the application of the principle of non-use of force is contingent upon the identity of the party responsible for the breach, whether it is a state actor or acting in the state direction. In the case of Viasat, on 10 May 2022 the UK's National Cyber Security Centre,[70] US Department of State,[71] and Council of the EU[72] officially attributed the attack to Russia. The Sandworm and APT44 a purported Russian GRU-backed hacking groups, by the NSA.[73] Both groups are associated with Russian military intelligence (GRU).[74] However, Russia repeatedly denied engaging in offensive cyber operations.[75]

Considering this, the principle of non-use of force is applicable in this scenario. The ICJ has affirmed that Articles 2(4) (Rules 68-70) and 51 (Rule 71-5) of the UN Charter, which prohibit the use of force and relate to self-defense, are relevant to "any use of force, irrespective of the weapons utilized."

---

[67] GUERRERO-SAADE, J. A.,VAN AMERONGEN M. Acid Rain - A Modem Wiper Rains Down on Europe, Sentinel Labs. In: *SentinelLABS* [online]. 31. 3. 2022 [2024-04-29]. Available at: <https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe>.

[68] Google anlysis. Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm. In: *cloud.google.com* [online]. 17. 4. 2024 [2024-04-29]. Available at: <https://cloud.google.com/blog/topics/threat-intelligence/apt44-unearthing-sandworm>.

[69] FADILPAŠIĆ, S. Russian Sandworm cybercrime group linked to multiple attacks. In: *msn.com* [online]. 18. 4. 2024 [2024-04-29]. Available at: <https://www.msn.com/en-us/news/other/russian-sandworm-cybercrime-group-linked-to-multiple-attacks/ar-AA1nevo2>.

[70] UK Government, note 61.

[71] BLINKEN, A. J. Attribution of Russia's Malicious Cyber Activity Against Ukraine. In: *US Department of State* [online]. 10. 5. 2022 [2024-04-29]. Available at: <https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine>.

[72] Council of the EU, Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. In: *Council of the European Union* [online]. 10. 5. 2022 [2024-04-29]. Available at: <https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union>.

[73] Carly Page. Viasat cyberattack blamed on Russian wiper malware. In: *techcrunch.com* [online]. 31. 3. 2022 [2024-04-29] Available at: <https://techcrunch.com/2022/03/31/viasat-cyberattack-russian-wiper/?guccounter=1>.

[74] Carly Page. Ukraine disrupts attempt by Russian hackers to take down energy provider, Tech Crunch. In: *techcrunch.com* [online]. 2. 4. 2022 [2024-04-29]. Available at: <https://techcrunch.com/2022/04/12/ukraine-disrupts-attempt-by-russian-hackers-to-take-down-energy-provider>.

[75] PEARSON, J. Russia downed satellite internet in Ukraine -Western officials. In: *Reuters* [online]. 11. 5. 2022 [2024-04-29]. Available at: <https://www.reuters.com/world/europe/russia-behind-cyberattack-against-satellite-internet-modems-ukraine-eu-2022-05-10>.

Furthermore, according to statements from public officials, the aim of disrupting satellite communications in Ukraine[76] on February 24, 2022,[77] was to escalate the conflict. Experts have suggested that the Viasat network also served as a communication provider for Ukraine's military and security forces,[78] making it a potential target for an attack intended to impact military command and control functions. This assessment was supported by remarks from the US[79] and the UK,[80] while the Council of the EU hinted at its potential involvement in facilitating military actions.[81]

By analogy, the categorization of the target in this incident resembled NATO's targeting of Serbian TV. In April 1999, NATO directed its attack at the central studio of the Serbian state-owned television and radio stations. Although the exact number of casualties remained uncertain, estimates suggested that 10–17 individuals lost their lives during the assault. The bombing of the TV studio formed part of a planned operation aimed at disrupting and degrading the C3 (Command, Control, and Communications) network. NATO officials justified this action by highlighting the dual military and civilian use of the television infrastructure, characterizing civilian television as "heavily reliant on the military command and control system, with military traffic also routed through the civilian system".[82]

Moreover, NATO asserted to Amnesty International that the RTS (Radio Television of Serbia) facilities were utilized "as radio relay stations and transmitters to support the activities of the Federal Republic of Yugoslavia (FRY) military and special police forces, and therefore they represent legitimate military targets".[83]

As per the provisions of Article 52 of API, which aim to provide enhanced protection for civilian objects, military objectives are strictly limited to "those that directly contribute to military operations and whose destruction, capture, or neutralisation offers a significant military advantage. These objects are characterised by their inherent nature, location, intended purpose, and current usage".

Therefore, the issue of target classification in the context of kinetic warfare is a highly debated topic, particularly when it comes to instances where the use of the target is dual civilian and military in nature. However, the situation becomes more intricate when considering cyber warfare. Although cyberattacks may be intended solely for military objec-

[76] LYNGAAS, S. US satellite operator says persistent cyberattack at beginning of Ukraine war affected tens of thousands of customers. In: *CNN* [online]. 30. 3. 2022 [2024-04-29]. Available at: <https://edition.cnn.com/2022/03/30/politics/ukraine-cyberattack-viasat-satellite/index.html>.

[77] BURGESS, M. A Mysterious Satellite Hack Has Victims Far Beyond Ukraine. In: *Wired* [online]. 23. 3. 2022 [2024-04-29] Available at: <https://www.wired.com/story/viasat-internet-hack-ukraine-russia>.

[78] NAKASHIMA, E. Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say. In: *The Washington Post* [online]. 24. 3. 2022 [2024-04-29]. Available at: <https://www.washingtonpost.com/national-security/2022/03/24/russian-military-behind-hack-satellite-communication-devices-ukraine-wars-outset-us-officials-say>.

[79] BLINKEN, A. J., note 67.

[80] UK Government, note 61.

[81] Council of the EU, note 68.

[82] Phil Taylo's papers. Final Report to the Prosecutor by the Cttee Established to Review the NATO Bombing Campaign. In: *University of Leeds* [online]. [2024-04-29]. Available at: <https://universityofleeds.github.io/philtaylorpapers/vp0164fe.html>.

[83] Amnesty International's initial comments on the review by the International Criminal Tribunal for the Former Yugoslavia of NATO's Operation Allied Force. 2000.

tives, the interconnected nature of cyberspace often leads to unintentional harm to civilian systems.

Moreover, the concept of direct participation of civilians in cyberspace, as we mentioned, increases the ambiguity of the legitimacy of the targeting.

Assuming the assault on Viasat genuinely disrupted Ukraine's military command and control operations, the military advantage gained would likely involve hindering Ukraine's ability to coordinate its forces effectively, thus potentially impacting its defensive capabilities. Assessing whether the attack was proportional would involve evaluating the extent of the disruption caused to military operations against any collateral damage inflicted on civilians or civilian infrastructure.

Therefore, the principle of proportionality holds increased significance in cyber warfare scenarios compared to the principle of distinction. The attack on telecommunications systems, given its potential to endanger government or military objectives, also posed a threat to civilian populations and civilian infrastructure, both within Ukraine and across Europe.

While there were no civilian casualties in the Viasat KA-SAT satellite incident, it resulted in the disabling of numerous broadband modems in Ukraine,[84] including those utilized by governmental and military entities.[85] This led to significant disruptions in internet communication and affected systems in the energy sector.[86] Moreover, tens of thousands of customers across Europe,[87] including satellite internet users from Poland, Germany, the UK, France, and the Czech Republic,[88] were impacted. The potential consequences of the attack also extended to the outage of remote monitoring and control systems for 5,800 wind turbines in Germany, operated by Enercon,[89] which remained offline for several weeks.[90]

The primary impact of the attack was felt by the Ukrainian civilian population, who were unable to access reliable information from the government during the conflict. However, civilians in other EU countries also experienced internet outages as a secondary effect of the attack, extending beyond the conflict area. Moreover, the systems in the energy sector were disrupted, leading to the outage of remote monitoring and control systems for 5,800 wind turbines in Germany. The UK's Foreign Secretary asserted that the cyberattack executed by Russia against Ukraine was intentionally malicious, resulting in grave repercussions for both individuals and enterprises in Ukraine and across the Europe. Consequently, there may be genuine doubts about whether the attack achieved a concrete and direct military advantage relative to the harm caused to civilian objects.

---

[84] GUERRERO-SAADE, J. A.,VAN AMERONGEN M. *Acid Rain - A Modem Wiper Rains Down on Europe, Sentinel Labs.*

[85] NAKASHIMA, E. *Russian military behind hack of satellite communication devices in Ukraine at war's outset, U.S. officials say.*

[86] BAJAK, F. Satellite modems nexus of worst cyberattack of Ukraine war. In: *AP News* [online]. 31. 3. 2022 [2024-04-29]. Available at: <https://apnews.com/article/russia-ukraine-technology-business-europe-broadband-internet-895f8aad2e71f56a5930aeaf833ff20f>.

[87] KA-SAT Network cyber-attack overview. In: *Viasat* [online]. 30. 3. 2022 [2024-04-29]. Available at: <https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview>.

[88] BURGESS, M. *A Mysterious Satellite Hack Has Victims Far Beyond Ukraine.*

[89] GUERRERO-SAADE, J. A.,VAN AMERONGEN M. *Acid Rain -– A Modem Wiper Rains Down on Europe, Sentinel Labs.*

[90] SATTER, R., Satellite outage caused 'huge loss in communications' at war's outset -Ukrainian official. In: *Reuters* [online]. 15. 3. 2022 [2024-04-29]. Available at: <https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15>.

CONCLUSION

The rise of cyberwarfare throws a wrench into existing legal frameworks governing armed conflict, especially regarding the UN Charter's definition of "use of force" under Article 2(4) and "armed attack". The challenge lies in pinpointing whether specific cyber activities cross the line into illegal use of force. For instance, the Stuxnet attack blurs this line by causing physical damage to the critical infrastructure.

Further complicating matters, the current framework relies heavily on the use of kinetic force. This necessitates a shift towards an effects-based approach to defining "armed force." This approach focuses on the impact on life and property, making it more relevant in modern contexts, such as cyberwarfare, where traditional notions of force may not be directly applied.

The anonymity of attackers, the interconnectedness of civilian and military infrastructure in cyberspace, and the cascading effects of cyberattacks contribute to the potential for widespread civilian harm.

Cyberattacks that unfolded during the Russia-Ukraine conflict exemplify these challenges. The use of wiper malware, targeting of critical infrastructure, and difficulty in attributing attacks highlight the urgent need for updated legal frameworks to address the unique realities of cyberwarfare.

An impact-based approach enables a distinction between cyberattacks and cyberespionage. Under this approach, certain activities, such as cyber espionage or intelligence collection, may not be considered to prohibit the use of force because they do not result in direct or indirect destruction. Activities such as propaganda, psychological warfare, or espionage, when conducted through cyber means, are generally deemed legitimate, unless explicitly prohibited.

The differentiation between various cyber activities is of utmost significance in determining whether an action amounts to the use of force or armed attack. The article concludes that even in kinetic attacks, where civilian objects and military objectives overlap, a challenge arises in classifying targets according to the principle of distinction. In such cases, the attainment of a clear and concrete military advantage may assume greater significance in assessing the legitimacy of the target, based on the principle of proportionality.

The research findings indicated that not every form of cyber activity could be deemed a use of force or armed attack. However, the deployment of the "AcidRain" malware against Viasat merited further examination, as it raised enquiries about legitimacy and justification.

Nevertheless, the attribution of culpability to hacker groups supported by the Russian government was a crucial factor in determining whether the incident could be classified as a use of force under the UN Charter.

Additionally, regarding the legality of the attack under IHL, the Viasat attack highlights the significance of proportionality in assessing cyber warfare, as the distinction between civilian and military targets in cyberspace is unclear. The study concluded that the legal issues surrounding cyber and kinetic attacks can be comparable, particularly when the target of the kinetic attack is of a similar nature and has dual uses.