Battlefields in Cyberspace: Cyberwarfare and International Humanitarian Law

Battlefields were solely advocated by the traditional army in the traditional warfare or armed conflict. With the evolution in the domains of warfare, the dimensions of warfare have also evolved. This acts as an ambit for numerous forms of warfare. However, the very point of distinction between these is that of the mode and the approach led by the evolving technology. This ambit does not fail to include cyberwarfare. In the 21st Century, it should not be difficult to understand the impact and the possibility of cyberwarfare in armed conflict, and the major concern it poses to the adherence of the same to the Laws of Armed Conflict (LoAC), following the rules of war, the cardinal principles, and the protection of civilian population. The major issue that cyberwarfare brings forth is the inability to track tangible form of battlefield or source to impose the rules and guidelines, or the LoAC. As the military and the civilian population share the common cyberspace, it often becomes a challenge to discriminate between the civilian and military objects. This article focuses on understanding cyberwarfare, its intersection with International Humanitarian Law (IHL), and how it affects the civilian population, its adherence to the IHL, and the cardinal principles.

Introduction

In late 2023, Yigal Unna, Israel's head of cyber defence, expressed worries about Iran intensifying its assaults on Israeli government and infrastructure. This is a prime example of the modern world in which cyberwarfare has emerged as a crucial area in addition to land, air, and sea tactics in armed engagements worldwide. Determining what constitutes war is imperative in the 21st Century. One could argue that war and its tools have changed from their physical origins, with each domain employing methods essentially distinct from one another. The only way to derive some commonality would be to use technology to take advantage of its features. This clearly includes using military tactics to wage a war.

The Cambridge dictionary defines cyber warfare as, “The activity of using the internet to attack a country’s computers in order to damage things such as communication and transport systems or water and electricity supplies”.[1]

Cyberwarfare is used to describe cyber acts that compromise and disrupt critical infrastructure systems, which amount to an armed attack which intentionally causes destructive effects (i.e., death and/or physical injury to living beings and/or destruction of property). Only governments, organs of the state, or state-directed or state-sponsored individuals or groups can engage in cyberwarfare.[2] Concern over cybersecurity began to grow in the 20th Century leading to the progression of cyberwarfare. Organisations handling these emerging cyber threats were established as a result of notable events like the Morris Worm in 1988. Military interest in protecting against cyberattacks surged in the early 1990s with the internet’s growth.[3]

Western nations including the United States (US), Russia, and China, have shifted their attention over the last 20 years from a passive defence to active engagement. This shift accelerated post-11 Sep 2001, leading to the creation of military cyber units such as the US Cyber Command, focusing on both offensive and defence cyber activities. This does not, however, end the discussion about the applicability of International Humanitarian Law (IHL) to cyberwarfare. Since the discovery of the new physical domains, the tools of battle have changed. The rules governing these conflicts, whether in space or beyond, are established by the customary IHL, often known as the laws of armed conflict.

IHL aims to protect individuals not participating in hostilities, particularly civilians, by regulating the conduct of armed conflicts. It focuses on restricting the impact of conflict on military targets through adherence to three cardinal principles: distinction, proportionality, and precautions. As cyber activities in conflicts become more prevalent, the question arises whether IHL adequately regulates these emerging forms of warfare. IHL's principles apply to cyber operations, requiring parties to distinguish between military objectives and civilian infrastructure. Protecting civilians is a key requirement of these principles, which becomes challenging during cyberwarfare. IHL applies to all military operations, cyber or kinetic, but only covers cyber actions within an armed conflict's context. Cyberwarfare concerns all states due to the interconnected nature of cyberattacks, which can impact multiple states, intentionally or not. To apply IHL to cyberconflicts, it is essential to determine whether cyberattacks constitute military force. Article 2, common to all Geneva treaties, states that “(This treaty) shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognised by one of them”.

The Tallinn Manual, created in 2013 by the North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence, is the first set of cyberwarfare guidelines. It consists of 95 rules across two sections:

- **International law pertaining to cyber security.** The right to self-defence in cyberspace and the exercise of national cyber sovereignty.
- **Internet law of armed conflict.** The rules that must be followed in armed conflict for certain individuals, occupations, neutral nations, etc.

The 2017 Tallinn Manual 2.0 addresses recurring cyber incidents outside military conflicts, focusing on peacetime international law. Its rules serve as customary international law, offering detailed guidance. The manual emphasises the state's right and duty to counter terrorism's adverse effects on human rights, playing a crucial role in cyberwarfare, cyberattacks, and cyber defence at national, regional, and international levels.

Protection during Cyberwarfare

One of the IHL's primary goals is the protection of people. There is ‘General protection against dangers arising from military operations’ for both the civilian population and individual civilians. Additional Protocol I (AP I) states that anyone under the authority of a ‘Party’ to the conflict who does not benefit from preferential treatment under the conventions or the protocol must always be treated humanely and must, at the very least, receive the protections of this article without facing any discrimination. Furthermore, the legislation stipulates that individuals who are protected are entitled to protection of their personhood, honour, family rights, religious beliefs and practices, and manners and customs under all situations. The protection of civilians during hostilities is based on the core IHL concepts of distinction, proportionality, and precautions.

The Principle of Distinction

“The ‘Parties’ to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives”, states Article 48 of the AP I, which lays out the principle of distinction. Similarly, the International Court of Justice defined this principle as a “Cardinal principle contained in the texts constituting the fabric of humanitarian law” in its Advisory Opinion on nuclear weapons. A strict reading of Article 48 permits strikes only against military targets. In cyberspace, strikes on civilian infrastructures would violate Article 48, while cyberattacks targeting military facilities for a ‘Definite military advantage’ are considered lawful. The dual-use nature of cyberspace blurs the boundary between military and civilian infrastructure, making target identification challenging. The principle of differentiation mandates that parties refrain from actions causing significant collateral harm and limit strikes to military targets. Additionally, AP I forbids attacks depriving civilians of necessities like food or water. As both military and civilian actors often use the same targets, applying the principle of distinction in cyberspace is challenging. Differentiating between military and civilian cyber systems is essential, as mandated by AP I, Article 58, which requires separating “Civilian objects from the vicinity of military objectives”. States must strive to distinguish military and civilian cyber systems, as this is the best method for ensuring lawful targeting in cyberwarfare.

The Principle of Proportionality

One of the most contentious IHL principles is proportionality, which acknowledges that civilian casualties or destruction of civilian property are inevitable during times of war. However, compared to cyber operations, the proportionality principle is simpler to apply in traditional kinetic combat. The idea of proportionality is crucial for safeguarding civilians and civilian assets in the cyber realm because most cyber infrastructures are dual-use.

Article 51(5)(b) of the AP I defines the proportionality principle, which is consistent with customary international law and applies to both international armed conflicts and non-international armed conflicts. Attacks that “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” are forbidden by Article 51(5)(b).

Two key components of the proportionality principle—the ‘Damage to civilian objects’ level in Article 51(5)(b) and the problem of indirect effects—deserve a more thorough interpretation and strategy for cyber operations that apply it. A cyberattack that successfully prevents information from being transmitted over the internet could have more serious repercussions than just bothering the public. As a result, cyberattacks have the potential to alter the relative importance of short-term repercussions and to make authorities face greater uncertainty than usual when deciding whether planned attacks are acceptable. However, military commanders have to make a distinction between the civilian population and legitimate military targets.

The Principle of Precaution

Within the framework of *jus in bello* (laws of war), the principle of precaution mandates that parties to a conflict—in this case, cyberwarfare—take steps to reduce the harm to civilians and civilian infrastructure. Reducing the possible humanitarian impact of military actions is the goal of this principle. By doing a thorough risk assessment and accounting for the possible risks and repercussions of their cyberattacks, the precautionary principle can be upheld in the context of cyberwarfare. This entails assessing the possibility of harm to non-combatants, interruption of vital services, and collateral damage to civilian infrastructure.

According to the proportionality principle, parties must also balance the possible harm to civilians and civilian infrastructure against the expected military advantage in their defence against an enemy attack. In other words, any possible collateral damage must be outweighed by the anticipated advantages of a cyber operation.

The Stuxnet Virus: A New Dawn in Cyber Operations

The Stuxnet virus is a prime example of the strategic use of digital tools to accomplish military goals and marks a turning point in cyberwarfare.[4] Stuxnet, which was created by Israeli and American intelligence services, was intended to interfere with Iran's nuclear enrichment capability by attacking the centrifuges' programmable logic controllers at the Natanz site. Stuxnet successfully caused physical harm without direct kinetic action by controlling the operation of these delicate machinery and providing operators with erroneous data.[5] This operation demonstrated how cyber tools can be used to achieve goals that would have otherwise required military action. However, its effects bring up important issues of collateral damage and sovereign

rights, especially when considering the consequences of using such technologies against countries that are considered unfriendly.

Stuxnet's effects go beyond its immediate technological implications; it calls into question established theories of war and national sovereignty. States may violate international rules governing activities against other countries by using cyber capabilities to further their strategic objectives. The risks involved in cyber operations are highlighted by the collateral damage caused by the virus, which unintentionally spread to systems all around the world. The inadvertent effects on non-targeted nations highlight the necessity of laws that control the use of such advanced viruses and guarantee responsibility for any resulting harm.[6]

Cyber Operations in the Russia-Ukraine Conflict: Geopolitical Ramifications

The continuing crisis between Russia and Ukraine has brought even more attention to how cyberwarfare and geopolitical conflicts are intertwined. Both state and non-state entities used cyber operations to accomplish strategic objectives during the conflict, frequently at the price of vital services and civilian populations. Widespread interruptions brought on by cyberattacks intended to destroy Ukraine's government and energy infrastructure have made the humanitarian catastrophe worse.[7]

These cyberattacks have impacted civilian infrastructure in addition to military targets, which has led to serious worries about the consequences for civilian safety and human rights. Significant collateral damage has resulted from cyberattacks that compromise vital infrastructure, which can impair vital services like emergency response systems, water supply, and energy, thereby affecting residents' quality of life. The debate over the morality and legality of cyberwarfare is made more difficult by the disregard for established IHL norms in these circumstances.[8]

Conclusion

Concerning the applicability of IHL for the protection of people, the emergence of cyberwarfare has created serious difficulties. Cyberattacks are not simply a radically different approach to combat, but they also occur at a time when the rules of armed conflict are being challenged by rising asymmetry, technological advancement, and more civilian involvement in conflicts than ever before. The special traits and complexity of cyberwarfare were not first addressed by the broad norms and principles of IHL.

The lack of measures in IHL to secure data and information in cyberspace is a serious issue that this research has raised. It is crucial to acknowledge cyberspace as unique and create laws that fully address its complexities in order to protect citizens from cyber threats. The protection afforded to tangible civilian data should be expanded by this law to cover data, information, and vital cyber infrastructure. To further guarantee adherence to IHL, a comprehensive legal analysis of cyber weapons, cyberwarfare means, and cyberwarfare techniques should be carried out.

Endnotes

[1] Cambridge Dictionary, “Cyber-Warfare”, Accessed 15 Jan 2025, https://dictionary.cambridge.org/dictionary/english/cyber-warfare

[2] United Nations Office on Drugs and Crime, "Cyberwarfare", *Education for Justice (E4J) Initiative,* Accessed 15 Jan 2025), https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html

[3] Allied Market Research, "The Evolution and Impact of Cyberwarfare: Understanding the Digital Battlefield". *Allied Market Research*, Accessed 13 Jan 2025, https://www.alliedmarketresearch.com/resource-center/trends-and-outlook/information-and-communication-technology-and-media/the-evolution-and-impact-of-cyberwarfare-understanding-the-digital-battlefield

[4] Kaspersky, "What Is Stuxnet?", *Kaspersky Resource Center*, Accessed 13 Jan 2025, https://www.kaspersky.com/resource-center/definitions/what-is-stuxnet

[5] Krebs, Brian, "Stuxnet Explained: The First Known Cyberweapon". *CSO Online*, 23 Sep 2010, Accessed 10 Jan, 2025, https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known-cyberweapon.html

[6] Ibid, 4

[7] Stanford University Freeman Spogli Institute for International Studies, "Russian Cyber Operations Against Ukrainian Critical Infrastructure", *Stanford Internet Observatory* (SIPR), Accessed 17 Jan 2025, https://fsi.stanford.edu/sipr/russian-cyber-operations-against-ukrainian-critical-infrastructure

[8] International Committee of the Red Cross, "Cyber Warfare and International Humanitarian Law", *International Committee of the Red Cross*, Accessed 12 Jan 2025, https://www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law