



## Original Article

# The Legal Implications of Cyber Warfare under International Humanitarian Law

**Dr. Shashikant Tripathi**

Associate Professor, Atal Bihari Vajpayee School Of Legal Studies, CSJMU, Kanpur,

Email- [drsktripathi@csjmu.ac.in](mailto:drsktripathi@csjmu.ac.in)

Manuscript ID:

JRD -2025-170501

ISSN: 2230-9578

Volume 17

Issue 5|

Pp. 1-5

May 2025

### Abstract:

*International humanitarian law (IHL) struggles to cope with the unprecedented challenge that modern conflict has created with the fact of cyber warfare becoming a key feature of battle. In this paper, traditional principles of armed conflict law are applied to cyber operations, exploring the legal gaps and interpretive issues which arise when cyberspace attacks critical infrastructure and civilian networks as well as military systems. This study shows, based on analysis of recent state practice, expert opinions and new case law, that principle of existing IHL principles are still valid of cyber warfare, yet that there are still substantial legal uncertainties as to attribution, proportionality and the protection of civilian cyber infrastructure. Here the article suggests that urgent legal standards clarification is required to prevent humanitarian protection erosion in cyberspace and proposes specific international legal development areas for the highest priority.*

**Keywords:** cyber warfare, international humanitarian law, digital attacks, civilian protection, military necessity

Submitted: 02 Apr. 2025

Revised: 08 Apr. 2025

Accepted: 23 May. 2025

Published: 31 May. 2025

### Introduction:

War has been fundamentally changed by the digital revolution. As operations become more involved in both interconnected networks and cyberspace, the divide between military and civilian digital infrastructure is continuing to blur. Cyber warfare in contemporary armed conflict has received growing attention in recent years with the 2007 cyber-attacks against Estonia, the 2010 Stuxnet operation against Iranian nuclear facilities, and the ongoing cyber aspects of the Ukraine conflict. This existing body of law developed largely in the context of kinetic warfare and physical destruction and human casualties and this recent development is posing challenges to that body of law.

The chapter that follows will demonstrate that international humanitarian law, as codified primarily in the Geneva Convention of 1949 and its Additional Protocols, sets out core principles relating to the conduct of hostilities. These principles are that there be distinction between combatants and civilians, proportionality in attack, precautions in attack and military necessity. However, there are difficult questions as to how these principles apply to cyber operations and particularly as to how digital attacks should be regulated under existing legal regimes.

### The Application of IHL to Cyberspace: - Legal Foundation and Threshold Issues-

The core IHL question in using the law of cyber warfare is what is an attack: when do cyber operations rise to the level of an attack under international humanitarian law? Under Additional Protocol I of the 1977 Geneva Conventions, an attack was defined as an act of violence against the adversary, either in offence or defence (Article 49; see also, Additional Protocol I, Article 51.) and the term violence was understood in terms of those acts that involved 'physical force causing death or injury to persons or damage to property. Yet, however, other forms of harm can be caused in cyber operations without traditional kinetic force.

### Creative Commons (CC BY-NC-SA 4.0)

*This is an open access journal, and articles are distributed under the terms of the [Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International](https://creativecommons.org/licenses/by-nc-sa/4.0/) Public License, which allows others to remix, tweak, and build upon the work noncommercially, as long as appropriate credit is given and the new creations are licensed under the identical terms.*

### Address for correspondence:

Dr. Shashikant Tripathi, Associate Professor, Atal Bihari Vajpayee School Of Legal Studies, CSJMU, Kanpur,

### How to cite this article:

*Tripathi, S. (2025). The Legal Implications of Cyber Warfare under International Humanitarian Law. Journal of Research & Development, 17(5), 1-5.*

<https://doi.org/10.5281/zenodo.15552906>



Quick Response Code:



Website:

<https://jrdrv.org/>

DOI: [10.5281/zenodo.15552906](https://doi.org/10.5281/zenodo.15552906)



In the Tallinn Manual 2.0, the view of leading international law experts is, broadly interpreted, to include cyber operations which result in death, injury or destruction (even without the use of physical force), because cyber-attacks can also be as functionally equivalent as kinetic attacks. For example, a cyber operation whose result is the power plant explosion or a hospital's medical equipment disruption has just as fatal consequences as ordinary weapons. This broad interpretation now finds support in state practice. Later, in 2021, the United States Department of Defence declared that 'cyberspace operations could also constitute uses of force or armed attacks under international law,' and that it is the effects of the uses and not the means, that determine the law status of a cyber operation.

### **The Principle of Distinction in Cyberspace:**

Principle of distinction prohibits to make war between parties to the conflict and said parties shall strive to the utmost to distinguish between combatant and civilians and between military objectives and civilian ones. Military objectives are objects which 'by their nature, location, purpose or use make an effective contribution to military action' (the definition in Article 52(2) of Additional Protocol I). This principle is quite hard to apply to cyber warfare. The boundaries between the military and civilians tend to merge as the digital infrastructure performs dual military and civilian use. Power grids, telecommunications networks and financial systems which are critical infrastructure, are usually used to support the civilian population, as well as to support military operations. However, the fact that cyberspace is intrinsically interconnected means that attacks on military networks can and most likely will affect and be experienced by civilian systems.

Ukraine's power grid was affected last year in 2016 with cyber-attacks from Russia backed group which resulted in power outages of almost 230,000 civilians. Electrical infrastructure supporting military installations may well be a legitimate military objective and may certainly be attacked, but the inherent civilian impact from such attacks can begin to chip away at the principle of distinction. These challenges, however, are increasingly gaining recognition in recent state practice. In the 2021 Brussels Communiqué NATO acknowledges that "in certain circumstances, significant malicious cumulative cyber activities might amount to an armed attack," a military language that reflects awareness that cyber operations must be assessed on impact rather than on method.

### **Proportionality and Precautionary Principles:**

An attack must not cause disproportion of civilian harm to expected military advantage. Article 51(5)(b) provides that "an attack must not be carried out when it may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof which would be excessive in relation to the concrete and direct military advantage anticipated". Proportionality in cyber warfare is a different beast to proportionality in physical war. The effects of cyber -attacks may be cascading, hard to predict or to control. Digital systems are inherently interconnected and seemingly limited operations will bring wide ranging disruptions. In 2017, Not Petya malware that started with a Ukrainian target affected civilian entities worldwide and is been costed at billions of dollars.

The proportions also prove more difficult to determine, as they are also analysed in the temporal dimension of cyber effects. Kinetic attacks have an obvious immediate result, but this is not so for cyber operations, the effects of which may be delayed or can appear over time. Questions about how to assess proportionality come when the full scale of civilian harm may not be known until after the attack. Parties to Additional Protocol I are obliged under Article 57 to do their "best to spare the civilian population," and to "take all feasible precautions in the choice of means and methods of attack," which applies in cyber space as well – including, at a technical level, designing cyber weapons to minimize civilian harm and implementing safeguards to prevent uncontrolled propagation.

### **Attribution Challenges:**

An interesting feature of applying IHL to cyber warfare, however, is the great challenge it poses in attribution. Conventional IHL then, presumes unambiguously defined conformity between the actions and party to the conflict. But cyber operations are commonly orchestrated deeply into attributions chains of state and non-state actors, proxy groups and sophisticated techniques used to hide responsibility. For a state's conduct to be attributable to it under international law, international law requires that there be 'effective control' over non-state actors for their actions to be attributed to a state. Conduct is also attributable to the state if it is performed by persons acting on the state's behalf or under its direction or control.

Cyberspace attribution challenges are brought out in recent cases. The SolarWinds supply chain attack in 2020, attributed to Russian intelligence services, targeted thousands of organisations around the world, but to attribute responsibility required substantial technical probing. Attribution risks in cyberspace include states escaping accountability for violations of IHL and that the attribution is incorrect and any responses directed accordingly.

### **Case Studies and State Practice: -**

#### **Stuxnet and Iran's Nuclear Program-**

It was the Stuxnet operation, found in 2010, that showed the impact cyber warfare can have. As a result of the malware developed jointly by the United States and Israel, approximately 1,000 uranium enrichment centrifuges at Natanz were physically harmed by the attack, according to reports. The use of Stuxnet by the United States and Israel

gives rise to several important concerns from an IHL viewpoint. The exercise indicated that cyber-attacks could now seriously harm physical properties as much as other weapons. The attackers developed this malware to target only particular industrial control details and steer clear of other civilian infrastructure. By being precise, sides likely observe the principle of clearly distinguishing targets and being if precaution is needed.

Still, attributing attacks in cyber warfare is very difficult. Though the evidence is clear, neither the US nor Israel have confessed to being responsible for carrying out the operation. Recognizing these acts is often difficult which adds problems to holding someone accountable under IHL.

### **Russian Cyber Operations in Ukraine:**

Even as conventional military action continues in Ukraine, so has the cyber operation. Ukrainian government networks, energy infrastructure and telecommunications systems have been targeted by Russian cyber-attacks against Ukrainian government networks, financial institutions and telecommunications systems. These operations are instructive with respect to IHL applicable to cyber warfare.

In 2015 and 2016, Ukraine's electrical grid was attacked directly with disruption of civilian infrastructure leading to power outages during the winter months. In all other respects, electrical infrastructure serving civilian populations would receive IHL protection from attack, unless the electrical infrastructure makes an effective contribution to military action. The method in the timing and scope of these attacks makes it seem likely that they were intended to revile the civilian population, rather than achieve some certain military goal, in violation of the principle of distinction.

During the 2022 phase of the conflict, more recent cyber operations have become more integrated with conventional military operations. Currently, cyber-attacks on Ukrainian government and military communications networks seem more clearly focused on legitimate military objectives. Nevertheless, it remains of concern that its scope of attacks against civilian infrastructure— including efforts to disable nationwide internet connectivity—provides the broadest IHL implications.

### **Estonia Cyber Attacks (2007):**

When the Soviet war memorial was moved to Estonia in 2007, it was the first large scale cyber-attack to occur on a country's whole digital infrastructure and left government websites, banks, media outlets and telecommunications networks paralyzed for several weeks.

These attacks took place outside the framework of armed conflict and are thus beyond the scope of IHL, yet they hold significant potential for framing our understanding of cyber warfare's effects on civilian population. It showed the strategic effects that are possible from cyber operations short of armed conflict.

### **Legal Gaps and Challenges: -**

#### **Temporal Aspects of Cyber Operations-**

Traditional IHL relies on the image of discrete acts of warfare with discrete temporal boundaries. For cyber, however, these are often persistent access to each other's networks, sleeping malware and more prolonged operations. For example, Stuxnet malware is said to have been active in Iranian networks for months or years before discovery. The temporal complexity of these events brooks with received notions of attack and defence under IHL. We question at which point a defensive cyber operation becomes an offensive attack and how 'the distinction principle' applies to cyber operations that have been inserted and remain dormant in civilian networks before being activated against military targets.

#### **Civilian Data and Digital Rights:**

The dimensional area of cyber warfare, as a novel form of warfare, raises new questions regarding the protection of civil data as well as digital rights as IHL. Unlike traditional humanitarian law that is concerned with the protection of persons and things, cyber operations can be directed against or lead to the adjudication of civilian data, with no associated physical damage. Civilian populations are at risk of experiencing significant harm to personal data, financial records and or digital communications through destruction, theft or malicious manipulation.

Of course, cyber operations can threaten civilian welfare without physical destruction by manipulating data: one need only look to the 2017 WannaCry ransomware attack which shut down hospital systems worldwide. But existing IHL frameworks do not offer guidelines to protect civilian digital assets and data.

#### **Autonomous Cyber Weapons:**

Artificial Intelligence and Machine Learning has enabled even greater autonomous cyber weapons with minimal human control to select and engage a desired target. Fundamental questions are being raised about human responsibility and accountability with respect to these capabilities under IHL.

Under Article 36 of Additional Protocol I, states must analyse new weapons under international law but in practice the pace of technological change in cyber capacities is frequently so rapid that it outstrips legal scrutiny. Autonomous cyber weapons capable of propagating and evolving on their own present particular problems for compliance with IHL principles requiring human judgment in decisions on targeting.

## Quantitative Analysis of Cyber Warfare Trends:

New data demonstrates that cyber warfare is becoming a bigger and bigger part of modern war. The Centre for Strategic and International Studies reports that 1,429 significant cyber incidents occurred between 2006 and 2023 – 34 percent were against government entities and 23 percent against critical infrastructure. Cyber capabilities are being massively spending money on by the military. The recently released United States Department of defence cyber budget grew from \$3.9Bn in fiscal year 2017 to \$11.2Bn in fiscal year 2023; aligned with its partners in NATO and other major powers. The challenges discussed above are revealed by attribution data. In fact, just 27 per cent of such cyberattacks, between 2020 and 2023, were formally attributed by victim states and even fewer resulted in legal accountability measures, according to research by the Atlantic Council.

Cyber warfare continues to grow with its civilian impact. As an example, the 2021 Colonial Pipeline ransomware attack impacted fuel supplies for the south-eastern United States and highlighted how cyber operations can generate strategic effects against civilian populations; additional similar incidents targeting healthcare, water treatment and transportation infrastructure continues to stress the vulnerability of these infrastructure systems to cyber-attack.

## Recommendations for Legal Development: -

**Clarification of Key Concepts-** In order to establish a clearer understanding of how existing IHL concepts apply to cyberspace, the international community should first do so. In particular we need to pay attention to the following areas:

1. A definition of "attack" in cyberspace: Clarifying, where possible, the circumstances under which cyber operations are to be considered an attack under IHL, including operations that cause functional damage (here: "impairment") rather than (physical) damage.
2. Criteria for identifying legitimate military targets in interconnected digital infrastructure: Military objectives in digital domain.
3. Assessment proportionality: Calculations of the proportionality measure when there are unpredictable cascading effects in the cyber-attacks.

## Attribution Standards-

Further development of international standards and procedures for cyber attribution would improve IHL related accountability. It might consist of:

1. Standards in a case of evidentiary nature: agreed criteria of state's responsibility for cyber operations.
2. International mechanisms for attributing cause for cyber-attacks.
3. Collective attribution: Attribution frameworks to ease some of this burden on victim states.

## Protection of All Digital Civil Infrastructure-

To achieve enhanced protection of civilian digital assets we need:

1. civilian data Recognition as protected objects under IHL of civilian data and digital services, an expanded definition of civilian objects.
2. Critical infrastructure protection (CIP): Digital infrastructure of such importance to civilian survival and well-being that special protection is needed.
3. Specific protection: Cyber ops civilians data protection obligations.

## Conclusion:

The application of international humanitarian law to cyber warfare is one of the most compelling challenges to contemporary international law. Existing IHL principles still apply, but come with gaps in the law as well as gaps in interpretation. As cyber capabilities increasingly become engrained in military operations and systems formerly considered civilian digital infrastructure increasingly become susceptible, the international legal community needs to take action urgently.

Classification concerns and the attribution challenges that necessarily arise, mean that state practice in this area is slowly developing but nontransparent and often opaque. Clear legal standards are all the more lacking, posing risks both to civilian protection and to military operators who must make dreaded targeting decisions under ever more uncertain legal frameworks.

In terms of promoting the further evolution of IHL as a coherent framework for regulation of cyber warfare, international community should emphasise on the clarification of legal standards which would be adopted in relation with existing IHL principles and also would take into account the particularities of cyberspace. Legal experts shouldn't be the only ones involved in this development, but also technical specialists who are aware of what cyber operations and what kind of effects they may generate.

The urgency of effective legal regulation is heightened by the growing and proliferating evolution of cyber capabilities. In this important field of modern warfare, the international community cannot afford legal uncertainty to continue, in the stakes are simply too high. In cyberspace we must protect civilian populations and do so by promptly and effectively adapting international humanitarian law to the digital age.



## References:

1. Traynor, Ian, "Russia accused of unleashing cyberwar to disable Estonia," *The Guardian*, May 17, 2007.
2. Zetter, Kim, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publishers, 2014), 47-52.
3. Greenberg, Andy, "The Untold Story of the 2018 Olympics Cyberattack, the Most Deceptive Hack in History," *Wired*, October 17, 2020.
4. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), Art. 49, June 8, 1977, 1125 U.N.T.S. 3.
5. Michael N. Schmitt, ed., *Tallinn Manual 2.0 on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2017), 415.
6. U.S. Department of defence, "Summary: Department of defence Law of War Manual" (2021), 2-3.
7. Additional Protocol I, Art. 52(2).
8. Lee, Robert M., et al., "Analysis of the Cyber Attack on the Ukrainian Power Grid," E-ISAC (2016), 4-7.
9. NATO Brussels Communiqué, June 14, 2021, para. 31.
10. Additional Protocol I, Art. 51(5)(b).
11. Greenberg, Andy, "The Untold Story of Not Petya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018.
12. *ibid*
13. Additional Protocol I, Art. 57.
14. *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States), Judgment, I.C.J. Reports 1986, 14, para. 115.
15. International Law Commission, "Articles on Responsibility of States for Internationally Wrongful Acts," Art. 8, U.N. Doc. A/56/10 (2001).
16. FireEye, "Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims with SUNBURST Backdoor," December 13, 2020.
17. Langner, Ralph, "Stuxnet: Dissecting a Cyberwarfare Weapon," *IEEE Security & Privacy*, Vol. 9, No. 3 (2011), 49-51.
18. Microsoft Digital Security Unit, "Special Report: Ukraine - An overview of Russia's cyberattack activity in Ukraine," April 27, 2022.
19. Tikk, Eneken, et al., "Cyber Attacks Against Georgia: Legal Lessons Identified," Cooperative Cyber Defence Centre of Excellence (2008), 12-15.
20. Collier, Rebecca, "WannaCry: The world's largest ransomware attack," *Computer Fraud & Security*, 2017(9), 5-8.
21. Additional Protocol I, Art. 36. <sup>1</sup> Centre for Strategic and International Studies, "Significant Cyber Incidents Database" (2023), available at <https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents>.
22. U.S. Department of defence, "Fiscal Year 2023 Budget Request: Cyberspace Activities," April 2022, 3.
23. Atlantic Council, "Cyber Attribution Database" (2023), available at <https://www.atlanticcouncil.org/programs/geotech-center/cyber-statecraft-initiative/>.
24. Turton, William and Mehrotra, Kartikay, "Hackers Breached Colonial Pipeline Using Compromised Password," *Bloomberg*, June 4, 2021.