International Journal of Cyber Warfare and Terrorism
Volume 11 • Issue 2 • April-June 2021

Cyber Warfare and the "Humanization" of International Humanitarian Law

Steven Kleemann, Berlin School of Economics and Law, Germany & University of Potsdam, Germany
https://orcid.org/0000-0002-0556-7706

ABSTRACT

Cyber warfare is a timely and relevant issue and one of the most controversial in international humanitarian law (IHL). The aim of IHL is to set rules and limits in terms of means and methods of warfare. In this context, a key question arises: Has digital warfare rules or limits, and if so, how are these applicable? Traditional principles, developed over a long period, are facing a new dimension of challenges due to the rise of cyber warfare. This paper argues that to overcome this new issue, it is critical that new humanity-oriented approaches are developed with regard to cyber warfare. The challenge is to establish a legal regime for cyber-attacks, successfully addressing human rights norms and standards. While clarifying this from a legal perspective, the author can redesign the sensitive equilibrium between humanity and military necessity, weighing the humanitarian aims of IHL and the protection of civilians—in combination with international human rights law and other relevant legal regimes—in a different manner than before.

KEYWORDS

Cyber-Attack, Cyberwar, IHL, IHRL, International Human Rights, International Humanitarian Law, Law and Technology, New Technologies

INTRODUCTION

Over time, the law of war has evolved, especially with regard to means and methods of warfare. Not only has the common name for the legal regime changed in recent decades, the focus itself has shifted toward the humanization of that law, which is now known mainly as International Humanitarian Law (IHL) instead of "law of war" or "law of armed conflict". This process was driven by centering human rights and the principle of humanity. Although, the term IHL originally referred to the four 1949 Geneva Conventions, it is now steadily used to designate the whole body of laws regulating war. Consequently, these evolutions are manifested in both the content and the phraseology of the law (Meron, 2000:239).

On the downside, the issue of cyber warfare is not only highly topical, it also faces many challenges in terms of its international legal framework. Therefore, the question arises whether digital warfare has rules or limits under IHL, and if so, how are these applicable? Further pressing questions are how to define 'attack' under IHL with regard to cyber operations and what constitutes the conduct of such operations. Finally, the interconnection of military and civilian cyberspace affects one of the core principles of IHL, the principle of distinction, and needs attention.

Using cyber operations during armed conflict can have harrowing humanitarian consequences (ICRC, 2013:1). Through attacks against states or even private computers and networks, civilians might be deprived of medical care, drinking water, electricity or other essential needs (ICRC,

DOI: 10.4018/IJCWT.2021040101

2013:1). Aircraft control systems, nuclear plants, and dams rely on computers and are therefore highly vulnerable targets. This threatens the lives of hundreds of thousands of people and, due to the interconnection of networks, it is rather difficult to limit the attack to only part of a system without impairing the whole (ICRC, 2013:1).

To avert future civilian suffering, it is urgent that the international community properly responds to new means and methods of warfare and clearly spell out what is acceptable and what is not in cyber warfare. Since wars have rules and limits in terms of means and methods of warfare, inter alia with regard to the use of missiles, artillery or rifles, this should also apply to cyber warfare and the potentially tremendous danger it represents.

The problems in this regard can be considered from various legal angles. However, the following article will lay its focus mainly on the *ius in bello*. Due to limited space it is also not possible to address all issues regarding cyber warfare within IHL in depth. The article's aim is therefore instead to survey probable issues, providing comprehensive information on certain controversial issues within the sphere of cyber war and the principle of humanity.

THE HUMANIZATION OF INTERNATIONAL HUMANITARIAN LAW

In contrast with human rights law, IHL condones or at least allows the killing and injuring of human beings not even directly participating in an armed conflict – "civilian victims of lawful collateral damage." (Meron, 2000:240) Besides that, deprivation of personal freedoms without a judgement, wide-scale restrictions of freedom of expression and assembly is possible (Meron, 2000:240). All this is acceptable during armed conflict as long as "the rules of the game" are followed. The law of armed conflict (LOAC) regulates the dimensions of a struggle of life and death between opponents who are deemed equivalent as they are mainly both states (Meron, 2000:240). International Human Rights Law (IHRL) however, applies in the relationship between unequal parties (states and individuals), and its aim is to protect the physical integrity and human dignity (Meron, 2000:240). It becomes apparent that the two regimes IHL and IHRL are different, and the 'humanization' of the law of war can, in some way, be considered a contradiction in terms. Two overarching principles are held in the balance: military necessity and humanity.

Despite the apparent divergences between regulatory substance of the two bodies of law, the process of humanization of IHL evolves at least from the late 19th century onwards. One focal sector in which this progression has taken place is the law of targeting, whose goal is to confine 'attacks', by proscribing combatants to direct them against civilians (Biggio, 2017:41). As noted, the increase of capabilities of cyber operations creates tensions between the violence-centred rationale of the law of targeting and the essence of cyber-attacks. Their effects could result in disastrous effects, even without causing physical harm (Biggio, 2017:41). This gives rise to uncertainty with regard to the type of cyber operations that could qualify as 'attacks' under targeting law. Regulating cyber-attacks under targeting law may reconfigure the sensitive equilibrium between military necessity and humanity. The principle of distinction illustrates how humanitarian notions shape the LOAC. This principle "should lie at the heart of modern LOAC", (Turns, 2014:836) as it is the one of the basic principles with regard to lawful targeting, codified not only in Article 48 Additional Protocol I to the Geneva Conventions (AP I), it is also part of customary international law (Turns, 2014:836). The general protection of civilians is laid down in Article 51 AP I where it is stated that, "[t]*he civilian population and individual civilians shall enjoy general protection against dangers arising from military operations* […] [and that] "[t]*he civilian population as such, as well as individual civilians, shall not be the object of attack* […] [and that] [i]*ndiscriminate attacks are prohibited*." Logically, civilians should generally be protected against military cyber operations and cyber-attacks directed against them are prohibited, as they are indiscriminate. However, despite the enormous danger inherent to cyber war, it is sometimes seen as less devastating through the use of non-lethal weapons, not necessarily