CYBER WARFARE AND THE FUTURE OF INTERNATIONAL HUMANITARIAN LAW

Anurag Singh, New Law College, BVP, Pune

ABSTRACT

The digitalisation of armed conflict has generated one of the most complex normative crises in the history of international law. State-sponsored cyber operations from targeted disruptions of critical infrastructure to covert influence campaigns now define contemporary geopolitical competition. Yet the legal architecture governing armed conflict, anchored in treaties drafted for an industrial age, struggles to accommodate the distinct characteristics of cyberspace: anonymity, velocity, dual-use technology, and the absence of legible territorial boundaries. This article examines the capacity of International Humanitarian Law (IHL) to regulate cyber warfare, interrogating how foundational principles distinction, proportionality, precaution, and humanity translate into the digital domain.

It surveys the inadequacy of existing treaty instruments, the contested contributions of the Tallinn Manual 2.0, and the structural barriers to binding norm development. The article argues that while IHL principles are theoretically extendable to cyber operations, their practical application remains critically under-determined, exposing civilian populations to unacceptable risk. It concludes by advancing a reformist agenda centred on treaty codification, mandatory attribution mechanisms, and a dedicated cyber-IHL monitoring body.

Keywords: Cyber Warfare, International Humanitarian Law, Tallinn Manual, Distinction, Proportionality, Critical Infrastructure, Normative Gap, Cyber Operations, Armed Conflict, Treaty Reform

I. Introduction

On 27 June 2017, a software update distributed through a routine Ukrainian accounting package carried within it a hidden payload that detonated across networks spanning six continents. The NotPetya cyberattack attributed by multiple Western governments to Russia's GRU caused an estimated ten billion dollars in damage, paralysed global shipping conglomerate Maersk, disrupted pharmaceutical giant Merck, and crippled large segments of Ukraine's financial infrastructure. No soldier crossed a border. No missile was launched. And yet the consequences for civilian life were profound and enduring.

NotPetya is not an isolated incident but a symptom of a structural transformation in the conduct of hostilities one that challenges the foundational premise of the laws of war: that armed conflict can be identified, bounded, and governed. The question animating this article is whether the existing corpus of International Humanitarian Law (IHL), developed in a world of rifles, trenches, and aerial bombardment, possesses the normative resources to regulate a form of warfare that is invisible, instantaneous, and conducted almost entirely in the electromagnetic spectrum.

The stakes are exceptional. IHL's protective mandate encompasses civilian safety, the immunity of humanitarian personnel, the inviolability of medical facilities, and the preservation of the natural environment. If cyber operations circumvent these protections without triggering legal accountability, the humanitarian bargain embedded in centuries of treaty-making unravels. This article proceeds in six substantive parts: situating cyber warfare within the existing IHL architecture; examining how core principles apply or fail to apply to cyber operations; surveying soft-law contributions and their limits; identifying structural barriers to legal development; advancing a reformist agenda; and concluding with a call for urgent normative action.

It is important to clarify what this article does not claim. It does not argue that IHL is wholly inapplicable to cyberspace the weight of scholarly opinion and state practice, at least among Western states, supports the contrary position. Nor does it suggest that cyberspace is a legal vacuum in which all conduct is permissible. Rather, the contention is that the gap between IHL's formal applicability and its practical enforceability is so wide, and the mechanisms for closing it so underdeveloped, that the law's protective function is presently more symbolic than real a gap between the law on the books and the law in action that demands urgent diplomatic

and scholarly attention.

II. Cyber Warfare and the Architecture of IHL

2.1 The Governing Framework

International Humanitarian Law regulates the conduct of hostilities and seeks to limit their humanitarian consequences. Its principal instruments include the four Geneva Conventions of 1949 and their Additional Protocols of 1977, the Hague Regulations of 1907, and weaponsspecific conventions targeting landmines, cluster munitions, and chemical weapons. These instruments bind all parties to a conflict, irrespective of whether the conflict is international or non-international, and irrespective of the justice of the cause for which it is waged.

IHL was architected for a physical domain for the movement of troops, the discharge of projectiles, the visible destruction of property. Its triggering mechanism, the existence of an 'armed conflict,' was interpreted by the ICTY in Prosecutor v. Tadic as requiring 'a resort to armed force between States or protracted armed violence between governmental authorities and organised armed groups.' Whether and when cyber operations satisfy this threshold is among the most contested issues in contemporary international law.

2.2 The Attribution Crisis

At the heart of IHL's application to cyberspace lies the attribution problem. Unlike kinetic operations where the origin of a missile or the insignia of a soldier provides presumptive evidence of state agency cyber operations are engineered for deniability. Advanced persistent threats route traffic through multiple jurisdictions, repurpose commercial malware to obscure state authorship, and exploit compromised civilian infrastructure in third countries. Technical attribution, even when achieved with confidence by intelligence services, is rarely made publicly available in a form capable of sustaining legal accountability. If a state cannot be credibly identified as the author of a cyber operation, neither the law of state responsibility nor IHL's individual criminal accountability provisions can be meaningfully engaged creating a systemic enforcement vacuum that sophisticated actors exploit with deliberate intent.

2.3 The 'Armed Attack' Threshold

A further complication concerns the relationship between IHL and the jus ad bellum. Article

2(4) of the UN Charter prohibits the use of force against the territorial integrity of any state; Article 51 preserves a right of self-defence against armed attack. Whether a cyber operation constitutes a prohibited 'use of force' or a qualifying 'armed attack' turns on an effects-based analysis. The Tallinn Manual 2.0 adopts a consequences test, asking whether the effects of a cyber operation are comparable to those that would trigger the applicable rule if achieved by conventional means. This approach, while defensible in theory, generates significant uncertainty in real-time operational decision-making.

III. Core IHL Principles in the Cyber Domain

3.1 Distinction

Article 48 of Additional Protocol I requires parties to a conflict to distinguish at all times between civilians and combatants, and between civilian objects and military objectives. Attacks may be directed only against military objectives objects which by their nature, location, purpose, or use make an effective contribution to military action and whose destruction offers a definite military advantage.

In the cyber domain, distinction confronts an almost intractable obstacle: the dual-use character of digital infrastructure. The internet simultaneously serves civilian communication and military command-and-control. A power grid illuminates hospitals and supplies military bases alike. A financial network processes civilian banking transactions and defence ministry payments. An adversary seeking to degrade military capability through cyber means will almost inevitably affect civilian systems not as a regrettable side effect, but as a structural consequence of the internet's architecture. The distinction principle was forged in a world where military and civilian objects were, at least presumptively, separable. Cyberspace renders that presumption untenable.

> "The central challenge for distinction in cyberspace is not the absence of legal norms but the absence of separable targets. When the same fibreoptic cable serves a paediatric ward and a military command post, the principle of distinction offers guidance but cannot deliver protection."

3.2 Proportionality and Precaution

Article 51(5)(b) of Additional Protocol I prohibits attacks expected to cause incidental civilian

casualties that would be excessive relative to the concrete and direct military advantage anticipated. In cyberspace, this calculus is complicated by two structural factors. First, the cascading effects of a cyber operation its capacity to propagate across networks beyond the attacker's intentions are frequently unknowable at the moment of decision. Second, the standard of the 'reasonable military commander' presupposes forensic clarity about civilian exposure that the opacity of networked systems rarely affords.

The precautionary principle under Article 57 requires attackers to take all feasible precautions to minimise civilian harm. In the cyber context, precaution might entail sandbox testing of malicious code to map its propagation characteristics or the inclusion of geographic limiters in malware to constrain reach. Whether states conducting offensive cyber operations systematically undertake such analysis remains largely unknown, a consequence of the opacity surrounding offensive cyber programmes worldwide.

3.3 The Martens Clause

First articulated in the Hague Conventions of 1899 and given canonical expression in Article 1(2) of Additional Protocol I, the Martens Clause provides that in cases not covered by specific treaty provisions, civilians and combatants remain protected by customary international law, the principles of humanity, and the dictates of public conscience. In the cyber domain where treaty coverage is effectively nil, the Martens Clause assumes unusual significance: it is the provision that prevents the conclusion that, because cyberspace is unregulated by treaty, anything goes. Its practical operationalisation, however, remains deeply contested among international law scholars and state actors alike.

IV. Soft Law and the Tallinn Process

4.1 **The Tallinn Manual 2.0**

In the absence of binding treaty law, the most significant attempt to systematise IHL's application to cyberspace is the Tallinn Manual 2.0 (2017), produced under the auspices of NATO's Cooperative Cyber Defence Centre of Excellence. Authored by an international group of independent experts, its ninety-seven rules and commentary represent the most comprehensive scholarly codification of international law as applied to cyberspace. The Manual affirms that IHL applies to cyber operations conducted in the context of armed conflict;

extends the concept of 'attack' under IHL to cyber operations producing destructive effects even absent physical damage; extends protected status to civilian cyber infrastructure; and addresses the status of civilian hackers who participate directly in hostilities, concluding they may lose civilian protection under the rule of direct participation.

4.2 **The Limits of Soft Law**

The Tallinn Manual's limitations are as instructive as its contributions. It binds no state. Its rules reflect the perspectives of predominantly Western international lawyers. Major cyber powers — Russia, China, Iran, and North Korea have explicitly rejected the Manual's framework, characterising it as an instrument of normative hegemony. The UN Group of Governmental Experts (GGE) convened to develop responsible-state-behaviour norms for cyberspace has repeatedly failed to reach consensus, with the 2017 GGE collapsing without agreement on IHL's applicability to state cyber operations. This normative fragmentation reflects a deeper geopolitical contest: states that have developed asymmetric cyber capabilities as a strategic equaliser have strong incentives to resist the imposition of legal constraints that would erode that advantage, producing a two-track system in which Western states assert IHL's applicability while a significant bloc declines to accept it.

The successor Open-Ended Working Group (OEWG), established in 2019 to run parallel to the GGE process, has broadened participation but has not resolved the fundamental normative disagreements. Its outputs consensus documents affirming general principles of responsible state behaviour have remained deliberately vague on IHL application, reflecting the need to achieve agreement among states with diametrically opposed interests. The combined experience of the GGE and OEWG illustrates the central paradox of soft-law development in cyberspace: the flexibility that makes non-binding instruments achievable in the short term also limits their capacity to generate the stable, universal expectations of conduct that effective law requires.

V. Structural Barriers to Legal Development

5.1 The Verification Problem

International legal frameworks that regulate weapons such as the Chemical Weapons Convention and the Ottawa Treaty on landmines rely on verification systems, including

inspections, declaration requirements, and confidence-building measures.

Cyber weapons, however, do not lend themselves to similar verification methods. Unlike traditional weapons, cyber tools cannot be stored in warehouses or easily tracked using satellite imagery.A country's offensive cyber ability is based on factors such as talent, knowledge, and access to vulnerabilities, none of which can be realistically measured or inspected.Therefore, any future treaty on cyber-IHL must treat the verification challenge as a primary concern, not a secondary issue.

5.2 The Civilian-Military Nexus

Modern offensive cyber operations heavily depend on private sector involvement. Vulnerabilities that enable cyberattacks are often found, recorded, and sold by commercial security researchers, intelligence agencies, and private brokers. The infrastructure used for conducting these operations such as cloud services, content delivery networks, and internet exchange points is mostly owned by private entities. This extensive reliance on private actors creates significant challenges for IHL, which is primarily designed to apply to state parties and organized non-state armed groups. The roles of private technology companies such as developers of offensive tools, owners of systems that may be attacked, and potential participants in defensive actions have no clear equivalent in existing treaties.

5.3 Artificial Intelligence and Autonomous Cyber Systems

The use of artificial intelligence in offensive cyber operations intensifies these challenges. Machine learning systems can now detect network vulnerabilities, create new malware, and conduct social engineering campaigns at a speed and scale far beyond human capability. The use of autonomous cyber systems raises serious legal questions under IHL, including who is in charge, who is responsible for actions, how much human oversight is sufficient, and whether algorithms can follow the rules of distinction and proportionality. These are not just theoretical concerns. Many states are actively developing and deploying autonomous cyber tools, and there is still no clear legal framework to govern these activities.

Another often overlooked issue is the challenge posed by low-intensity cyber operations that do not meet the threshold of armed conflict but can still cause serious harm. Continuous attacks on critical infrastructure such as repeated probing of energy systems, ransomware attacks

targeting hospitals, and long-term espionage affecting personal data may not individually trigger IHL protections, but their cumulative effect on civilians can be substantial. IHL's binary approach which separates conflict from non-conflict is not well-suited for a domain marked by constant, low-level cyber activities. Addressing this gap may require the development of a more graduated system of cyber norms that applies across the entire spectrum from peace to war.

VI. Towards a Reformist Agenda

6.1 Treaty Codification

The most effective solution to the existing legal gap is the negotiation of a binding treaty.

Such a treaty does not need to cover all aspects of cyber activity, as that would be unrealistic. A more realistic goal is a focused convention that protects critical civilian infrastructure from cyberattacks, such as energy grids, water treatment systems, financial networks, healthcare facilities, and communications systems. Drawing from the examples of the 1925 Geneva Protocol and the 1972 Biological Weapons Convention, this treaty would establish clear prohibitions against cyberattacks targeting designated civilian objects and set up international verification and accountability mechanisms.

6.2 Mandatory Attribution Mechanisms

The lack of effective enforcement in cyber-IHL must be addressed through credible, independent attribution measures. Current practices, which rely on unilateral assessments by national intelligence agencies and diplomatic announcements, are not sufficient. They often produce classified, contested, and politically biased reports. An international body, similar to the Organization for the Prohibition of Chemical Weapons (OPCW), composed of state experts with appropriate security clearances, could provide a multilateral framework for attribution with greater legal and political credibility. This body could also develop standardized procedures for preserving evidence and documenting the chain of custody in cyber investigations which are essential for accountability.

6.3 A Dedicated Monitoring Body and Capacity Building

The specialized nature of cyber operations supports the creation of a standing international

institution tasked with monitoring compliance with cyber-IHL obligations, investigating violations, and offering interpretive guidance. Existing mechanisms of IHL such as the ICRC, protecting power system, and fact-finding commissions under Additional Protocol I are not well-suited for the cyber environment due to their design limitations. A new institution, with technical expertise, investigative powers, and links to the UN Security Council and the International Court of Justice, could provide the necessary infrastructure for an effective cyber-IHL system. At the same time, states must incorporate these obligations into military targeting procedures, rules of engagement, and command structures. Law schools and military academies should also develop dedicated curricula that address the application of IHL in the digital domain.

VII. Conclusion

The growing use of cyber warfare capabilities has introduced a form of conflict for which IHL was not designed and to which it does not easily apply. While the principles of distinction, proportionality, and precaution are theoretically applicable to cyber operations, these principles face significant structural challenges in the digital environment including dual-use infrastructure, uncertainty about cascading effects, and the difficulty of reliable attribution. These challenges reduce the effectiveness of IHL in practice. Soft-law instruments like the Tallinn Manual 2.0 have made valuable theoretical contributions but do not bind any state and have not led to a universal legal consensus.

The humanitarian consequences of this legal gap are very real. Cyber operations targeting energy infrastructure in Ukraine, disrupting hospital systems during conflict, and sabotaging water treatment facilities are examples of actions that, if carried out using traditional military means, would clearly trigger IHL obligations and potentially result in criminal liability. The fact that the same consequences, through cyber means, lead to legal uncertainty rather than accountability highlights a critical gap the international legal community must address urgently.

The reformist agenda proposed here including the codification of critical infrastructure protections in a treaty, establishing mandatory multilateral attribution mechanisms, creating a dedicated cyber-IHL monitoring body, and integrating IHL into military doctrine is ambitious yet achievable.

The history of IHL shows that humanitarian law has continuously evolved to meet new challenges.

REFERENCES

Treaty Instruments and International Documents

1.Geneva Convention (IV) Relative to the Protection of Civilian Persons in Time of War, 12 August 1949, 75 UNTS 287.

2.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.Charter of the United Nations, 26 June 1945, 1 UNTS XVI, Arts 2(4), 51.

4.Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on Their Destruction, 13 January 1993, 1974 UNTS 45.

Cases and Judicial Materials

5.Prosecutor v. Tadic (Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction) ICTY-94-1AR72 (2 October 1995) [70].

6.Case Concerning Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America) [1986] ICJ Rep 14.

7.Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226.

Books and Monographs

8.Michael N Schmitt (ed), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd edn, Cambridge University Press 2017).

9.Yoram Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict (3rd edn, Cambridge University Press 2016).

10. Marco Roscini, Cyber Operations and the Use of Force in International Law (Oxford University Press 2014).

11.Thomas Rid, Cyber War Will Not Take Place (Hurst & Company 2013).

12.Heather Harrison Dinniss, Cyber Warfare and the Laws of War (Cambridge University Press 2012).

Journal Articles and Reports

13.Michael N Schmitt, 'Cyber Operations and the Jus in Bello: Key Issues' (2011) 87 International Law Studies 89.

14.Gary Corn and Robert Taylor, 'Sovereignty in the Age of Cyber' (2017) 111 AJIL Unbound 207.

15.Oona Hathaway and others, 'The Law of Cyber-Attack' (2012) 100 California Law Review 817.

16.Jens David Ohlin, 'Did Russian Cyber Interference in the 2016 Election Violate International Law?' (2017) 95 Texas Law Review 1579.

17.ICRC, 'International Humanitarian Law and Cyber Operations During Armed Conflicts' (Position Paper, October 2019).

18.UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, Report (UN Doc A/68/98, 24 June 2013).

19.NATO Cooperative Cyber Defence Centre of Excellence, 'Cyber Definitions' (2021) <https://ccdcoe.org>.

20.Andy Greenberg, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' Wired (22 August 2018).