Journal DOI: https://doi.org/10.64184

Journal Email: info@ashurjournal.com

Journal home page: https://ashurjournal.com/index.php/AJLPS/about

This journal is open access & Indexed in

IRAQI Academic Scientific Journals Google الباحث العلمي Crossref

Article Info.	
Sections: Law.	**Received: 2025 June 02**
Accepted: 2025 June 18	**Publishing: 2025** September **1**

Are Cyber Powers Challenging International Humanitarian Law, or Is Cyberspace Still a Legal Blind Spot?

Dr. Ahmed Aubais Al-Fatlawi

Professor of Public International Law at the University of Kufa: Faculty of Law

orcid.org/0000-0002-5556-7245

ahmeda.alfatlawi@uokufa.edu.iq

Abstract

This study investigates the complex relationship between cyber warfare and international humanitarian law (IHL), focusing on whether cyberspace is legally ambiguous or overlooked by states with advanced cyber capabilities. Utilizing a dual approach, it emphasizes the International Committee of the Red Cross (ICRC)'s affirmation of IHL's adaptability. It examines the legal criteria outlined in the Tallinn Manual regarding when cyber operations qualify as armed conflict. The findings indicate that while customary IHL principles can apply in the digital realm, significant data protection, civilian targeting, and attribution ambiguities hinder effective enforcement. The paper argues that major cyber powers often reject IHL applicability, not due to legal gaps, but as a strategic choice disguised as ambiguity. In conclusion, the study offers original proposals, including the recognition of "critical civilian datasets" requiring protection and the introduction of a legal standard called "functional lethality," advocating for a proactive regulatory framework to enhance humanitarian protections in cyber warfare.

Keywords: Cyberattacks, International Humanitarian Law, Digital Warfare, Tallinn Manual, Armed Conflict, Legal Accountability, Civilian Protection, Military Objectives in Cyberspace, Customary Law, Digital Infrastructure

Introduction

The rise of cyber conflict has outpaced the legal systems established to contain it. This study investigates whether the principles of international humanitarian law (IHL)—traditionally grounded in physical warfare—can effectively regulate the unique challenges posed by cyberattacks during armed conflict. Central questions arise: Are cyber operations being unjustly exempted from IHL? Do cyber-capable states exploit legal ambiguity to evade responsibility? To address these issues, the study is divided into two main sections:

• Section One analyses the position of the International Committee of the Red Cross (ICRC), affirming that cyber operations fall within the scope of IHL, even when treaties do not explicitly mention "cyber."

• Section Two delves into the Tallinn Manual's expert framework, offering legal criteria to determine when cyber operations constitute the "use of force" or "armed attacks."

Through both legal interpretation and real-world cases, the study aims to clarify the threshold of legality in cyberspace, and whether humanitarian obligations are being purposefully ignored or genuinely constrained by legal frameworks insufficiency.

Section One: ICRC point of view

The digitalization of warfare has exposed gaps in conventional legal doctrine. This section explores how the International Committee of the Red Cross (ICRC) affirms that international humanitarian law (IHL) is not obsolete but adaptable, even in cyber warfare. Through an analysis of foundational treaties, interpretive doctrines, and the Martens Clause, we examine how IHL principles can and must apply to cyber operations. A breakdown of legal authority, normative gaps, and the evolving recognition of digital assets as targets and protected entities follows.

Part 1.1 – Foundational Applicability of IHL to Cyber Operations

From a legal perspective, international humanitarian law (IHL) establishes the framework governing cyber attacks during armed conflict to protect victims from harm. Although IHL lacks explicit definitions of concepts like cyberwarfare and cyber operations, we can rely on definitions from military documents and the insights of legal experts.

The International Committee of the Red Cross (ICRC) defines "cyber operations during armed conflict" as attacks on computer systems, networks, or Internet-connected devices used as means of warfare. The ICRC firmly states that cyber warfare methods are subject to IHL, imposing clear restrictions on cyber attacks in armed conflict.

Moreover, the lack of specific military activity controls does not allow unrestricted execution. The evolving nature of cyber technology does not exempt these operations from the stringent application of IHL as a means of hostile action.[1]

Cordula Droege, a legal adviser at the International Committee of the Red Cross, asserts that cyber attacks are "operations launched against or through a computer or computer system via data flow." These actions can include hacking, collecting, altering, or encrypting data, often classified as attacks under international

humanitarian law.[2] The Chancellor's statement cited Article 49, paragraph 2, of Additional Protocol I (1977).[3]

The core objective of international humanitarian law is not merely to establish regulations for hostilities during armed conflicts; rather, it encompasses a proactive approach to embrace and govern future developments in the landscape of warfare. This law is fundamentally designed to adapt to the evolving nature of conflict, ensuring that its principles remain relevant as new technologies and methods of warfare emerge.

The significance of this adaptability is underscored by the St. Petersburg Declaration of 1868, which articulates a forward-looking vision: "The principles established must be upheld in light of future advancements that science may bring to military armament." This declaration serves as a pivotal reference point, affirming the commitment of the international community to uphold humanitarian standards in the face of continual scientific progress and innovation in military capabilities".[4]

One of the key principles of international humanitarian law is outlined in Article 36 of Additional Protocol I, adopted in 1977. This article mandates that during the evaluation, development, or acquisition of new weapons or methods of warfare, High Contracting Parties must determine if their use, in specific or all circumstances, would violate this Protocol or any applicable international law. This requirement emphasizes the responsibility of states to assess the legality and humanitarian implications of military innovations, ensuring adherence to international legal standards in armed conflicts.[5]

There is no doubt that this obligation includes means and methods based on digital medical technology. We assert that international humanitarian law applies to cyberattacks in ongoing armed conflicts. This view is reinforced by the International Court of Justice, which highlighted in its 1996 advisory opinion on the legality of nuclear weapons that humanitarian law principles apply to all forms of warfare and all types of weapons, including future technologies. This acknowledgement emphasises the necessity of integrating modern technologies into the legal framework governing armed conflict while maintaining a focus on humanitarian considerations".[6] This approach undoubtedly includes cyber-attacks and is firmly recognised by experts across the field.[7]

Part 1.2 – Legal Voids and the Martens Clause

Despite ongoing developments in law, a significant legal vacuum persists regarding the regulation of cyberattacks. Advocates assert that cyberspace is an independent realm, distinct from the physical world. Certain strands of Anglo-Saxon jurisprudence emphasize that it operates as an unregulated domain, allowing individuals to engage in various activities, including hostile ones, without legal constraints.

This perspective arises from cyberspace's unique nature, where passwords and computers create barriers separating it from physical reality. Consequently, it becomes challenging to assign jurisdiction to any specific state. Therefore, cyberspace remains largely exempt from traditional international regulations, which have struggled to govern even more conventional frontiers like outer space. This legal

ambiguity underscores the urgent need for a coherent framework to address activities in this rapidly evolving digital environment.

Proponents of this trend argue that current international humanitarian law conventions do not explicitly address cyber attacks on computer networks. They emphasize the recent emergence of advanced electronic control technologies, which challenge the applicability of traditional humanitarian law principles to modern warfare. As cyber attacks are a relatively new phenomenon, the lack of specific regulations reflects the difficulty of adapting established legal norms to the evolving landscape of digital conflict.[8]

Supporters of this trend highlight the term "cyber," which is absent from key legal documents like the Hague and Geneva Conventions and the United Nations Charter. Instead, these frameworks focus on the use of armed force. They cite conflicts such as the Russian-Estonian tensions and Russia's actions against Georgia, illustrating difficulties in responding to such cyber attacks due to uncertainty in applying international law. As a result, these operations often remain uncategorized as armed conflicts, revealing significant gaps in our legal understanding of warfare in the digital realm.[9]

While international humanitarian law (IHL) lacks explicit cyber-specific provisions, this does not amount to legal permissiveness. Instead, it reflects an interpretive challenge—requiring current IHL rules to be applied with contextual sensitivity to digital operations.

It is essential to actively apply the Martens principle, which reflects customary international law, to address potential misinterpretations of a legal vacuum. This principle is acknowledged in the preamble to the Fourth Hague Convention[10], the Geneva Conventions of 1949[11], and Additional Protocol I .[12] By doing so, we can promote a more responsible and legally sound approach to cyber engagements in conflict scenarios.

Part 1.3 – Civilian-Military Distinction and Digital Targets

In international humanitarian law, civilian objects represent the sanctity of life, being all those that are not military objectives. Military objectives[13], as articulated in Article 52, paragraph 2, of Additional Protocol I, are those that significantly contribute to military action, whether by their nature, location, purpose, or use. Our commitment to peace compels us to limit attacks to military objectives, ensuring that any destruction, capture, or disabling of such objects under the current circumstances leads to a meaningful military advantage,honoring the principles of humanity and justice.[14]

The definition of military objectives under international humanitarian law primarily focuses on tangible entities, raising important questions about cyber attacks. Specifically, it challenges us to discern which elements of an information system can be deemed legitimate targets: the physical infrastructure or the digital data contained within.

While the prevailing interpretation excludes digital data from being classified as a ‘thing,’ recent legal arguments suggest that data of critical civilian relevance should be protected as civilian objects due to their strategic and humanitarian value. The

International Committee of the Red Cross (ICRC) described "things" in 1987 as "visible and tangible," meaning that attacks on data alone do not constitute military operations. However, targeting data could be regarded as an attack if it disrupts cyber infrastructure functions or leads to significant consequences, qualifying the operation as an armed attack. This highlights the complexity of addressing both physical and digital aspects in modern warfare.[15]

A minority of experts argue that digital data should be treated as an "object" for targeting in cyber operations. They believe the majority's view is overly narrow, as failing to include operations that specifically target data may leave critical civil datasets—such as social security information, tax records, and banking details—unprotected under the law of armed conflict.

These experts highlight that Article 48 of Additional Protocol I emphasizes the need to protect the civilian population from the effects of hostilities. They contend that the seriousness of an operation's consequences, rather than just the nature of the damage, should be the deciding factor in determining legality. Thus, they assert that essential civil data should be categorized as civilian objects and safeguarded by international law.[16]

From the perspective of jurist Marco Sassoli, it is essential to consider the unique characteristics of cyber attacks when evaluating their classification under international humanitarian law. He argues that a pressing need exists to revisit and potentially redefine what constitutes military objectives in this evolving context. The crux of the issue lies in interpreting the effects of cyber operations, which determines whether they can be classified as attacks. This classification remains contentious, especially when considering scenarios such as data deletion.

According to the "effects approach," an operation may be considered damaging or destructive based on its outcomes. Therefore, framing the act of data deletion as an attack can be legitimized by redefining military objectives under international humanitarian law standards. Specifically, this entails recognizing that the military advantage gained from "neutralizing" a target—rather than merely destroying it—can fulfill the criteria outlined in Article 52, paragraph 2 of Additional Protocol I. Thus, even if an operation stops short of physical destruction, the strategic significance of neutralizing a cyber asset may satisfy the requirement for defining military objectives.[17]

Part 1.4 – International Legal Responses and Norm Development

International reactions have increasingly highlighted the growing awareness and acknowledgment among states regarding the application of international law in the realm of cyberspace. This emerging consensus was notably encapsulated in the findings of the Reports of the United Nations Group of Governmental Experts published in 2013 and 2015. The Group concluded that "international law, in particular the Charter of the United Nations, applies to the use of information and communication technologies by States," underscoring its critical role in upholding global peace and stability.[18]

The significance of this conclusion was recognized and celebrated by the United Nations General Assembly during its 70th session in 2015.[19] The Assembly not only

welcomed this affirmation but also reiterated its importance at subsequent sessions, particularly during the 73rd session in 2018 and further discussions in 2019.[20] This ongoing dialogue reflects an evolving understanding of the need for a secure, open, and accessible ICT environment, which is vital for fostering international cooperation and safeguarding peace in the digital age.

The 2015 report emphasized "well-established international legal principles," including humanity, necessity, proportionality, and distinction.[21] While it did not mention International Humanitarian Law (IHL) explicitly, Michael Schmidt noted that these principles align closely with its fundamental tenets, highlighting their importance in ensuring humane treatment in conflict situations.[22]

NATO has firmly stated that international humanitarian law applies to cyber operations during armed conflicts, emphasizing the need for legal frameworks in digital warfare.[23] Similarly, the Paris Call for Confidence and Security in Cyberspace, supported by 78 countries as of April 2020, reinforces this principle regarding cyberattacks. Furthermore, the heads of government from 54 Commonwealth nations have expressed their commitment to exploring how international law, including the United Nations Charter and applicable humanitarian law, can be applied in all aspects of cyberspace, highlighting the importance of a legal foundation in an increasingly digital world.[24]

The ICRC emphasises that applying international humanitarian law to cyber operations during armed conflict does not support the militarisation of cyberspace or legitimise cyber warfare. All actions remain subject to the United Nations Charter and customary international law, particularly the prohibition of force. Cyberspace should be approached peacefully, like all other domains.[25]

It is essential to highlight that, in addition to the guidelines set by the United Nations Charter against the use of armed force—including cyber operations—international humanitarian law (IHL) also imposes crucial restrictions on the conduct of hostilities. This applies when states or non-state actors engage in cyber attacks during armed conflicts.

IHL does not legitimize cyber operations or military actions in this context; rather, it introduces specific limitations that complement those in the UN Charter and customary international law. Notably, IHL prohibits the development of cyber capabilities that could be deemed indiscriminate weapons or that might cause unnecessary injury or suffering, thereby safeguarding fundamental humanitarian principles even in the digital battlefield.[26]

The ongoing discussion surrounding the application of humanitarian legal principles to cyberattacks, alongside the potential creation of additional regulations to address any legal gaps, does not negate the fact that states continue to evolve international law, agree upon voluntary guidelines, and collaborate on shared interpretations of existing regulations. For instance, upon the establishment of the UN Open-ended Working Group in 2018, a significant majority of nations within the UN General Assembly endorsed a framework of "international norms, standards, and principles for responsible state behavior," which builds upon standards developed by the United Nations over the years. Additionally, there are scholarly proposals

advocating for stricter legal or political constraints on cyber operations in the context of armed conflict.[27]

Herbert Lin notes that although countries like the United States, China, Russia, and Israel are widely believed to possess advanced offensive cyber capabilities, none of them have officially acknowledged conducting cyber operations. This silence underscores a pattern of strategic ambiguity and avoidance of formal legal responsibility regarding cyber conflict and its regulation under international humanitarian law.[28]

Ultimately, while strong legal foundations support the applicability of IHL to cyber operations, the notion of 'global consensus' remains partially aspirational. Cyber-capable states often interpret IHL selectively—either downplaying its relevance or invoking legal ambiguity as strategic cover.

Recent multilateral discussions highlight that this recognition does not legitimize the militarization of cyberspace or endorse the deployment of harmful cyber operations. Rather, it underscores the importance of upholding legal standards and ethical considerations in an increasingly digital battleground.

Section Two: An Expert Perspective from the Tallinn Manual

When cyberattacks transcend sabotage and approach warfare, how do we classify and regulate them? This section investigates the legal reasoning behind the Tallinn Manual's criteria for armed conflict in cyberspace. From assessing intensity and duration to examining state control and proxy involvement, we confront the realities of attribution and escalation. The subsections that follow outline when IHL applies, how responsibility is assigned, and why conventional thresholds of force are no longer sufficient for digital aggression.

Part 2.1 – Conditions for Applying IHL to Cyber Conflicts

One of the key issues that requires our attention and discussion is the application of International Humanitarian Law (IHL) in situations of armed conflict. Specifically, we need to explore the circumstances under which IHL becomes applicable. Additionally, we will examine the perspectives of the experts involved in the Tallinn Manual, who provide valuable insights into this complex topic. In the following sections, we aim to provide a comprehensive analysis of these viewpoints and clarify the nuances surrounding the application of IHL in armed conflicts.

The key requirement for applying International Humanitarian Law (IHL) is the existence of an armed conflict. This term was introduced in the four Geneva Conventions of 1949, replacing the traditional term "war" and redefining how we understand and regulate hostilities. This change underscores the necessity of a legal framework that protects those not participating in the conflict while promoting humanitarian principles.[29]

Armed conflict includes direct hostilities,[30] covering both traditional warfare and modern cyber warfare. This term pertains to both international and non-international conflicts, with cyber activities needing to support military operations to be classified as relevant.[31]

A notable example is the 2008 conflict between Russia and Georgia, where cyber tactics disrupted communications and influenced hostilities.[32] Similarly, during the

Lebanon conflict on September 17-18, 2024, Israel launched cyber attacks that detonated communication devices, tragically impacting civilians.[33] This illustrates the complex intersection of technology and warfare and the evolving nature of armed conflict today.

In principle, the application of armed force that does not qualify as an armed attack is generally not included. However, there is an exception for operations that affect the delivery of humanitarian assistance, which are subject to the law of armed conflict, even if they do not rise to the level of an "armed attack".[34] The law of armed conflict is designed to regulate conduct during hostilities and protect those involved in armed conflicts. It does not apply to individuals or organizations not engaged in warfare. For example, if a private company commits information theft to gain an unfair market advantage, this act of corporate espionage falls outside the law's jurisdiction.[35]

The International Criminal Tribunal for the Former Yugoslavia (ICTY) has defined a key criterion for identifying armed conflicts: to classify a non-international armed conflict, there must be a racial element linked to protracted armed violence. This emphasis highlights the complex tensions that often fuel such conflicts.[36]

The complexities of modern conflicts reveal significant challenges in applying international humanitarian law to cyberattacks. Key difficulties include identifying the origin of the attack—whether it originates from a state or non-state actor—and understanding its purpose, such as disrupting critical infrastructure or stealing sensitive data. Additionally, assessing the precise effects of these attacks can be challenging, as their repercussions may not be immediately clear. Despite these hurdles, it is crucial to uphold the principles of international humanitarian law, ensuring accountability and humanitarian considerations in the digital realm.[37]

The criteria for identifying an international armed conflict, based on customary international law, are specified in Article II of the Geneva Conventions of 1949. This article states: "This Convention shall apply in the event of declared war or any armed clash between two or more High Contracting Parties, even if one does not recognize a state of war." This emphasises the need for adherence to international humanitarian standards, regardless of formal declarations".[38] The Convention recognizes the complexities faced during times of partial or total occupation of a High Contracting Party's territory. It remains applicable even in situations where the occupying forces do not face armed resistance, acknowledging the challenges and hardships that arise in such circumstances".[39]

Part 2.2 – Attribution and the Spectrum of State Control

The International Group of Experts has reached a consensus that an international armed conflict can be characterized as such whenever there are hostile acts that involve or are confined to cyberattacks between two or more states engaged in a conflict. This definition also applies in scenarios where an organized armed group, which operates under the effective control of one state, actively participates in the conflict by conducting hostile proxy operations against another state. These criteria reflect the evolving nature of warfare in the modern age, where cyber operations can play a pivotal role in international relations and conflict dynamics.[40]

The issue of whether the actions of an organized non-State armed group can be considered as being against another State, and whether these actions can be attributed to that State under the concept of "international conflict," was specifically addressed in the judgment of the Appeals Chamber of the International Criminal Tribunal for the Former Yugoslavia.[41] The Appeals Chamber articulated the Standard of Overall Control to assess the relationship between Bosnian Serb units and the former Yugoslavia. This framework allowed the Chamber to draw a significant conclusion regarding the nature of the conflict, ultimately deeming it sufficient to establish the presence of an international armed conflict.[42] In 2007, the International Court of Justice ruled on the case of Bosnia and Herzegovina versus Serbia and Montenegro concerning the Convention on the Prevention and Punishment of the Crime of Genocide. The Court determined that the "standard of overall control" was both applicable and appropriate for assessing the extent of Serbia and Montenegro's involvement in the wartime actions, highlighting the complexities of state responsibility in international law.[43] In the ICC's 2012 ruling in the Lubanga case, this point was thoughtfully acknowledged, reflecting a deeper understanding of the complexities involved.[44]

In light of the above analysis, we conclude that when one state exerts comprehensive control over a structured group of hackers targeting the cyber infrastructure of another state, and this results in substantial material damage, the situation qualifies as an armed conflict. Such a conflict can indeed be characterized as international in nature.

To elaborate further, consider the example of State A: it does not necessarily have to issue direct orders instructing the group to target specific components of State B's infrastructure. Instead, it is sufficient for State A to maintain sufficient oversight and direction over the hacker group, enabling them to initiate cyberattacks against selected cyber targets. This dynamic highlights the modern complexities of international conflict, where traditional military engagements can shift into the realm of cyberspace, blurring the lines of responsibility and accountability.[45]

Support from one state to a non-state armed group does not necessarily transform a non-international armed conflict into an international armed conflict between the supporting state and the state where the conflict occurs. This principle is established in the Tadić case, where the Appeals Chamber ruled that actions such as providing funding, training, and equipment are insufficient to classify the situation as an international conflict unless the supporting state exerts overall control over the non-state group. If that level of control is not achieved, the supporting state's involvement may still be deemed an internationally wrongful act, indicating interference in the internal affairs of the affected state.[46]

The "standard of overall control" does not apply to individuals or groups that are not sufficiently organized, unless they have received explicit instructions from a State. In such instances, their actions may be attributed to that State when determining the existence of an international armed conflict, according to ICTY jurisprudence.[47]

There is a lack of definitive evidence suggesting that the hackers who carried out the cyber attacks against Estonia in 2007 were operating under the directives of any government. Furthermore, no nation has publicly endorsed or supported such cyber activities. Consequently, in addition to the ongoing debate about whether the incident qualifies as an armed conflict, it cannot properly be categorized as an international armed conflict.[48] For States that are party to Additional Protocol I of 1977, the deployment of armed force in circumstances where groups of people are engaged in struggles against colonial rule, foreign military occupation, or oppressive racist regimes is recognized as an international armed conflict. This designation acknowledges their exercise of the fundamental right to self-determination, highlighting the significant global legal and ethical implications of such conflicts.[49]

The explanation of the use of armed force and the criteria for defining a conflict is somewhat vague and requires clarification. To qualify as an armed conflict, a situation must be "armed, widespread, and protracted," indicating a sustained level of hostility.

Hostile actions can involve a combination of kinetic (physical) operations and cyber attacks, or may consist solely of cyber operations. This distinction is increasingly relevant in today's digital landscape.

The 2016 commentary on the First Geneva Convention of 1949 by the International Committee of the Red Cross emphasizes, "Cyber operations that have effects comparable to traditional kinetic actions can constitute international armed conflicts." It stresses that if these operations destroy civilian infrastructure, damage military targets, or cause casualties, they should be treated the same as conventional attacks. This highlights the need for a nuanced understanding of modern warfare in light of evolving technologies and their impact on international humanitarian law.[50]

The international expert group agreed that cyberattacks can escalate to armed conflict, exemplified by the 2010 Stuxnet operation against Iran, which caused significant damage to the centrifuges at the Natanz nuclear facility.[51] Meets the armed criterion.[52]

We examined hypotheses regarding the law of armed conflict's applicability to cyberattacks, both in scenarios without kinetic hostilities and within the context of ongoing conventional armed conflicts.[53] Having articulated the international humanitarian legal framework governing cyber attacks, we will decisively examine the approaches and criteria used to adapt these attacks. Furthermore, we will assert that these actions clearly fall within the realm of offensive or defensive acts of violence, emphasizing the critical need to understand their implications in contemporary warfare.

Part 2.3 – Assessing Armed Force through Tallinn Criteria

Michael Schmidt[54] and the international team of experts in the Tallinn Manual have set eight legal and policy criteria that should be considered in order to determine when the scale and effects of cyber attacks with harmful consequences are of a non-physical nature of destruction, yet similar to the resulting physical destruction damage caused by kinetic energy attacks.[55] The criteria are:

A - Severity of Damage: This criterion decisively evaluates the ramifications of a cyber attack by determining the extent of the damage inflicted, which includes the destruction of vital systems and injuries that could lead to fatalities. Given the significant material losses and the direct threats to personal safety, such incidents are unequivocally categorized as acts of armed aggression, underscoring their critical impact on national interests.

The assessment hinges on three key factors: the scope, duration, and intensity of the damage, with severity being paramount in establishing whether the attack constitutes an act of armed force in legal terms. Ultimately, the more profound the consequences for national security and public safety, the more readily a cyber attack will be recognized as a significant threat, warranting a resolute and comprehensive response..[56]

B- Immediacy: This concept clearly defines the time interval between a cyber attack and the damage it inflicts. Attacks that produce immediate effects are overwhelmingly seen as justifiable grounds for the use of force, especially when compared to those with delayed consequences that may take weeks or months to unfold. The sooner the damage is evident, the more likely states are to reject diplomatic resolutions, focusing instead on the urgent need to counter immediate threats. Consequently, immediate repercussions take precedence over concerns about the gradual accumulation of effects, driving states to act decisively in response to these urgent challenges.[57]

C. Directness: This concept highlights the immediate link between armed force and its negative consequences, especially in contrast to political or economic coercion.[58] Generally, the weaker the initial act and its outcomes, the less likely a State will be held accountable for violating the prohibition against armed force.

This criterion assesses directness and causation; in armed actions, cause and effect are often clear. For example, an explosion directly harms people or property. In the context of cyberattacks, those with a clear connection between an action and its consequences are more likely to be deemed acts of force, while those with indirect or unclear relationships may not meet this threshold.[59] Thus, the clarity of causation is vital in determining the nature of the action and subsequent accountability.

D- Invasion: Traditional military invasions entail armed forces physically entering another nation's territory to assert dominance. This stands in contrast to economic or political coercion, which, while exerting force, does not involve military action. In the context of cyber warfare, the focus shifts to the extent of cyber aggression directed at undermining a state's sovereignty. The more intrusive a cyber attack, particularly one that seeks to challenge a nation's control, the more significant its consequences. Cyber incursions have become vital tools for espionage in today's interconnected world, enabling states to collect intelligence without engaging in direct military conflict. However, under current international law, these activities are generally not classified as acts of force or armed attacks, provided they remain confined to the realm of espionage.[60]

C. Ability to determine effects: This criterion pertains to the clarity and precision in evaluating the outcomes of armed force compared to other coercive methods, with a focus on attack damage assessment.[61] In traditional warfare, consequences can often be quantified easily—such as the number of casualties and the extent of infrastructure damage.[62] Conversely, in cyber warfare, the repercussions are frequently less discernible and more challenging to measure. The more tangible and quantifiable the outcomes, such as loss of life or disruption of vital services, the more accurately they reflect the degree of interests impacted. Evaluating these effects in the cyber realm requires a nuanced understanding, given the potential for long-term economic and social ramifications.

D. Hypothetical legality: In the realm of international law, certain behaviors are inherently deemed impermissible, while their opposites are often regarded as acceptable. For instance, international law does not impose restrictions on the use of rumors, psychological warfare, or espionage amid a conflict. When these tactics are applied in a cyber context, they are generally perceived as legitimate strategies, reinforcing the complex landscape of modern warfare.[63]

E. State responsibility: This criterion explores the relationship between a state and cyber attacks, which can manifest in two distinct ways. A state may independently orchestrate cyber operations, demonstrating full control, or it may collaborate with non-state actors, reflecting effective control when the state supports or influences these entities.

In accordance with the 2001 draft articles on State Responsibility, particularly Articles 4 and 8, a stronger connection between a state and cyber attacks increases the likelihood that these actions will be classified as a use of armed force. This underscores the importance of establishing clear accountability in the evolving landscape of cyber warfare and international relations.[64]

G. Military character: This criterion was introduced by the International Group of Experts in the drafting of the Tallinn Manual (2.0). It states that the closer a cyber attack is to military operations, particularly hostile ones, the more likely it will be classified as a use of force. This aligns with the Charter of the United Nations, which asserts in its preamble that "armed force shall not be used except in the common interest"[65] ,while Article (44) uses the term "force" without the condition of "armed".[66] In situations that unmistakably call for the application of military force, it is widely accepted that such force refers specifically to actions taken by the army or other armed services. Furthermore, the military nature of the cyber infrastructure from which a cyber attack originates plays a critical role in interpreting these contexts under the Charter, elevating the discussions around such attacks to the level of armed force.[67]

Part 2.4 – Normative Divergence: Use of Force vs. Armed Attack

Upon a thorough examination of the previously established criteria, we must pose an important question: Are these benchmarks sufficient for accurately characterizing armed attacks within the broader context of the use of military force? We contend

that these criteria fall short when it comes to comprehensively describing cyber attacks, especially when contrasted with traditional understandings of armed conflict.

This inadequacy arises largely from the intricate nature of cyber attacks, where a multitude of specific circumstances plays a pivotal role in their assessment. States weigh a variety of critical factors in their evaluations, including the prevailing political climate at the time of the incident, the intensity and severity of the attack, the likelihood of escalating into future military confrontation, the identity of the attacker, their historical patterns of cyber aggression, and the significance of the targeted infrastructure or entity.

Therefore, it is essential to recognize that the terms "use of force" and "armed attack" embody distinct normative purposes and implications. This distinction underscores the inherent complexity involved in categorizing cyber attacks as acts of armed aggression, revealing the nuances that differentiate them from traditional forms of military engagement.

Conclusion:

This study concludes that while international humanitarian law remains normatively capable of applying to cyber warfare, its implementation is obstructed not solely by legal ambiguity but by the political will of cyber powers who either deny its relevance or invoke selective interpretations. The evidence suggests that states with advanced cyber capabilities often choose to circumvent IHL, either through strategic ambiguity or by exploiting the lack of explicit treaty references to cyberspace.

Two critical truths emerge:

1. Cyber powers may deliberately avoid acknowledging IHL in cyberspace to maintain operational flexibility while avoiding legal accountability.
2. Legal ambiguity is often a pretext, not a real barrier, as states invoke “legality” to justify actions that violate humanitarian norms.

The study offers two key innovations:

- Recognition of “critical civilian datasets” (e.g., health, financial, welfare systems) as protected civilian objects under IHL, even in the absence of kinetic effects.
- A proposed doctrine of “functional lethality”, to evaluate non-kinetic cyber operations based on the systemic humanitarian disruption they cause rather than physical destruction alone.

Ultimately, the future of IHL in cyberspace depends not just on adapting old rules but on confronting the political motivations that undermine them. A Digital Convention, co-developed by states, civil society, and legal scholars, is urgently needed to bridge this gap, clarify state obligations, and protect civilians in the era of digital warfare.

[1] ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflict, Geneva, 2011 and ICRC Challenges Report 2011, pp. 41-42.

[2] https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber. warfare-interview-2011-08-16.htm

[3] Article 49, paragraph 2, of Additional Protocol I of 1977 stipulates that: "The provisions of this right to the right (protocol) relating to all attacks shall apply to attacks in any territory from which they are launched, including the national territory of one of the parties to the conflict under the control of the adversary." See

Additional Protocol I of 1977, available on the ICRC website: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977 Last visited 9-2-2025

[4] St. Petersburg Declaration of 1868, Declaration of the Renunciation of the Use of Explosive or Charged Projectiles or Explosive or Flammable Substances Weighing less than 400 G, in Time of War, Petersburg, 29 T 2 - 11 K 1 1868.

[5] Article (36) of Additional Protocol I , previous source.

[6] I.C.J. Report 1996 Legality of the Threat or Use of Nuclear Weapons ,para. 86. Available at https://www.icj-cij.org/case/95 last accessed 9-2-2025

[7] Tallinn 2.0, on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Comment, rule (80)

[8] Brown, D., Proposal for an international convention to regulate the use of information System in Armed Conflict, Harvard International Law review, Vol.47, 2006, p. 179.

[9] Omar Mahmoud Omar, Electronic Warfare in International Humanitarian Law, Dirasat Journal, Sharia and Law Sciences, issued by the European University of Amman, Volume (46), Issue (3), 2019, p. 136.

[10] Hague Convention respecting the Laws and Customs of War on Land on October 18, 1907 (preamble), available on the University of Minnesota website http://hrlibrary.umn.edu/arabic/RegulationsLawsCustomsWar.html Last visited 13-2-2025

[11] Article 63 of the First Geneva Convention; Article 62 of the Second Geneva Convention; Article 142 of the Third Geneva Convention; Article 158 of the Fourth Geneva Convention. Available on the ICRC website, https://www.icrc.org/ar/law-and-policy/geneva-conventions-and-their-commentaries last visited 13-2-2025

[12] Article 1 (2) of Additional Protocol I.

[13] Article 52 (1) Ibid.

[14] Article 52 (2) Ibid.

[15] Tallinn 2.0, on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Comment (5) & (6) on Rule (100).

[16] Tallinn Manual 2.0,op.cit, Comment (7).

[17] Marco Sassoli, op.cit, p. 536.

[18] United Nations General Assembly Resolution, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General (A/68/98) of 24 June 2013, para. 19 and (A/70/174), 22 July 2015, para. 24.

[19] United Nations General Assembly Resolution (A/RES/70/237), "Developments in the field of information and communications in the context of international security", on 30 December 2015, preamble, paragraph. 16.

[20] United Nations General Assembly Resolution (A/RES/73/27) "Developments in the field of information and communications in the context of international security", on 11 December 2018, preambular paragraph. 17;
UN General Assembly Resolution (A/RES/73/266), "Promoting responsible State conduct in cyberspace in the context of international security", on 2 January 2019, preambular paragraph. 12.

[21] United Nations General Assembly Resolution (A/70/174), para. 28 (d).

[22] Michael N. Schmitt, France Speaks Out on IHL and Cyber Operations: Part I, EJIL:Talk!,Blog of the European Journal of International Law,30 September 2019,p.1.

[23] NATO, Wales Summit Declaration (issued by the Heads of State and Government participating in the North Atlantic Council meeting in Wales), 5 September 2014, para. 72, op. cit. Available at: Last visited 12-2-2025: Whoa, whoa, whonato.int/cps/en/natohq/official_texts_112964.Break it

[24] See: Paris Call of 12 November 2018 for Confidence and Security in Cyberspace", available at last visited 11-2-2025: https://pariscall.international/en/call

[25] ICRC, International Humanitarian Law and Cyber Operations during Armed Conflict, Position Paper to the Open-ended Working Group on Developments in Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Promoting Responsible State Conduct in Cyberspace in the Context of International Security, 2019, p. 3.

[26] John Marie Henkarts and Duswald-Beck, "Customary International Humanitarian Law", vol. I, Rules, ICRC, Brent Wright Advertising and Advertising Press, Cairo, 2007, Rules 70, 71. pp. 211-217 .

[27] Marco Sassoli, op.cit, p. 542.
(Sassoli suggested pursuing consultations between states on appropriate interpretations of law that could be constantly adapted to technological developments, which in turn would influence state practice and ultimately lead to customary law.)

[28] Lin, H., "Cyber Conflict and International Humanitarian Law," International Review of the Red Cross, Vol. 94, No. 886, Summer 2012, p. 519.

[29]The term "armed conflict", instead of "war", was first used in the four Geneva Conventions signed on 12 August 1949, and the use had great legal significance, by providing as much protection as possible to those affected by acts accompanying the armed conflict, and to counter the claim of any State that might engage in armed violence against a non-State party, and to argue that there was no need to provide the guarantees granted under These conventions, considering that internal violence is not war, but war between states, see common Article 2 of the Geneva Conventions from the first to the fourth. See also:
ICRC, Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher, ICRC, Geneva, January 2009.p.7.

[30] Some defined direct hostilities by saying: "The parties to the conflict resort to the means and methods of hitting the enemy, while direct participation means the individual contribution of a person to these acts, see: Nils Melzer, An Interpretive Guide to the Concept of Direct Participation in Hostilities under International Humanitarian Law, International Committee of the Red Cross, first Arabic edition, Regional Media Center, Cairo, 2010, p. 42.

[31] Tallinn 2.0, op.cit, Comment (2) on Rule (80).

[32] Ibid, Comment (6) on Rule (80).

[33] UN, General Assembly, Identical letters dated 19 September 2024 from the Chargé d'affaires a.i. of the Permanent Mission of Lebanon to the United Nations addressed to the Secretary-General and the President of the Security Council, General Assembly Seventy-ninth session Agenda item 34 The situation in the Middle East,A/79/367 S/2024/685 ,25 September 2024.

[34] Tallinn 2.0, Comment (4) on Rule (80).

[35] Tallinn 2.0, op.cit, Comment (8) on Rule (80).

[36] ICTY, The Prosecutor v. Ramush Haradinaj et al., Trial Chamber I, Judgment,, Case No. IT-04-84-T, 3 April 2008, para. 60.

[37] Tallinn 2.0, op.cit, Comment (10) on Rule (80)

[38] Article (2) of the Geneva Conventions from the first to the fourth.

[39] Article (2) of the Geneva Conventions from the first to the fourth.

[40] Tallinn 2.0, op.cit, Rule (82); and Comment (2).

[41] ICTY, Prosecutor v. Tadic, Appeal Chamber, Case No. (IT-94-1-A), Judgment of 15 July 1999, paras. 131, 140, 145.

[42] ICTY, Prosecutor v. Tadic, Appeal Chamber, op.cit, paras. 162.

[43] ICJ, Reports 2007, Bosnia and Herzegovina v. Serbia and Montenegro, Judgment, para. 404.

[44] ICC, Lubanga judgment: Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Trial Chamber judgment (Int'l Crim. Ct. 14 March 2012), para. 541.

[45] Tallinn 2.0, op.cit, Comment (4) on Rule (82).

[46] ICTY, Prosecutor v. Tadic, Chamber judgment, op.cit, para. 137.

[47] ICTY, Prosecutor v. Tadic, Chamber judgment, op.cit, paras. 132, 137, 141, 145.

[48] Tallinn 2.0, op.cit, Comment (8) on Rule (82).

[49] Article 1(4) of Additional Protocol I, op. cit.

[50] Jean-Marie Henckarotz, ICRC, Commentary on the First Geneva Convention of 1949, Arabic version, United Kingdom, Cambridge Press, 2016, paragraph. 255. Available at the link Last visited 21-5-2023: https://shop.icrc.org/updated-commentary-on-the-geneva-conventions-of-august-12-1949-volume-i-2016-pdf

[51] Tallinn 2.0, op.cit, Comment (15)&(17& on Rule (82).

[52] Ibid, Comment (14) on Rule (82).

[53] Marco Roscini, Cyber Operations and the Use of Force in International Law, op.cit, p. 41.

[54] Michael Schmidt is a professor of public international law from the United States of America and has developed a number of principles related to cyberattacks, including the Tallinn Manual, commissioned by NATO and published in Cambridge University Publications in 2013, for more see:
International law and cyber ops: Q & A with Mike Schmitt... https://sites.duke.edu › 2021/10/03 › last accessed 21-12-2024.

[55] Michael N. Schmitt, Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, op.cit, p. 914. ; also, Tallinn Manual 2.0, Comment (9) on Rule (69).

[56] Tallinn 2.0, op.cit, Comment (9) on Rule (69).

[57] Ibid, Comment (9) on Rule (69)

[58] Silver, Daniel B. "Computer network attack as a use of force under Article 2 (4) of the United Nations Charter." International Law Studies,, vol. 76. No.1,2002, p.89.

[59] Tallinn 2.0, op.cit, Comment (9) on Rule (69).

[60] Tallinn 2.0, op.cit, Comment (9) on Rule (69). Comment (9) on Rule (69).

[61] Silver, Daniel B, op.cit, p. 90.

[62] Tallinn 2.0, op.cit, Comment (9) on Rule (69).

[63] Tallinn Manual 2.0, Comment (9) on Rule (69). also see: Schmitt, Michael N. Cyber operations in international law: The use of force, collective security, self-defense, and armed conflicts. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy, 2010, Vol. 151, pp. 155-156; also see: Jeffrey Carr, op.cit, p. 61.

[64] Tallinn Manual 2.0, Comment (9) on Rule (69). ; also, Schmitt, Michael N. Ibid, pp. 155-156.

[65] (Preamble) Charter of the United Nations.Available on the United Nations website https://www.un.org/ar/about-us/un-charter/full-text, last visited -3-2025

[66] Article (44), ibid.

[67] Tallinn Manual 2.0, Comment (9) on Rule (69).; also see, Kriangsak Kittichaisaree, Public International Law of Cyberspace, Springer, Switzerland, 2017, p. 165.

References:

1. Additional Protocol I of 1977 , available on the ICRC website: https://ihl-databases.icrc.org/en/ihl-treaties/api-1977 Last visited 5-2-2025
2. Brown, D., Proposal for an international convention to regulate the use of information System in Armed Conflict, Harvard International Law review, Vol.47, 2006.
3. Charter of the United Nations. Available on the United Nations website https://www.un.org/ar/about-us/un-charter/full-text last visited 19-3-2025
4. First Geneva Convention, Second Geneva Convention, Third Geneva Convention, Fourth Geneva Convention. Available on the ICRC website, https://www.icrc.org/ar/law-and-policy/geneva-conventions-and-their-commentaries last visited 18-2-2025
5. Hague Convention respecting the Laws and Customs of War on Land of October 18, 1907 (preamble).Available on the University of Minnesota website http://hrlibrary.umn.edu/arabic/RegulationsLawsCustomsWar.html last visited 5-2-2025
6. https://www.icrc.org/ar/doc/resources/documents/interview/2011/cyber. warfare-interview-2011-08-16.htm
7. I.C.J. Report 1996 Legality of the Threat or Use of Nuclear Weapons. Available at https://www.icj-cij.org/case/95 last accessed 31-12-2024
8. ICC, Lubanga judgment: Prosecutor v. Lubanga, Case No. ICC-01/04-01/06, Trial Chamber judgment (Int'l Crim. Ct. 14 March 2012).
9. ICJ, Reports 2007, Bosnia and Herzegovina v. Serbia and Montenegro, Judgment.
10. ICRC, Exploring humanitarian law: IHL Guide, A legal manual for EHL teacher, ICRC, Geneva, January 2009.p.7.
11. ICRC, International Humanitarian Law and Cyber Operations during Armed Conflict, Position Paper presented to the Open-ended Working Group on Developments in Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Promoting Responsible State Conduct in Cyberspace in the Context of International Security, 2019.
12. ICRC, International Humanitarian Law and Cyber Operations during Armed Conflict, Position Paper presented to the Open-ended Working Group on Developments in Information and Telecommunications in the Context of International Security and the Group of Governmental Experts on Promoting Responsible State Conduct in Cyberspace in the Context of International Security, 2019.
13. ICRC, International Humanitarian Law and the Challenges of Contemporary Armed Conflicts, Geneva, 2011 ICRC Challenges Report 2011.
14. ICTY, Prosecutor v. Tadic, Appeal Chamber, Case No. (IT-94-1-A), Judgment of 15 July 1999.

15. ICTY, The Prosecutor v. Ramush Haradinaj et al., Trial Chamber I, Judgment, Case No. IT-04-84-T, 3 April 2008.
16. International law and cyber ops: Q & A with Mike Schmitt... https://sites.duke.edu › 2021/10/03 › last accessed 21-12-2024.
17. Jean-Marie Heinkerts, ICRC, Commentary on the First Geneva Convention of 1949, Arabic version, United Kingdom, Cambridge Press, 2016, para. 255. Available at the link Last visited 19-3-2025https://shop.icrc.org/updated-commentary-on-the-geneva-conventions-of-august-12-1949-volume-i-2016-pdf
18. John Marie Henkarts and Doswald-Beck, "Customary International Humanitarian Law", Volume I, Rules, ICRC, Brent Wright Advertising and Advertising Press, Cairo, 2007.
19. Kriangsak Kittichaisaree, Public International Law of Cyberspace, Springer, Switzerland, 2017.
20. Lin, H., "Cyber Conflict and International Humanitarian Law," International Review of the Red Cross, Vol. 94, No. 886, Summer 2012.
21. Marco Sassoli, International Humanitarian Law: Rules, Solutions to Problems arising in Warfare and Controversies UK, Edward Elgar, 2019.
22. Michael N. Schmitt, France Speaks Out on IHL and Cyber Operations: Part I, EJIL:Talk!, Blog of the European Journal of International Law,30 September 2019.
23. NATO, Wales Summit Declaration (issued by the Heads of State and Government participating in the North Atlantic Council meeting in Wales), 5 September 2014, para. 72, op. cit. Available at: Last visited 12-12-2024:www.nato.int/cps/en/natohq/official_texts_112964.htm
24. Nils Melzer, An Interpretive Guide to the Concept of Direct Participation in Hostilities under International Humanitarian Law, ICRC, First Arabic Edition, Regional Media Center, Cairo, 2010.
25. Omar Mahmoud Omar, Electronic Warfare in International Humanitarian Law, Dirasat Journal, Sharia and Law Sciences, issued by the European University of Amman, Volume (46), Issue (3), 2019.
26. Paris Call of 12 November 2018 for Confidence and Security in Cyberspace", available at last visited 11-3-2025: https://pariscall.international/en/call
27. Schmitt, Michael N. Cyber operations in international law: The use of force, collective security, self-defense, and armed conflicts. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for US Policy, 2010, Vol. 151.
28. Silver, Daniel B. "Computer network attack as a use of force under Article 2 (4) of the United Nations Charter." International Law Studies,, vol. 76. No.1,2002.
29. St. Petersburg Declaration of 1868, Declaration of the Renunciation of the Use of Explosive or Charged Projectiles or Explosive or Flammable Substances Weighing less than 400 G, in Time of War, Petersburg, 29 T 2 - 11 K 1 1868.

30. Tallinn 2.0, on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Comment, rule (80).
31. Tallinn 2.0, on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017, Comment (5) & (6) on Rule (100).
32. UN General Assembly Resolution (A/RES/70/237), "Developments in the field of information and communications in the context of international security", 30 December 2015, preamble.
33. UN General Assembly Resolution (A/RES/73/27) "Developments in the field of information and communications in the context of international security", 11 December 2018.
34. UN, General Assembly, Identical letters dated 19 September 2024 from the Chargé d'affaires a.i. of the Permanent Mission of Lebanon to the United Nations addressed to the Secretary-General and the President of the Security Council, General Assembly Seventy-ninth session Agenda item 34 The situation in the Middle East,A/79/367 S/2024/685 ,25 September 2024.
35. United Nations General Assembly Resolution (A/70/174)
36. United Nations General Assembly Resolution (A/RES/73/266), "Promoting responsible State conduct in cyberspace in the context of international security", on 2 January 201912.
37. United Nations General Assembly Resolution, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General (A/68/98) of 24 June 2013, para. 19 and (A/70/174), on 22 July 2015.