INDUSJLSS.COM IJLSS INDUS JOURNAL OF LAW & SOCIAL SCIENCES

**Citation:** Nawaz, Adil, and Manahil Irfan. "The Legal Status of Cyber Warfare under International Humanitarian Law." Indus Journal of Law and Social Sciences 4, no. 1 (Spring 2024): 24–35. https://doi.org/10.70540/ijlss.2024(IV-I).03

Check for updates Cite Us

# The Legal Status of Cyber Warfare under International Humanitarian Law

**Pages:**1– 11 **Vol.**IV, **No.**I (Spring 2024) **p- ISSN:**3078-3666 **e- ISSN:**3078-3283

**Mr. Adil Nawaz** Advocate, District and Session Court
Department: Law Graduates from "University of Peshawar"

**Miss. Manahil Irfan** Advocate, District and Session Court
Department: Law Graduates from "University of Peshawar"

***Doi:****10.70540/ijlss.2024(IV-I).03* *Doi Link:* *https://doi.org/10.70540/ijlss.2024(IV-I).03*

Contents



***Abstract:*** *Such unprecedented challenges to the application of traditional International Humanitarian Law (IHL) have been caused by the rapid growth of cyberwarfare capabilities. Within the scope of the current legal standards and the application to cyberspace of armed conflict, the article also focuses on the Geneva Conventions and other Protocols. The most significant legal ambiguities identified in the study after the review were the applicability of the proportionality concept in cyberspace where consequences are unpredictable and may have far-reaching effects, the distinction between civilian and military cyber infrastructure, and the perception of cyberattacks as attacks under IHL. Recent state actions, including cyber activities in Ukraine, Georgia, and Estonia, highlight the urgent need for clarity in the law. The article argues that even though the present principles of IHL still have relevance to the realm of cyber warfare, their comprehension has to be distorted to reflect the particular characteristics of cyberspace, namely, issues of attribution, dual-use systems, and transnational effects. The research concludes that there needs to be a more comprehensive international agreement to prevent basic humanitarian protection from being undermined by cyber activities in modern warfare.*

**Keywords:**
Cyber warfare, International Humanitarian Law, Geneva Conventions, Armed conflict, Cyber-attacks, Distinction principle, Proportionality, Attribution, State responsibility, Dual-use infrastructure, Cross-border cyber operations

## 1. Introduction

The Not Petya malware breach on June 27, 2017 of the digital infrastructure of Ukraine and its subsequent spread across the globe caused billions in losses and targets hospitals, shipping companies, and government functions[1] that begs a big question in international law: What are the implications of the well-established principles of the International Humanitarian Law (IHL) in case of a conflict involving fiber optic cables and data centers?

Cyber warfare can be illustrated as the most significant development in military warfare since the development of aerial power. Unlike conventional tools of war, which cause physical destruction, cyber operations have the capacity to disable critical infrastructure, manipulate the information systems and cause pain to civilians without surpassing the limits of traditional physical warfare.[2] The law also has a price: when a cyber-attack on the network of a hospital prevents essential medical services, what is the legal analogy of a missile strike at the same place.

This article argues that despite the fact that existing IHL principles may be applied to cyber warfare, their application requires significant doctrinal development and state practice to address the specifics of the online realm. The analysis proceeds in three parts: first is how cyber warfare is integrated into the jus ad bellum framework in the sense of reasonableness of force use; second is how the fundamental principles of international humanitarian law i.e. Distinction, proportionality, and precautions, apply to cyber warfare; and third is the current efforts to clarify the law i.e. The Tallinn Manual procedure and the emerging state practice.

This legal change is extremely significant. The International Committee of the Red Cross (ICRC) believes that the next battlefield is cyberspace[3] but the necessary questions of civilian safety and allowable attacks in digital conflicts are not clarified completely.

## 2. Current Legal Framework and Threshold Issues

### 2.1 Defining Cyber Warfare and the Armed Attack Threshold:

The initial step in the application of international law to cyberwarfare is threshold questions: when are cyberattacks considered armed attacks that invoke the right to self-defense of Article 51 of the UN Charter, and when are cyber hostilities considered armed conflicts that are legally recognized under the IHL.[4] The test that was developed by the International Court of Justice in the Nicaragua case and is known as the scale and effects test.

---

[1] Andy Greenberg, The Little-Known Tale of NotPetya, the Most Destructive Cyberattack in History 22 August 2018 Wired The world was destroyed because of a cyberattack on Ukraine and Russia with a Russian code.)https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[2] Significant Cyber Incidents Since 2006," Centre for Strategic and International Studies (2024) Important Cyber Incidents: https://www.csis.org/programs/strategic-technologies-program.

[3] manual Tallinn Manual 2.0 on International Law Relevant to Cyber Operations, Michael N. Schmitt (ed.), 2nd edn, Cambridge University Press 2017, 3045.

[4] International Committee of the Red Cross, Cyber Operations in Armed Conflicts and International Humanitarian Law (ICRC Position Paper, November 2019) 1.

The scale and effects test are referred to as the test developed by the International Court of Justice in the case of Nicaragua[5] can be applied but the problem of cyber operations which apply kinetic mechanisms is problematic. Even without physical damage, cyber operations can lead to tremendous havoc because traditional attacks, which cause immediate physical damage, are not the case. The 2007 Estonian cyber-attacks proved that digital operations can effectively put a country in a state of inability to operate the banking, media and government systems without following the traditional armed attack principles.[6]

The Tallinn Manual 2.0 follows an effects-based approach, consistent with the opinions of most international legal experts. In cases where the consequences of cyber operations are comparable to those of traditional attacks, they are considered to be armed attacks.[7] In this evaluation, the factors of severity, immediacy, directness, invasiveness, measurability, and presumed legitimacy of targets are taken into account.[8]

### 2.2 The Temporal Challenge: When Does Armed Conflict Begin?

Cyber activities challenge conventional temporalized armed conflict. IHL applies to a conflict that is armed conflict, but it may be hard to distinguish the start of a conflict, as cyber-attacks can take place continuously and at low levels without a definite timeframe[9] as observed in the case of the war in Georgia and Russia in 2008, which was preceded and accompanied by cyber-attacks not existing at any specific boundaries.[10]

Besides, attribution issue such as determining the actor on cyber activities also makes threshold establishment more complicated. In contrast to traditional attacks, cyber operations often involve the use of non-state proxies, criminal networks, or false flag activities that hide the involvement of the state, which is hard to establish in cyberspace.[11] In cyberspace, Article 5 on State Responsibility by the International Law Commission is not usually met.[12]

## 3. Core IHL Principles of Cyber Operations

### 3.1 The Principle of Distinction in Cyberspace

The principle of IHL that separates combatants and civilians, military and civilian objects is challenged differently

[5] United Nations Charter, article 51; See Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons [1996]. Rep. 226, paragraph 39, ICJ.
[6] Nicaragua v. United States: Armed Forces and Paramilitary Activities in and against Nicaragua (Merits) [1986] ICJ Rep 14, para 191, 195.
[7] VII Jason Richards, Service Denial, The Estonian Cyber Conflict and the Implications of the Incident on 18 International Affairs Review 1 (U.S. National Security, 2009).
[8] Schmitt (n 3) 341-343.
[9] ibid 343-347.
[10] Cambridge University Press, 2016, p. 15-18. Yoram Dinstein, The Conduct of Hostilities in the Law of International Armed Conflict, 3 rd. edition...
[11] 60 parameters Joshua E. Kastenberg and Stephen W. Korns, Georgia Cyber Counterpunch (2008) 60 parameters.
[12] Jason Healey (ed), A Fierce Domain: Conflict in Cyberspace, 1986 to 2012 (Atlantic Council 2013) 180-195.

in cyberspace.[13] The integrated nature of cyberspace means that[14] potentially civilian systems may have dual-use capabilities or significant military purposes.

### 3.2 Civilian Infrastructure as a military Objective.

The issue is can civilian cyber infrastructure can be considered as a legitimate military target because it facilitates military actions. According to the Tallinn Manual, civilian cyber infrastructure can fall under a military target in situations where its destruction can give a definite military advantage and contribute to military operations in an effective way.[15] In systems with equal infrastructure based on the civilian and the military, this criterion is however hard to apply.

Consider electrical grids: notwithstanding that the generation of power is a strictly civil activity in its essence, the military bases and weaponry use electricity as well. Traditional IHL states that power plants may be treated as valid targets in case they are of significant military use and their destruction can bring a visible military advantage.[16] But cyber-attacks on power plants can target specific military facilities through active manipulation of the network, potentially reducing the overall harm to civilians.[17]

### 3.3 Information as Safeguarded Non-Combatant Assets

The condition of civilian data poses a new legal issue. The Tallinn Manual assumes that information related to civilians is just as well protected as corporeal civilian property and it follows that any destruction or manipulation of such information without military necessity would be considered an illegal attack[18] on civilian targets unless it reaches a military level of significance.

The current state practice favors this interpretation. The ICRC has highlighted that medical data should be given specific protection owing to the fact that its destruction may result in civilian loss similar to that witnessed by kinetic attacks[19] such as the Ireland Health Service executive attack in 2021, which encrypted patient records and disrupted medical neutrality.[20]

### 3.4 Proportionality in Cyber Warfare

The IHL doctrine of proportionality would prohibit in cyberspace any attack that causes excessive civilian harm compared with the anticipated military advantage.[21] The balance here is particularly difficult to attain in a

[13]Articles 4-11, International Law Commission Draft Articles on State Responsibility in the Case of Internally Wrongful Acts (2001) UN Doc A/56/10.
[14] The Nineteenth, the Protection of the Victims of International Armed Conflicts (protocol I), 8 June 1977, Article 48, 1125 UNTS 3, Supplementary to the Geneva Conventions of August 12, 1949.
[15] Ibid., art. 52(2).
[16] Schmitt (n 3) 439-442.
[17]Final Report to the Prosecutor by the Committee Formed to Assess the NATO Bombing Campaign against the Federal Republic of Yugoslavia (ICTY 2000) para 91.
[18]Stateless Attribution: Fostering Global Accountability in Cyberspace, John S. Davis et al. (RAND Corporation 2017) 4567.
[19] Schmitt (n 3) 447-450.
[20] Health Service Executive, 'HSE Cyber Incident: After Event Independent Review' (December 2021).
[21] (16 October 2020) ICRC, 'Health care in danger: cyberattacks'

networked environment because networks are interconnected.

### 3.5 Reverberating Effects and Civilian Harm

Interconnection of networks can cause unpredictable results of cyber-attacks in regard to the civilians. This can be seen in the Stuxnet case of 2010 which targeted the nuclear facilities in Iran. It can be argued that the short-term military objective of disrupting uranium enrichment was commensurate, the malware went beyond the target of disrupting the uranium enrichment operations and spread to the civilian industrial systems across the globe.[22]

The Tallinn Manual requires consideration of the reasonably foreseeable ripple effects in the process of proportionality assessment[23] however, the ability to determine foreseeability in the context of complex cyber systems presents challenges to traditional legal frameworks. Do military leaders take into account potential spillover effects of networks? What do we weigh between the benefits of the military and the possible civilian destruction?

### 3.6 Temporal Dimensions of Cyber Harm

Cyber operations may cause either delayed or long-term effects in contrast with attacks that are kinetic and result in immediate damage. Malware may remain idle over extended periods of time or cause gradual system degradation. Such a time-based complexity makes assessments of proportionality more challenging since civilian casualties can occur a long time after the first action.

The Not Petya attack in 2017 illustrates this issue. The malware was originally intended to attack the government and infrastructure of Ukraine but the architecture[24] thereof had global consequences, with hospitals, shipping companies, and factories feeling the consequences long after the fact of its release, forcing a reevaluation of proportionality in cyber warfare.[25]

### 3.7 Precautionary Obligations in Cyberspace

IHL requires that parties always take necessary care of safeguarding civilians and civilian objects.[26] This will involve the duty to select methods and means that minimize civilian loss of life and to give advance warning where circumstances permit.[27] In cyberspace, these requirements translate into certain technical and operational requirements.

### 3.8 Technical Precautions

The weaponry should be made in such a way that the impact of civilians is reduced by technical means. This can involve geofencing (restricting malware to particular geographic coverage), target validation, self-destruction

[22] Protocol I (n 14) article 51(5)(b)
[23] Kim Zetter, Countdown to Zero Day: Stuxnet and the First Digital Weapon in the World (Crown Publishers 2014) 350-367
[24] Schmitt (n 3) 467-470.
[25] According to Ellen Nakashima et al. Washington Post, January 12, 2018, the CIA has evaluated that the Russian military was suspect of the hack known as NotPetya in Ukraine.
[26] Mondelez International Inc v Zurich American Insurance Co, 2021 WL 6540989 (US District Court Illinois 2021).
[27] Protocol I (n 14) article 57(1).

capability[28] or a combination of these features, with the Stuxnet malware, although later becoming prolific, including checks by specific industrial control systems and geographic identifiers.[29]

The technical nature of precautionary steps however makes questionable the possibility of feasible implementation. Should states build cyber weapons that have flawless containment even when such limitations limit military capability? According to the Tallinn Manual precautionary obligations should be feasible under operational conditions, but this does not offer much guidance to emerging technologies.[30]

### 3.9 Warning Obligations

The traditional IHL presupposes that an advance warning is given about attacks on civilians except in situations that do not allow it.[31] In the world of cyberspace, the duty of giving warnings has its own challenges. The alert of looming cyber-attacks can enable defenders to take countermeasures which can offset military advantage. Besides that, the urgency of the majority of cyber activity may make the possibility of prior notice technically impossible.

The ICRC has proposed that cyber-attack warnings must be operationally feasible but without revealing military targets.[32] This may involve broad notification of the upcoming attack on particular sectors as opposed to detailed target information. Nevertheless, there is the state practice that is still the narrow and most of the military cyber doctrines practiced perpetuate operational security at the expense of the warning requirement.

## 4. Contemporary developments and legal clarification

### 4.1 The Tallinn Manual Process and Expert Consensus.

Tallinn Manual may be considered the most successful attempt to apply the existing international law into cyberspace. Conceived by two editions (2013 and 2017) under the guidance of experts in international law, the Manual examines how IHL principles apply to cyber operations[33] and has informed the state stance and military cyber doctrine in many countries around the world.

### 4.2 Key Contributions

The main contribution that the Manual has made is that it has translated abstract legal principles into a practical guide to cyber operations. Its provisions on targeting civilian infrastructure, information protection, and precautionary requirements offer structures of legal argumentation in areas hitherto not included in the

[28] ibid arts 57(2)(a), 57(2)(c).
[29] Schmitt (n 3) 481-485.
[30] Zetter (n 23) 180-195.
[31] Schmitt (n 3) 484.
[32] Protocol I (n 14) art 57(2)(c).
[33] ICRC (n 4) 8-9.

international law discussion.[34]

Nevertheless, another issue found in the Manual is that there are major disputes between professionals. The question of whether non-state cyber entities fall within the scope of state accountability, whether armed conflict can be found to take place in cyberspace, and whether human rights law can be enforced extraterritorially in cyberspace are controversial matters[35] that demonstrate a more profound failure to apply traditional legal concepts to new technology.

### 4.3 Recent State Practice and Doctrinal Development

The law of cyber warfare at the state level has yet to be properly developed, but it is actively being elaborated in military manuals, government posts and experience on the practice. The 2022 Russia-Ukraine conflict offers the first-ever lessons on the way states frame the legal restrictions on cyber activity.

The law of cyber warfare in state practice is still a very small area under development, and it is developing gradually by creating military manuals on the practice of warfare, its posts by government, and its experiences. The 2022 Russia-Ukraine crisis offers unprecedented understanding of the ways states imagine legal limits on cyber activities.

### 4.4 NATO and Allied Positions

In 2016, the Warsaw Summit of NATO recognized the sphere of cyberspace as part of the scope of operation and therefore permits the application of Article 5 to collective defense in suitable circumstances[36]although it did not specify what circumstances would arise when the use of collective defense was necessary in an incident of cyber-attacks.

The United States has proposed the most detailed public policy regarding the law of cyber war. The Department of Defense Law of War Manual specifically reflects on cyber operations within IHL, with much of its consideration consistent with that of the Tallinn Manual[37] but significant gaps still exist, especially concerning autonomous cyber weapons and cross-border data transfer in the context of armed conflict.

### 4.5 The Ukraine Conflict and new practice

The 2022 Russian invasion of Ukraine has involved widespread cyber operations along with conventional warfare that has provided a practical demonstration of the law of cyber warfare. At the beginning of the war, Russia has carried out cyber-attacks on the Ukrainian government telecommunications and energy infrastructure[38] whereas Ukraine has responded with cyber-attacks against Russian targets and by accepting the help of volunteer cyber

[34] Michael N Schmitt (ed), Tallinn Manual on the International Law Relevant to Cyber Warfare (Cambridge University Press 2013); Schmitt (n 3).
[35] Schmitt (n 3) 1-15.
[36] same source 565-580.
[37] NATO, 'Warsaw Summit Communiqué' (9 July 2016) paragraph 70.
[38] The US Department of Defense, Law of Armed Conflict Manual, June 2015, revised 2016; ch. 16.

militias.[39]

Such activities pose new legal issues on the involvement of civilians in cyberspace warfare. The traditional IHL allows civilians to join the levée end masse scenarios, yet cyber operations make it tricky to establish the scope of the geography, the time constraint, as well as the combatant status.[40] The incorporation of civilian cyber into the military operations by Ukraine indicates a change in state action in regard to civilian involvement in cyber warfare.

### 4.6 International Committee of the Red Cross Position

ICRC has played a leading role in clarifying how IHL can be applied to cyberspace. According to its 2019 position paper, the current application [41] claims of cyber-specific legal frameworks do not negate IHL to cyber operations, and the protection of civilians and civilian infrastructure, especially healthcare and essential services is essential.

### 4.7 Healthcare Protection

The ICRC has highlighted specific issues relating to cyber-attacks on medical systems, and said that any digital interference with medical services and medical infrastructure may pose the same threat to patient security as kinetic attacks[42] which must be given specific protection under IHL.

These concerns are supported by recent cyber-attacks on systems of healthcare systems during the COVID-19 pandemic. The 2020 attack on a University Hospital in Dusseldorf that displaced patients and allegedly caused the death of one of them can exemplify the way cyber operations targeting healthcare can require a breach of the medical neutrality principles provided by IHL.[43]

## 5. Critical Assessment and Future Challenges

### 5.1 Enforcement and Accountability Gaps

Cyber warfare law has enormous gaps in its enforcement even though it has gone through doctrinal development. In contrast to conventional weapons, cyber operation often deals with privately owned infrastructure, cross-border formations, and non-state actors, which act with a certain level of state regulation.[44] These attributes make it more difficult to apply the traditional ways of the enforcement regime of state responsibility and personal criminal liability.

### 5.2 Attribution and State Responsibility

[39]Microsoft, Special report: Ukraine - summary of Russia-based cyberattacks (27 April 2022).
[40]Andy Greenberg, Ukraine's IT Army has raised up 300,000 hackers. Yet, Is It Allowed? Wired (March 21, 2022).
[41]Protocol I (n 14) art 4(A)(6); see also Hague Convention IV Regarding the Laws and Customs of War on Land, 18 October 1907, art 2.
[42] ICRC (n 4) 2-3..
[43] ibid 10-11.
[44] Catalin Cimpanu, 'Patient dies after ransomware attack reroutes her from German hospital' ZDNet (18 September 2020).

The attribution problem is probably the biggest obstacle to cyber warfare law. In order to establish state responsibility, one must prove that cyber operations can be ascribed to the state because of its agents or persons acting under its direction and control.[45] But the use of non-state proxies, criminal networks, and false flag operations that blur direct connections to the state authority is becoming increasingly used by states.

The latest progress in the field of cyber attribution indicates that some unity might be reached regarding the standards of circumstantial evidence. The 2017 NotPetya attack indictments of 2018 were not based on actual evidence of state ownership, but on technical indicators, intelligence sources, and operational patterns.[46] To convert such evidence into legal conclusions that the state owned the attack remains a difficult task.

### 5.3 Individual Criminal Responsibility

Cyberspace IHL violations can be a subject of war crimes punishable individually under the Rome Statute[47] but there are special difficulties in prosecuting cyber war crimes: jurisdiction, preservation of evidence, and technical difficulty of cyber actions.

The preliminary examination of alleged cyber war crimes in the case in Georgia by the International Criminal Court provides information on the manner in which the prosecutorial would treat the situation[48] but no international prosecution of cyber war crimes has received a trial, leaving a lot of legal ambiguity on the standards of individual responsibility.

### 5.4 Autonomous Cyber Weapons and Legal Compliance

The first challenge to IHL compliance[49] is the development of autonomous cyber weapons, i.e. malware capable of target selection and autonomous attack on victims without human oversight, because the speed and scale of such an autonomous system might be beyond the ability of a human agent to manage.

### 5.5 Machine Learning and Targeting Decisions

The use of machine learning algorithms to identify targets and optimize attacks is becoming increasingly popular in advanced cyber weapons. Such systems might develop out of their initial programming, and it is doubtful that the autonomous targeting decisions[50] of military commanders can be held to any meaningful responsibility.

The ICRC has made the case that autonomous weapon systems must be meaningfully under human control, meaning that humans need to make targeting choices when it comes to civilian protection[51] but the high speed of cyber weapons (in the range of milliseconds) and the complexity of network operations make this difficult to

[45]Jason Healey, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks' (Atlantic Council Issue Brief, January 2011).
[46] ILC Articles (n 13) art 8.
[47] Six Russian GRU Agents Accused of Globally spreading Malicious Software and other Cyberattacks, US Department of Justice, October 19, 2020.
[48]Neutralized, 17 July 1998, 2187 UNTS 3, article 8.
[49]ICC, Preliminary Examination Activities Report 2019 (5 December 2019) paras 158-172.
[50]Losing Humanity: The Case Against Lethal Machines, Human Rights Watch (November, 2012) 1 5.
[51]Stuart Russell, Human Compatible: Artificial Intelligence and the Control Issue (Viking 2019) 173-195.

achieve. However, it should be noted that some new technologies are being developed, and these are likely to be adopted by the law courts as they come into existence.

The pace of technological change in cyber capabilities is such that it keeps exerting continuous pressure on legal development by creating gaps between legal frameworks and the realities of operations. Significant further development of quantum computing, artificial intelligence, and the Internet of Things is therefore likely to need further legal adjustment.[52]

### 5.6 Quantum Computing Implications

Quantum computing holds the potential to transform the offensive and defensive capabilities of cyber[53] including making existing encryption technologies obsolete and allowing new capabilities to be achieved without kinetic action. The impact on civilian protection is also immense: quantum-enabling surveillance technologies can only threaten the privacy rights on a scale never before seen, whereas quantum cyber weapons may be capable of causing effects previously possible only through kinetic action.

The legal frameworks should be able to foresee these developments before the situations of fait accompli are achieved through large-scale deployment. The European Union proposed the Cyber Resilience Act proposes regulatory strategies for new cyber technologies, and yet international legal adaptation is minimal.[54]

## 6. Recommendations and Future Directions

### 6.1 Institutional Mechanisms for Legal Development

The existing ad hoc method of the expansion of the law of cyber warfare with the assistance of expert processes and the bilateral state practice needs to be institutionalized in order to make the law evolve constantly. A number of processes have the potential to increase the clarity and adherence to the law.

### 6.2 Multilateral Treaty Negotiation

Although the process of the Tallinn Manual has offered important clarification, non-binding expert opinion can never be used to replace the state-negotiated legal obligations. A multilateral weapon of cyber war, like a weapons prohibition treaty, might create explicit legal norms with the flexibility to operate.[55] Nevertheless, the chances of full-scale cyber warfare treaties seem minimal due to its strategic competition and uncertainty in technology. Less ambitious strategies could target particular challenges, including healthcare insurance, civilian infrastructure, or automated weapon restrictions.[56]

---

[52] ICRC, Autonomous weapon systems Technical, military, legal, and humanitarian considerations (Expert Meeting Report, March 2014) 2528.

[53] World Economic Forum, global risks report 2024, January 2024, pages 4552.

[54] Authors: National Institute of Standards and Technology, 2022 by title

[55] European Commission, Draft Regulation on cybersecurity standards of network and information systems COM (2022) 454 final.

[56] UNTS, preview UNTS 211, 18 September 1997, Convention on the Prohibition of Anti-Personnel Mines.

### 6.3 International Judicial Clarification

The international tribunals can make authoritative rulings on the law of cyber warfare by cases or advisory opinions. Criminal prosecution in the case of the International Court of Justice in Genocide Allegations (Ukraine v.). Cyber activity could be considered by the Russian Federation as possibly carrying the purpose to commit genocide, thus would have precedential importance in future cyber warfare jurisprudence.[57] The judiciary has been offering state duties on the internet and it has been the European Court of Human Rights to hear the cases where government spies on its citizens and cyber-attacks.[58]

### 6.4 Practical Implementation Measures

In addition to what is being done in legal development on paper, actions on the ground would improve adherence to the current IHL principles in cyber activities.

### 6.5 Military Training and Doctrine

Cyber operations are technical, and therefore, military cyber units need specialised training on IHL compliance. Such training should cover both legal and technical aspects of implementation with the understanding that the operators should know the civilian protection needs and precautionary measures involved.[59] Law compliance could be systematized through the development of targeting protocols of cyber operations comparable to those aimed at conventional weapons. These protocols are to cover target validation processes, collateral damage analysis, and reverberating effects.[60]

### 6.6 Public-Private Cooperation

Since cyberspace depends on privately operated infrastructure[61] to protect civilians, collaboration between the military and civilian actors is needed. The legal frameworks are to explain the duties of private companies that host military cyber missions and the duties of protection to the civilian infrastructure providers. Cyber red cross/red crescent markers that are set up to depict the existence of a secure system would aid in identifying and securing civilian infrastructure in the event of cyber warfare. Nevertheless, these mechanisms need technical standards of implementation and verification processes that international law[62] does not have today.

---

[57]The statement 'Promoting responsible State activity in cyberspace as far as international security is concerned' (2021) UN Group of Governmental Experts, UN Doc A/76/135.

[58] The Convention on the Prevention and Punishment of the Crime of Genocide (Russia v.) has claims of genocide. P. pursuant to the agreement of Ukraine), Provisional Measures Order of the International Court of Justice (16 March 2022).

[59] ECtHR ansökan nr 35252/08, Centrum för Rättvisa mot Sverige, 19 juni 2018.

[60]Marco Roscini, Use of Force by Cyber Operations and International Law (Oxford University Press 2014) 220-245.

[61]Program on Humanitarian Policy and Conflict Research, Handbook on International Law Relevant to Air and Missile Warfare (Cambridge University Press 2013) 45-67.

[62] The Public Core of the Internet: An International Agenda for Internet Governance' (Netherlands Scientific Council for Government Policy 2018). Dennis Broeders et al.,

## 7. Conclusion

One of the most difficult issues of contemporary international law is the legal status of cyberwarfare in the framework of the international humanitarian law (IHL). Although the existing IHL principles, namely, the principles of distinction, proportionality, and precaution, set the principled framework of protecting civilians in cyberspace, the principles of digital operations, in their turn, require significant intellectual maturation and nationalization to consider the peculiarities of cyberspace warfare. Also, questionable threshold issues, such as when a cyber operation counts as an armed attack and when it begins to appear that it is an armed conflict, pose interpretation challenges as well. The fact that the data remains a civilian asset, the fact that networks are interconnected, and the presence of ripple effects also offer interpretation challenges. Despite the pronounced gaps in the enforcement of the existing legal standards and the technical adjustment of reality, the Tallinn Manual process and the emerging state practice have also cast important light on how to fit IHL into the cyber environment.

The necessity of a legal understanding grows as cyber warfare capabilities grow and conflicts become more and more blended with digital capabilities and old-fashioned military force. The Russia-Ukraine conflict has presented some rare insights into the essence of cyber activities in warfare, yet the international legal community must make use of them to come up with strong legal provisions to protect civilians in cyberspace. In the development of legal regulation in future, institutional improvement in rule-making, real measures to make military adherence to rules and measures to be proactive to address new developments should be considered. The key question is not whether IHL applies to cyberspace, as the International Committee of the Red Cross (ICRC) and other distinguished scholars agree on this point, however, how do we make sure that the conventional principles of military necessity and protection of civilians will be maintained in the twenty-first century digital combat? It is only as international law is progressively refined based on operational realities and humanitarian concerns that it can be used to avert the escalation of cyber conflict to the wanton destruction of civilian life and critical infrastructure.

**Reference**

[1] Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' *Wired* (22 August 2018) https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[2] Center for Strategic and International Studies, 'Significant Cyber Incidents Since 2006' (2024) https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

[3] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (2nd edn,

Cambridge University Press 2017) 30-45.

[4] International Committee of the Red Cross, 'International humanitarian law and cyber operations during armed conflicts' (ICRC Position Paper, November 2019) 1.

[5] Charter of the United Nations, art 51; see also Legality of the Threat or Use of nuclear weapons (Advisory Opinion) [1996] ICJ Rep 226, para 39.

[6] Military and Paramilitary Activities in and against Nicaragua (Nicaragua v United States) (Merits) [1986] ICJ Rep 14, paras 191, 195.

[7] Jason Richards, 'Denial-of-Service: The Estonian Cyberwar and its Implications for U.S. National Security' (2009) 18 International Affairs Review 1.

[8] Schmitt (n 3) 341-343.

[9] ibid 343-347.

[10] Yoram Dinstein, *The Conduct of Hostilities under the Law of International Armed Conflict* (3rd edn, Cambridge University Press 2016) 15-18.

[11] Stephen W Korns and Joshua E Kastenberg, 'Georgia's Cyber Left Hook' (2008) 60 Parameters 60.

[12] Jason Healey (ed), *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012* (Atlantic Council 2013) 180-195.

[13] International Law Commission, 'Articles on Responsibility of States for Internationally Wrongful Acts' (2001) UN Doc A/56/10, arts 4-11.

[14] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977, 1125 UNTS 3, art 48.

[15] ibid art 52(2).

[16] Schmitt (n 3) 439-442.

[17] Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia (ICTY 2000) para 91.

[18] John S Davis and others, *Stateless Attribution: Toward International Accountability in Cyberspace* (RAND Corporation 2017) 45-67.

[19] Schmitt (n 3) 447-450.

[20] Health Service Executive, 'HSE Cyber Attack: Independent Post Incident Review' (December 2021).

[21] ICRC, 'Health care in danger: cyberattacks' (16 October 2020) https://www.icrc.org/en/document/health-care-danger-cyberattacks.

[22] Protocol I (n 14) art 51(5)(b).

[23] Kim Zetter, *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon* (Crown Publishers 2014) 350-367.

[24] Schmitt (n 3) 467-470.

[25] Ellen Nakashima and others, 'Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes'

*Washington Post* (12 January 2018).

[26] Mondelez International Inc v Zurich American Insurance Co, 2021 WL 6540989 (USDC Ill 2021).

[27] Protocol I (n 14) art 57(1).

[28] ibid arts 57(2)(a), 57(2)(c).

[29] Schmitt (n 3) 481-485.

[30] Zetter (n 23) 180-195.

[31] Schmitt (n 3) 484.

[32] Protocol I (n 14) art 57(2)(c).

[33] ICRC (n 4) 8-9.

[34] Michael N Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press 2013); Schmitt (n 3).

[35] Schmitt (n 3) 1-15.

[36] ibid 565-580.

[37] NATO, 'Warsaw Summit Communiqué' (9 July 2016) para 70.

[38] US Department of Defense, *Law of War Manual* (June 2015, updated 2016) ch 16.

[39] Microsoft, 'Special Report: Ukraine - An overview of Russia's cyberattacks' (27 April 2022).

[40] Andy Greenberg, 'Ukraine's "IT Army" Has Assembled 300,000 Hackers. But Is It Legal?' *Wired* (21 March 2022).

[41] Protocol I (n 14) art 4(A)(6); see also Hague Convention IV Respecting the Laws and Customs of War on Land, 18 October 1907, art 2.

[42] ICRC (n 4) 2-3.

[43] ibid 10-11.

[44] Catalin Cimpanu, 'Patient dies after ransomware attack reroutes her from German hospital' *ZDNet* (18 September 2020).

[45] Jason Healey, 'Beyond Attribution: Seeking National Responsibility for Cyber Attacks' (Atlantic Council Issue Brief, January 2011).

[46] ILC Articles (n 13) art 8.

[47] US Department of Justice, 'Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Cyber Attacks' (19 October 2020).

[48] Rome Statute of the International Criminal Court, 17 July 1998, 2187 UNTS 3, art 8.

[49] ICC, 'Report on Preliminary Examination Activities 2019' (5 December 2019) paras 158-172.

[50] Human Rights Watch, 'Losing Humanity: The Case Against Killer Robots' (November 2012) 1-5.

[51] Stuart Russell, *Human Compatible: Artificial Intelligence and the Problem of Control* (Viking 2019) 173-195.

[52] ICRC, 'Autonomous weapons systems: Technical, military, legal and humanitarian aspects' (Expert Meeting

Report, March 2014) 25-28.

[53] World Economic Forum, 'The Global Risks Report 2024' (January 2024) 45-52.

[54] National Institute of Standards and Technology, 'Post-Quantum Cryptography Standardization' (2022).

[55] European Commission, 'Proposal for a Regulation on cybersecurity requirements for network and information systems' COM (2022) 454 final.

[56] Compare Convention on the Prohibition of Anti-Personnel Mines, 18 September 1997, 2056 UNTS 211.

[57] UN Group of Governmental Experts, 'Advancing responsible State behavior in cyberspace in the context of international security' (2021) UN Doc A/76/135.

[58] Allegations of Genocide under the Convention on the Prevention and Punishment of the Crime of Genocide (Ukraine v Russian Federation), ICJ Provisional Measures Order (16 March 2022).

[59] Centrum för Rättvisa v Sweden, ECtHR App no 35252/08, 19 June 2018.

[60] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford University Press 2014) 220-245.

[61] Program on Humanitarian Policy and Conflict Research, *Manual on International Law Applicable to Air and Missile Warfare* (Cambridge University Press 2013) 45-67.

[62] Dennis Broeders and others, 'The Public Core of the Internet: An International Agenda for Internet Governance' (Netherlands Scientific Council for Government Policy 2018).

[63] Knut Dörmann, 'The Legal Situation of "Unlawful/Unprivileged Combatants"' (2003) 85 International Review of the Red Cross 45.