CYBER WARFARE AND INTERNATIONAL HUMANITARIAN LAW: LEGAL AND POLICY REFORM PROPOSALS FOR SRI LANKA

Zahara Rajabdeen[1]

1. Introduction

In the twenty-first century, cyber operations have transformed the nature of conflict, allowing states and non-state actors to disrupt digital infrastructure, interfere with essential services and target civilian population. The International Committee of the Red Cross (ICRC) has repeatedly emphasized the growing humanitarian risks associated with cyber operations.[2] While technologically advanced states have started to adopt new legal, institutional and military frameworks to address challenges of cyber conflict, many developing countries remain unprepared. Sri Lanka is one such nation that is increasingly reliant on digital infrastructure, yet lacks the legal mechanisms required to regulate cyber warfare. Although Sri Lanka has enacted cybercrime legislation and established institutional mechanisms, these frameworks talk about cybercrimes as criminal acts, not cyber warfare. This regulatory gap is a growing threat to Sri Lanka's civilian population, critical infrastructure, and national security system. This article addresses the central problem of the absence of a legal and policy framework in Sri Lanka to regulate cyber warfare or ensure compliance with International Humanitarian Law in the cyber domain. While most research on cyber warfare focuses on international armed conflicts, this article adopts a broader approach by examining the applicability of International Humanitarian Law to cyber operations in both international and non-international armed conflicts, including situations involving non-state armed groups. It argues that Sri Lanka

[1] The author is a 2nd year undergraduate, pursuing an LL.B at the Department of Law, University of Jaffna. The author extends sincere gratitude to Yanitra Kumaraguru (an independent researcher and expert on cyber warfare and International Humanitarian Law, who was previously a lecturer at Faculty of law, University of Colombo) for her invaluable guidance and mentorship throughout the presentation of this research paper.

[2] ICRC, *International humanitarian law and cyber operations during armed conflicts* (Geneva: ICRC, 2019) <https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-armed-conflicts?utm.com> accessed date: 03rd December 2025.

needs specific legal reforms to deal with cyber warfare while respecting humanitarian principles.

2. Conceptual Background: Cybercrime, Cyber-Attacks, Cyber Warfare

Clear conceptual distinctions are important because domestic law, international criminal law and IHL each regulate different categories of cyber activities.

2.1. *Cybercrime*

There is no universally accepted definition, but it is commonly understood as offences committed using computer systems, including unauthorized access, data theft, ransomware, and online fraud[3]. This understanding is reflected in international instruments such as the Budapest Convention, which focuses on the confidentiality, integrity, and availability of computer data systems. Cybercrime is ordinarily not considered an armed conflict and does not fall under IHL.

2.2. *Cyber-Attacks*

A cyber-attack refers to malicious activity targeting networks, systems, or data, aiming to disrupt, corrupt, or steal. Cyber-attacks may occur during peacetime or wartime.[4] However, not all attacks constitute "cyber warfare". Whether a cyber-attack falls under IHL depends on the context, effects, and the nature of the operation.

2.3. *Cyberwarfare*

There is no single, universally accepted definition of cyber warfare, but the Tallinn Manual, a non-binding document on the international law applicable to cyber operations, interprets cyber warfare as an operation conducted as part of or during an armed conflict. When such operations cause physical destruction, death, injury, or disable critical infrastructure and occur in conflict, they may qualify as "attack" under IHL.[5]

---

[3] Convention on Cybercrime, opened for signature in Budapest, 23 November 2001, ETS No. 185 (entered into force 1 July 2004).

[4] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2017).

[5] Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (CUP 2017).

3. Cyber Warfare: Nature and Humanitarian Impact

Cyber warfare is unlike traditional war, which operates in an invisible, borderless, and highly interconnected environment. Its tools include malware, logic bombs, ransomware, distributed denial-of-service (DDoS) attacks, supply-chain compromise, and manipulation of industrial control systems.[6] One defining feature of cyber warfare is its non-physical mode of attack. Cyber operations can cause disruption without firing a single bullet: disabling power grids, shutting down hospitals, altering bank data, or manipulating the transport network.

Another feature is the difficulty of attribution. Cyber operations may occur across multiple jurisdictions, via proxy servers, or by non-state hacker groups. This anonymity enables states to conduct hostile operations below the threshold of armed conflict, creating legal and strategic uncertainty. Cyber warfare is also characterized by the blurring of civilian-military boundaries. Military and civilian digital systems share the same infrastructure, such as undersea cables, satellites, or cloud platforms; therefore, an attack on a military target can easily spill into civilian networks. For countries like Sri Lanka, where digital infrastructure is developing and highly interconnected, such spillover could have severe humanitarian consequences.

4. Humanitarian Impact of Cyber Operation

The humanitarian consequences of cyber warfare can be as severe as traditional war, even without violence. Real-world cyber operations illustrate that cyber warfare is not a theoretical concern but capable of causing large-scale humanitarian, economic and security consequences. Three major incidents, Stuxnet, the Ukraine power-grid attacks, and NotPetya, demonstrate how cyber operations can disrupt essential services, undermine civilian well-being and blur the line between peacetime cyber operations and wartime cyber operations. *Stuxnet (2010)*[7] is the first cyber operation to cause physical destruction. Stuxnet targeted Iran's Natanz nuclear facility by manipulating industrial control systems and causing physical damage to approximately 1000

[6] Nicolas Tsagourias, *International Law and Cyber Warfare: The Legal Regulation of Computer Network Attacks* (Routledge 2012).

[7] Kim Zetter, *Countdown to Zero Day* (Crown 2014) 215.

centrifuges. Although some scholars classify Stuxnet as an example of cyber warfare, others argue that it did not constitute an internationally recognized armed conflict and therefore may fall outside IHL. Regardless of this debate, Stuxnet illustrates how cyber operations can produce destructive conflict. Another is the attack on *Ukraine Power-Grid Attacks (2015-2016)*[8]*;* this case is a real example of a cyber operation**.** In 2015, a coordinated cyber operation disrupted electricity to over 225,000 civilians in Ukraine. A second attack in 2016 used malware designed specially target power-grid systems. This incident demonstrates how a cyber operation can disable essential infrastructure, as electricity blackouts directly endanger hospitals, heating and communications. Under IHL, civilian objects are generally protected from attack by the principle of distinction, and objects indispensable to the survival of the civilian population are protected, making the threshold for lawful attack particularly strict. *NotPetya (2017)*, initially aimed at Ukraine via a compromised software update, became one of the most destructive cyber operations in history. Within hours, it spread globally, impacting companies such as Maersk, Merck, FedEx and critical logistics providers. The total economic damage exceeded USD 10 billion.[9] This causes humanitarian impacts, disruption of medical and pharmaceutical production supply-chain services, and paralysis of global shipping ports. Many experts debated whether NotPetya qualifies as a cyber-attack under IHL, because it did not occur within a defined armed conflict and primarily caused economic damage.[10] Despite this ambiguity, NotPetya is invaluable for analysis because it demonstrates how cyber operations can unintentionally escalate, cross borders, and disrupt essential civilian services, showing why states like Sri Lanka must prepare legal mechanisms even for ambiguous or "grey zone" cyber incidents.

These cases show the complex and evolving nature of cyber operations. Some incidents, such as the Ukraine case, clearly fall under IHL, while others are debated. Nevertheless, all examples show that cyber

[8] Robert Lee, *Michael Assante and Tim Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid* (2016) 3.

[9] Andy Greenberg, *Sandworm* (Doubleday 2019) 120.

[10] Jack Goldsmith, 'The NotPetya Attacks and International Law' (2017) *Lawfare.*

operations can cause severe humanitarian, economic, and social consequences, highlighting that Sri Lanka's legal and policymaking must address both peacetime and wartime cyber operations, including clear and ambiguous forms of cyber harm.

5. International Humanitarian Law and its Applicability to Cyber Warfare

International Humanitarian Law applies to all forms of warfare and all kinds of weapons, including those of the future.[11] This principle, affirmed by the International Court of Justice (ICJ), means that cyber operations conducted during an armed conflict must comply with IHL. The ICRC similarly emphasizes that IHL applies regardless of the means or methods of warfare.[12]

Although more discussion on cyber warfare focuses on international armed conflict, cyber operations may also arise in non-international armed conflicts involving non-state armed groups. In such contexts, IHL continues to apply through common Article 3 of the Geneva Conventions and, where applicable, Additional Protocol II.[13] Though the legal rules for non-international conflicts are less detailed than for wars between countries, the main protections remain the same, especially the ban on attacking civilians and objects. Therefore, Sri Lanka's national laws on cyber war should be strong enough to handle cyber operations carried out by both state and non-state actors during any type of conflict.

Therefore, cyber operations must comply with the core IHL principles:

i. Distinction: cyber operation must distinguish between civilian objects and military objectives.[14]

---

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

[12] L. Gisel, T. Rodenhauser, and K. Dormann, 'Twenty years on: International humanitarian law and the protection of civilians against the effects of cyber operations during armed conflicts' *International Review of the Red Cross* (2020) 1–48.

[13] Additional Protocol II to the Geneva Conventions of 12 August 1949, 'Protocol Additional to the Geneva Conventions and relating to the Protection of Victims of Non-International Armed Conflicts' (1977). <https://legal.un.org/avl/ha/pagc/pagc.html?utm_com> accessed date 03rd December 2025.

[14] Additional Protocol I to the Geneva Conventions (1977) art 48.

ii. Proportionality: incidental civilian harm must not be excessive in relation to anticipated military advantage.[15]
iii. Humanity: operation must not cause unnecessary suffering or superfluous injury.[16]

6. Challenges in Applying IHL to Cyber operation

Applying IHL to cyber operations poses significant challenges, as civilian and military networks are interconnected; therefore, an attack on a military system may spill over into civilian infrastructure, and a cyber operation may cause physical destruction, such as disabling hospital IT systems. Attribution remains technically complicated, especially when the proxy groups or anonymous networks are used. Many cyber operations fall below the threshold of kinetic violence, yet still produce humanitarian consequences.

These challenges demonstrate that, although IHL applies to cyber operations in theory, its application in practice remains complex and inadequate. Cyber warfare can cause humanitarian harm comparable to traditional warfare, yet current frameworks struggle to regulate attribution, proportionality assessments, and the blurred civilian-military boundaries in cyberspace.

7. Sri Lanka's Legal and Policy Framework: Gaps and Limitations

*Computer Crimes Act (2007)***:** The Act criminalizes unauthorized access, data theft, interference with systems, and related offences.[17] However, it does not regulate state military cyber operations, impose IHL obligations, or address attacks on civilian infrastructure.

[15] Ibid, art 51(5)(b).
[16] Ibid, arts 35–57.
[17] Computer Crime Act No. 24 of 2007 <https://www.icta.lk/ictaassets/uploads/2016/03/ComputerCrimesActNo24of2007.pdf> accessed date: 03rd December 2025.

Sri Lanka CERT|CC[18]**:** CERT provides incident response and cybersecurity coordination but has no mandate regarding cyber operations occurring in armed conflict.

National Cyber Security Strategy (2019-2023): The Strategy emphasizes critical infrastructure protection and cybersecurity governance but does not regulate cyber warfare, attribution, or IHL compliance.[19]

Budapest Convention[20]: The Convention is relevant to Sri Lanka because it is a States Party and has aligned its domestic cybercrime legislation, particularly the Computer Crimes Act, with the Convention's framework. As a result, the Convention forms part of Sri Lanka's broader cyber governance architecture and shapes how the state understands and regulates cyber activities. But the Convention is limited to criminal cooperation and law enforcement and does not address state responsibility, military cyber operation or application of IHL during armed conflict, thereby exposing a significant gap.

Therefore, existing law demonstrates that Sri Lanka is not institutionally or legally empowered to respond to a cyber operation that may occur during armed conflict. This gap makes Sri Lanka vulnerable not only to cyber threats but also to humanitarian, economic, and national security risks. Moreover, global experience shows that cyber operations do not remain confined to borders and may spill over into civilian systems even when the original target is military. Without a legal mechanism to regulate state behaviour, ensure oversight, or protect essential services, Sri Lanka is facing severe disruption like the incidents witnessed in other countries. So, comprehensive legal reform is essential for national security and humanitarian protection.

8. Comparative State Practice

Examples from other countries show that it is possible and practical to create domestic laws that regulate cyber operations, and many states are

[18] Sri Lanka CERT|CC, *Annual Report* (2022).
[19] ICTA, *National Cyber Security Strategy 2019–2023* (Government of Sri Lanka 2019).
[20] Budapest Convention.

already doing so. For instance, Estonia,[21] one of the world's most digitally advanced countries, has included cyber operations in its national security and defense policies while giving strong importance to protecting civilian infrastructure. Similarly, both the United Kingdom[22] and the United States treat cyber operations as part of their military activities. They have made it clear through military manuals and operational doctrines that such activities must comply with the Law of Armed Conflict; the same rules apply to traditional warfare. Even though these countries do not yet have a specific Cyber Warfare Act, their examples show that cyber warfare can still be effectively regulated through national laws that include International Humanitarian Law principles. These examples support the argument that Sri Lanka can create its own special legislation to control cyber warfare, ensuring both national security and respect for humanitarian law.

9. Recommendation

Sri Lanka should enact a Cyber Warfare Act; such legislation should clearly define key concepts, including cyber operation, cyber warfare, critical infrastructure, and military cyber capability. Thereby distinguishing cyber warfare from cybercrime and ordinary cybersecurity incidents. A clear definition is important to prevent the inappropriate application of criminal law frameworks to military or national security cyber operations. To effectively incorporate IHL into domestic cyber regulation, the proposed Cyber Warfare Act should codify the IHL principle as a binding legal obligation on state cyber operations. The Act should require that any cyber operation conducted by state authorities during armed conflict, whether international or non-international, comply with the principles of distinction, proportionality, military necessity, and protection of civilians. For

[21]<https://en.wikipedia.org/wiki/Cyber_Command_%28Estonia%29?utm.com#External_links> accessed date 08th January 2026.

[22] Foreign, Commonwealth & Development Office and Ministry of Defence, *Voluntary Report on the Implementation of International Humanitarian Law at Domestic Level* (*Second Edition)* (UK Government, 1 October 2024, last updated 23 October 2024) <https://www.gov.uk/government/publications/implementation-of-international-humanitarian-law-at-domestic-level-2024-voluntaryreport/voluntary-report-on-the-implementation-of-international-humanitarian-law-at-domestic-level-second-edition?utm.com> accessed date: 08th January 2026.

example, cyber operations directed at military objectives should be prohibited where they foreseeably disrupt civilian infrastructure such as hospitals, electricity grids, water systems, or telecommunications networks.

Incorporating IHL into domestic cyber regulation would also strengthen accountability mechanisms. The proposed legislation should impose command responsibility for illegal cyber operations that cause civilian harm, clarify the chain of authority for cyber command, and provide for parliamentary or judicial oversight of offensive cyber capability. This approach helps Sri Lanka follow international standards in managing cyber activities.

Moreover, Sri Lanka would also benefit from establishing a National Cyber Command responsible for coordinating military, intelligence, and civilian cyber responses. Now, responsibilities are fragmented across the Sri Lanka CERT|CC, the Ministry of Defense, and the Information and Communication Technology Agency. A centralized command structure would enhance real-time threat detection, improve inter-agency communication, and ensure responses to hostile cyber operations are rapid, coordinated, and legally regulated. This body should also be responsible for developing national cyber defense doctrines that reflect IHL obligations and define operational limits for cyber activities during conflict.

Finally, Sri Lanka should expand international cooperation in cybersecurity and cyber defense. Cyber warfare is inherently transnational, and many states—particularly developing nations struggle to respond independently. Participation in regional cyber defense networks, information-sharing partnerships, and capacity-building programs in the Asia-Pacific region would enhance Sri Lanka's defensive readiness. Engaging more actively with organizations such as the ICRC, INTERPOL, and UN cybercrime and cybersecurity platforms would ensure that Sri Lanka's domestic reforms reflect evolving global standards. International cooperation also helps develop expertise, technology transfer, and best practices essential for addressing cyber threats that transcend borders.

10. Conclusion

As Sri Lanka becomes increasingly digitized, the absence of a clear legal and institutional framework exposes the country to significant humanitarian and strategic risks. Existing cybercrime and cybersecurity measures are insufficient to address cyber operations during armed conflict. Strengthening national law through a Cyber Warfare Act and improving oversight are important steps to ensure that Sri Lanka is prepared for future cyber threats and aligned with international humanitarian obligations.