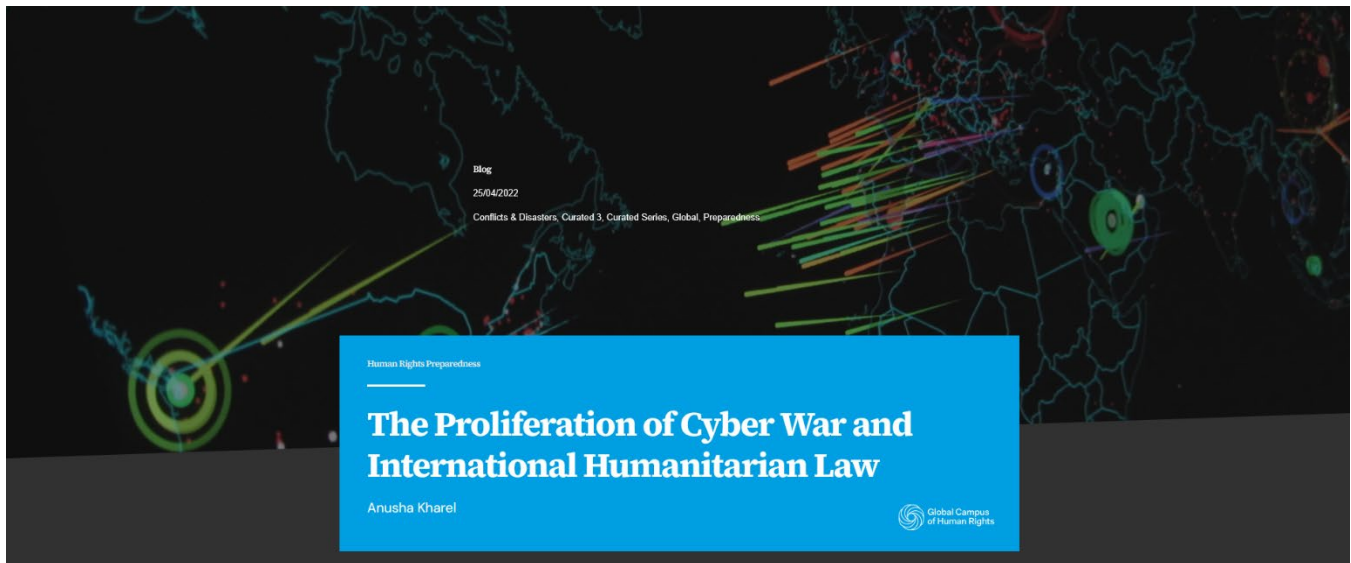




The Proliferation of Cyber War and International Humanitarian Law

Anusha Kharel*

Abstract: The extraordinary growth of cyberspace has created new possibilities and threats in warfare. It has become crucial to identify a common understanding of cyber warfare if we are to effectively protect civilians from the direct and intentional effects of cyber operations.

The concept of warfare is everchanging in the international game of power. From sword battles in the past to drone attacks today, we have seen the international game of power driven to shift and evolve by [technology](#). The 'space' of battle has expanded too. In particular, the [extraordinary growth](#) of cyberspace has created new possibilities and threats.

Cyberwarfare does not have a clear definition, however it is widely understood as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with a proportional kinetic [use of force](#). It may include a range of activities using information and communication technology to cause social, ideological,

* Anusha Kharel is an Advocate and a Teaching Assistant at Kathmandu School of Law. Her areas of interest are human rights law, public international law and international relations. She is a graduate of Kathmandu School of Law.

religious or political harm. Cyber operations can result in serious consequences in an armed conflict as their effect is not limited to the targeted system. For example, air traffic control systems, nuclear plants and other such systems operated through technology can be manipulated, with enormous impact on the lives of civilians. We can see the [WannaCry Ransomware Attack](#) in 2017 as an example. It affected thousands of civilian infrastructures, including hospitals and transport services, in over [100 countries](#).

Cyberwarfare and international humanitarian law

International Humanitarian Law (IHL) is the body of law that seeks for humanitarian reasons to limit the means and [methods of warfare](#). IHL seeks to protect those who are not or are no longer involved in hostilities from the effects of an armed conflict. The Hague Convention of [1899](#) and [1907](#), the four Geneva Conventions of 1949, i.e., [Geneva Convention I](#), [Geneva Convention II](#), [Geneva Convention III](#), [Geneva Convention IV](#), and their Additional Protocols [I](#), [II](#) and [III](#), are the main sources of IHL that are applicable in an International Armed Conflict (IAC). IHL was drafted with traditional kinetic warfare in mind, thus its application in cyberwarfare needs to be critically analysed.

The first question that arises is: can cyber war be considered an armed conflict? It is clear that IHL applies to the situation of armed conflict. However, what amounts to an 'armed conflict' has not been defined in any of the IHL treaties, which means we need to look through [jurisprudential lens](#) to answer the question about the status of cyber warfare. [Jean S. Pictet](#), a prominent figure who contributed to the development of IHL, inter alia, commented that under the Geneva Conventions:

any difference arising between two states and leading to the intervention of armed forces is an armed conflict within the meaning of Article 2. (see [Geneva Convention I](#), [Geneva Convention II](#), [Geneva Convention III](#), [Geneva Convention IV](#))

Pictet emphasised that the first shot theory onto opposing forces is sufficient to trigger an [IAC](#). The International Criminal Tribunal on Former Yugoslavia (ICTY) also adopted Pictet's view in the [Tadic Case](#). Further, the IHL treaties anticipate of development of new means and methods of warfare. Thus, it can be argued that IHL principles and rules apply to new means and methods of warfare, including the cyber system. If the IHL principles and rules were not to apply to new means and methods, it would not have been necessary for the states to examine their legality as required by Article 36 of the 1977 Additional Protocol I. Furthermore, the [ICJ's Advisory Opinion](#) on Legality of the Threat or Use of Nuclear Weapons also endorses that IHL principles are applicable to 'all forms of warfare and all kinds on weapons' in an armed conflict, including 'those of future'.

Therefore, it can be argued that cyberwarfare falls within the scope of definition of 'armed conflict' and thus, IHL is applicable. Besides, a group of experts have prepared a non-binding document, the [Tallin Manual](#), which states that IHL applies to cyber warfare. It has

contributed to opening the discussion among states about the challenging issues concerning cyberwarfare. However, whether the traditional rules laid down by the IHL are sufficient for the protection of the civilians is yet to be seen.

Importance of IHL in cyberwarfare

The rules and principles of IHL address a number of issues during an armed conflict. Among others, the principles of humanity, military necessity, distinction, proportionality and precaution are very much relevant during a cyberwar. These principles are designed to limit the act of hostilities and prevent civilians from direct and excessive incidental harm. Additional Protocol I outlines that the parties to the conflict at all times should distinguish between civilians and combatants, between civilian objects (such as a house or other dwelling or a school) and military objectives (such as military weapons, vehicles, equipment, installations). The principle of distinction has also been recognised as a 'cardinal principle constituting the fabric of humanitarian law' in the [ICJ's Advisory Opinion](#) on Legality of the Threat or Use of Nuclear Weapons. Applying this principle, in any cyberwarfare, attacks should only be targeted at military objectives. Any attacks on civilian objects would constitute a breach of Article 48 of the Additional Protocol I. However, the protection falls short for several reasons, including: (1) the [specific distinction](#) of civilian and military objects is unclear, particularly in respect of data and functionality of cyber systems, and there is [disagreement](#) as to whether civilian data enjoy the same protection as civilian objects; (2) calculation of damage to civil property in a cyber warfare is vague; and (3) there is a [lack of guidance](#) as regards indirect effects to be accounted. When we talk about protecting civilians and civilian objects in the cyber domain, the principle of proportionality is paramount as cyber infrastructures have the nature of [dual-use](#). Unlike traditional kinetic warfare, settling proportionality in a cyber warfare is contentious. There is one cyberspace which is shared by the military and the civilians and is interconnected. It is unclear and vague what constitutes damage to the civilian property and the calculation of damage, and thus application of this principle is challenging in cyber warfare. Therefore, the damage to civilian objects and anticipated indirect effects must be factored into the [proportionality assessment](#), while planning and execution of a cyber-attack.

Way forward

Cyber operations have become a reality in armed conflicts. Thus, it has become crucial to identify a common understanding of cyber warfare if we are effectively to protect civilians from the direct and intentional effects of cyber operations. For this, states need to acknowledge that IHL applies to cyber warfare and engage in discussions and deliberations on how to apply IHL and determine whether the challenges posed by such cyber operations during an armed conflict are sufficiently addressed by the existing rules and principles of IHL.

In the absence of a binding instrument specifically dealing with cyber warfare, the complexities and challenges of cyber operations during armed conflict have not been effectively addressed. While countries like China and Russia have pushed for regulations concerning cyber warfare as part of the [Shanghai Cooperation Organization](#) in 2009 and the International Information Security [Code of Conduct](#) in September 2011, it is high time for the international community to conduct a dialogue and decide on the formulation of a succinct law dealing with cyber warfare.