(JOINT JURIST)

[NATIONAL-LEVEL | PEER-REVIEWED | OPEN-ACCESS LEGAL JOURNAL]

| VOLUME 1 | ISSUE 1 |APRIL- MAY 2026

ABOUT THE JOURNAL

The **Joint Jurist** is a strictly law-focused national publication designed to bridge the gap between academic research and litigation expertise. We operate on a **Double-Blind Peer-Review** model, ensuring that every published work meets the highest standards of original scholarship and academic integrity. Our platform is dedicated to providing an openaccess environment for legal professionals, scholars, and students to contribute to the evolving legal discourse.

EDITORIAL & ADVISORY BOARD

The Joint Jurist Journal is guided by a distinguished panel of legal luminaries and academicians committed to fostering excellence in legal scholarship.

- **Advocate Suraj Shandil**
- **Dr. Seema Gupta**
- **Dr. Mohd Rafiq Dar**
- **Dr. Harshita Thalwal**
- **Ms. Sabrina Bath**
- **Ms. Soumya Sharma**

NAME	DESIGNATION	INSTITUTION/AFFILIATION	SPECIALIZATION & IMPACT
Advocate Suraj Shandil	Founder, CEO & Editor-in-Chief	**High Court of Himachal Pradesh**	IPR Specialist, Courtroom Strategy & Legal Research.
Prof. (Dr.) Seema Gupta	Editorial Board Member	**Associate Professor / Chandigarh University (CU)**	Constitutional Law, IPR, & Supreme Court Certified Mediator/ Interdisciplinary Legal Studies.

| VOLUME 1 | ISSUE 1 | MAY 2026

" DIGITAL FRONTLINES: INTERNATIONAL HUMANITARIAN LAW IN CYBER CONFLICTS "

AUTHOR: Kunwar Veer Vikram Pratap Singh /*UGC NET QUALIFIED / LLM (Cyber Law and Cyber Crime Investigation) / /Uttar Pradesh State Institute of Forensic Science Affiliated to NFSU Gandhinagar*

Abstract

"As warfare transcends the physical battlefield, the application of International Humanitarian Law (IHL) to cyber operations presents a profound legal paradox. This paper presents the existence of critical protection gaps to civilian data and dual-use infrastructure as a result of digital warfare as it is concluded that the principles of International Humanitarian Law (IHL) still apply to these scenarios, despite the fact that the doctrine was developed in times of kinetic conflict. By analyzing the threshold of 'armed attack' and the principle of distinction in digital environments, the study identifies critical 'protection gaps' regarding civilian data and dual-use infrastructure. It concludes that while IHL principles are resilient, a 'Digital Geneva Convention' or a specialized Protocol is necessary to prevent unchecked state-sponsored digital aggression."

Introduction: The Invisible Frontline

The old pattern of seeing war as a symphony of muscular power, and as a spectacle of the tumbling artillery, and the actual passage of men over material boundaries, has been essentially broken by the coming of the digital era. We are now on the threshold of a new era characterized by the Invisible Frontline with the theatre of conflict being no longer quantified by hectares of territory but by architecture of silicon and the flow of binary code[1]. This shift in the traditional to the cyber warfare is not only a technological innovation but a major ontological change in the way the international community conceptualizes the meaning of force, aggression and sovereignty[2]. The weapons in this invisible realm are not ballistic but algorithmic and geared towards breaching the vital organs of any state; its power grids, financial

clearinghouses, water treatment plants and communication systems without even a single shot. The strategic appeal of cyber operations is the asymmetry of the operations and anonymity that cyber operations offer. It takes only one rogue actor or an agency sponsored by a state to disable the administrative apparatus of a superpower thousands of miles away in nearly no physical footprint and with a degree of plausible deniability that a conventional military attack would not have allowed. This produces a gray area of continual tension which lies between peace and open conflict, a grey area where laws of war are in practice always neglected, and yet never actually applied.

The 'Attack' Threshold and Article 49

The legal core of cyber-hostilities is whether the threshold of the attack as embodied in Article 49 of Additional Protocol I to the Geneva Conventions is met.[3] Conventionally, the expressions used in definition of humanitarian law (IHL) in relation to an attack include the idea that any act of violence against the opponent is to be classified as an attack (either offense or defense)[4]. It is a definition created in the middle of the 20th century, which assumes that the expression of force will be kinetic or physical, in terms of bullets, bombs or blades. Nevertheless, in the modern setting of cross-border cyber activities, this "physicalist-understanding provides a significant protection gap[5]. The discussion revolves around, whether the definition of violence is the tools used (the employment of kinetic energy) or the effects created (the damage caused). According to a strict, traditionalist interpretation, a cyber attack that destroys the social security database of a country, or shuts down its central bank would not be an attack since it is not a matter of releasing physical force. This paper argues that this very limited interpretation is becoming more and more outdated and does not meet the humanitarian aims of the Geneva Conventions that aim to protect civilian populations against the devastating consequences of conflicts.

The most recent common ground among liberal legal theorists and those writing the Tallinn Manual is the functioning damage or consequentialist approach[6]. Within this framework an act of a cyber operation is deemed to be an attack when it causes persons injury or death, or the destruction or the loss of functionality of objects[7]. The difficulty is there in the case of a massive disruption that a given operation can cause, unless it is physically disrupted. As an example, when malicious software-induced outage of a city power supply in the middle of a freezing winter scenario leads to indirect deaths by the inability of heating and medical devices to operate, the act is digital, yet the violence is real. The existing legal contradiction is in the gray area where the cyber activities remain short of physical destruction but lead to system

breakdown. By placing a high bar in defining an attack, IHL unwillingly encourages states to employ sub-threshold cyber warfare with the understanding that the actions they take will not result in the application of the armed conflict law and the right to self-defense pursuant to Article 51 of the UN Charter[8].

Moreover, the threshold of attack is indissolubly connected with the security of the so-called civilian objects in Articles 52. When a digital operation is not a legal attack, it is possible that the restrictive law of proportionality and military necessity do not apply strictly, and important civilian data can be altered or deleted. This paper proposes an evolutionary reading of Article 49 that admits to digital presence a privileged interest. As the need to use data emerges as a necessity to survive, as a society, be it at the hospital registers or the distribution of food, the definition of violence should change to the functional as opposed to the kinetic. The inability to modernize the concept of an attack under Article 49 will push IHL into a sense of irrelevance, where the most common and destructive types of modern war conflicts will have no regulation whatsoever by the treaties made to humanize war. As such, the suitability of IHL hinges on its capability to bridge the physical-digital divide and offer a reliable barrier against any operation disrupting the fundamental balance of civilian life, on the basis of its size and its impact.

The Principle of Distinction in a Wired World

The Principle of Distinction, a principle of the International Humanitarian Law (IHL) spelled out in Article 48 in Additional Protocol I, is the so-called cardinal rule of the rule of distinction, which prescribes that parties to a conflict should at all times differentiate between the civil population and combatants, and non civilians and military targets[9]. The difference between theatrical and domestic space in a conventional physical theater is ensured with respect to the visual elements: uniforms, marked vehicles, and physical segregation of barracks and residential areas. But in the 21 st century wired world, it is the pillar on which the whole world rests, and which possesses an existential crisis. Internet architecture is by its nature unconcerned with the status of internet users. [10]The digital and the physical worlds differ in the fact that unlike the physical world where a hospital and a munitions factory might be at different geographical coordinates, the digital world needs to use shared infrastructure. Civilian banking information, emergency communications, and even personal communications are sometimes on the same fiber optic cable, router, and satellite links as are used by military command-and-control networks. This dual-use character of the digital backbone renders it virtually unattainable to concentrate on a military goal in cyberspace without unintentionally attacking or disrupting non-military networks as well.

What makes the situation even more complicated is the fact that the divide between combatants and civilians is indistinct. When the kinetic era was in force, a civilian was able to become a combatant by picking up a rifle; when the cyber era is in play, a civilian programmer sitting in a high rise office will do a line of code that will cause the air defense system of an enemy to shut down. This emergence of the civilian hacker or even patriotic cyber-collective questions the legal immunity otherwise given to non-combatants. Even in the case of IHL, the civilians are not deprived of protection except that they direct participation in hostilities (DPH) ousman[11]. But what constitutes the direct involvement in a cross-border cyber-op is hotly disputed in terms of the law. Is it DPH to have given technical assistance to any state-operated hacking outfit[12]? Is the very act of writing a malware and not deploying it a loss of a protection? By using the civilian population as a human shield to perpetrate digital aggression through person fronting the civilian as proxies, states are actively undermining the Principle of Distinction when they engage civilian proxies to retain plausible deniability.

Additionally, the topic of targetability of data is also controversial. Although IHL safeguards the objects, it is not globally agreed on whether intangible information, like social security records, land titles, medical history, or others, would be considered as such an object. When data is not an object, then destruction or manipulation of it may not be technically in violation of the Principle of Distinction. This article uses hyper-connected society as the basis of arguing that data is a functional equivalent of a physical asset. Destroying a vaccination database of a country is as detrimental to the civilian population as destroying a real-life medical warehouse. A systems-based view of the interpretation of the Principle of Distinction should be used to ensure the sufficiency of IHL. The law should examine the civilian use of network, instead of just doing the physical nature of the target. In the absence of a serious re-characterization of civilian data as a safeguarded interest the wired world turns into theater of complete war, in which the civilian population is no longer bystander, but primary though unseen target. Failure to impose the distinction strictly in cyberspace does not only pose any threat to digital assets but the whole humanitarian system may be on the point of collapse as indiscriminate warfare under the name of technological necessity will be acceptable.

The Attribution Gap and Plausible Deniability

Attribution is the one problem that has proven to be the biggest impediment to the successful application of the International Humanitarian Law (IHL) in the electronic space. The presence of an aggressor in the conventional armed conflict is normally defined by physical presence - marking an aircraft, the position of a naval ship, or the recognizability of uniform of a soldier.

When it comes to cross-border cyber warfare, the internet digital architecture has been purposely created in such a way that it enables anonymity. A mix of spoofing IP addresses, routing attacks across several layers of zombie servers in neutral third-party states and encryption allows an aggressor to initiate a crippling attack akin to the trail of forensic breadcrumbs that leaves the finger print on a dozen different directions. This Attribution Gap provides a strategic space in which technical capability to detect an attacker is far behind that of the attacker to cause harm[13]. As a practitioner of law, this leaves an evidentiary loophole in that, without any clear connection between a malicious code line and to a state that could be deemed sovereign, the laws of state responsibility cannot be invoked, and the victim state has no clear legal avenue to pursue or any lawful response.

This technical anonymity is used as a weapon of the doctrine of Plausible Deniability. States are growing to depend on the use of proxies- privatized military contractors and criminal syndicates; but also on the services of the so-called patriotic hacktivists groups- to conduct their own cyber activities[14]. In keeping some distance between these actors, states are able to profess ignorance of the existence of the hostile activity or inability to control the hostile activity within the borders of the states. According to the contemporary principle in international law as developed by the International Court of Justice (ICJ) in the Nicaragua case, a state can only be able to bear responsibility of the actions of individuals belonging to a particular community only when it exercises effective control over the activity. The effective control is almost impervious to prove in the cyber world. A state may fund, provide intelligence or even the malware itself to a proxy group but unless they can prove that that particular command to press the button was issued by the state, then the legal connection has not been proven. This enables aggressors to circumvent the bans (the UN Charter and the Geneva Conventions) and allows them to wage a type of warfare that is in essence lawless, yet not yet on the level of formal armed conflict.

Moreover, the concept of deterrence based on which the world order is founded is placed in danger by the so-called Attribution Gap. The risk-to-reward ratio of cyber aggression is very positive when an actor is familiar with the fact that he can act behind a digital veil. The present system of IHL is based on the name and shame phenomenon and the possibility of being prosecuted in the International Criminal Court (ICC)[15]. The Rome Statute however by the ICC must identify certain persons to find criminal liability. In an international cyber attack in which the attacker is a black hat group or a government agency that is faceless, the chances of a successful prosecution are small. In this article, it is argued that the international community

should change towards a Due Diligence standard in order to bridge this gap[16]. According to such an evolution, a state would be accountable, not only to the cyber-attacks that it triggers, but also to its inability to ensure that the territory and infrastructure does not fall into the hands of third parties and is used to inflict damage on other states. It is only when the evidentiary bar is lowered, that it may no longer be effective control but rather a test of the so called sovereign due diligence that the law can start to close the attribution gap to deprive digital aggressors of their plausible deniability camouflage.

Conclusion: Toward a Digital Protocol

Cross-border cyber warfare is currently in evolutionary stages, and it comes across as one of the most sensitive issues to the stability of the international legal order ever. To elaborate on this aspect of digital operations, as this article has seen, the main conflict is that there is no fit between the kinetic based drafting of the Geneva Conventions and the virtual, borderless existence of digital activities.

To sum up, the sufficiency of the available IHL is at the moment of the brink. Although this is an excellent scholarly guidebook on how to take the long walk, the Tallinn Manual does not give the binding power needed to limit the behavior of states in the flare of geopolitical competition. What is needed is a two pronged solution: an extreme interpretation of the current treaties by international courts and eventual codification of a special tool – a so-called Digital Protocol – that tackles the specific issues of attribution and plausible deniability. We should shift towards a sort of Sovereign Due Diligence model wherein states are assigned some responsibility on the bad code that flies out of their borders. Digital age is not to be one of wanton lawlessness; it is supposed to be the time when IHL demonstrates its universality. This can be accomplished by recalibrating our legal definitions in ways that safeguard the so-called digital integrity of the human person, that is, the rule of law can be an effective check on power, notwithstanding when that power is exercised with a keyboard as opposed to a cannon.

Bibliography:

[1] Michael N. Schmitt, Cyber Operations and the Jus ad Bellum Revisited, 56 Vill. L. Rev. 569 (2011).

[2] Marco Roscini, Cyber Operations and the Use of Force in International Law 45–47 (2014)

[3] Protocol I, supra note 5, art. 49.

[4] Id

[5] Michael N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare 77–79 (2013).

[6] Id. At 78–80

[7] Id. At 79

[8] U.N. Charter art. 51.

[9] Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 48, June 8, 1977, 1125 U.N.T.S. 3.

[10] Yoram Dinstein, The Conduct of Hostilities Under the Law of International Armed Conflict 82–84 (3d ed. 2016).

[11] Protocol I, supra note 1, art. 51(3)

[12] Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International

Humanitarian Law 46–49 (ICRC 2009).

[13] Michael N. Schmitt, Cyber Operations and Accountability, 42 Yale J. Int'l L. 1, 15–17 (2017).

[14] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), 1986 I.C.J. 14, 115.

[15] Rome Statute of the International Criminal Court art. 25, July 17, 1998, 2187 U.N.T.S. 90.

[16] Michael N. Schmitt & Liis Vihul, Sovereignty in Cyberspace: Lex Lata and Lex Ferenda, 4 Tallinn Paper No. 2 (2014).