ISPI
ITALIAN INSTITUTE
FOR INTERNATIONAL
POLITICAL STUDIES

COMMENTARY
3 May 2018

INTERNATIONAL HUMANITARIAN LAW IN CYBER OPERATIONS

Edoardo Greppi

University of Turin and ISPI

Cyber Warfare today is emerging as a new challenge, since the actors involved in contemporary armed conflicts also carry out attacks on computer networks. Terrible humanitarian consequences may arise from attacks on transportations systems (such as the control of civilian air traffic) or on electrical power, water supplies, chemical or nuclear plants, dams or oil structures and pipelines. This is to be seen in the wider context of cybersecurity issues with reference to critical infrastructures.

This application of new technologies as methods of warfare, only portrayed in fiction movies until a few years ago, has become a matter of serious concern for International Humanitarian Law (IHL) institutions and for governments, as well as for scholars and practitioners. International Humanitarian Law principles and rules have originally been conceived and extensively developed to address "physical warfare", the conduct of hostilities with the use of certain weapons, in the framework of the war on land, on sea, in the air and in the outer space. Now the cyberspace has become the fifth domain of warfare, in which operations against computers or computer systems through a data stream are conducted as means and methods of warfare in an armed conflict. Fortunately, up to now, cyber warfare has not given origin to serious humanitarian consequences. Nevertheless, a general concern for possible civilian casualties exists, even if only as indirect consequences (the Stuxnet case, and the damage to the Iranian nuclear programme).

The essential question relates to the possibility of applying the same principles and rules to a virtual world as the cyber context is. The International Committee of the Red Cross (ICRC) is developing and encouraging reflections and studies addressing key questions. Can cyber operations trigger the applicability of IHL? What can be qualified as "acts of violence" amounting to "attacks" in cyberspace? How the principle of proportionality can be applied when facing cases of "collateral

Edoardo Greppi, ISPI Senior Associate Research Fellow and Professor at the University of Turin.

damage" to civilian objects, considering that civilian and military computer networks are frequently closely interrelated? The principle of precaution in the attacks must also be recalled, in order to avoid excessive incidental damage to civilian objects, which are based and working on sophisticated computer systems, as it is in the case of hospitals and hydro-electric plants.

The pillar of IHL in the conduct of hostilities is the principle of distinction, which Additional Protocol I of the Geneva Conventions qualifies as the "Basic Rule". However, what does it mean in terms of the obligation of lawful combatants to distinguish themselves from the civilian population when they are acting in cyberspace operations?

In a very comprehensive approach to these delicate issues, there is a broad consensus on the idea that in this domain all relevant principles and rules of IHL fully apply, and that there is no legal void. The International Committee of the Red Cross (ICRC) addressed the problem of risks and vulnerabilities in the hostile use of cyberspace in its 2016 Report on "International humanitarian law and the challenges of contemporary armed conflicts" submitted to the 22nd International Conference of the Red Cross and Red Crescent (October 2015). According to the ICRC, IHL applies, even if cyber warfare is not expressly prohibited or regulated by existing treaties. Challenges are related to "the difficulties created by the anonymity on which cyberspace is built; the lack of clarity with regard to the application of IHL to cyber operations in the absence of kinetic operations; the debate pertaining the notion of attack under IHL rules governing the conduct of hostilities; and challenges in applying these rules to cyber warfare, in particular the prohibition of indiscriminate attacks and the rules on precautions in the attacks" (page 40 of the Report). Cyber operations amounting to an attack under IHL and directed, for example, at essential civilian infrastructures, are violations of IHL unless such infrastructure is at the same time used for military purposes, turning it into a legitimate military objective. The most comprehensive and detailed study on the applicability of international law to cyberspace is the Tallinn Manual (2013).

Many examples show the difficulty to differentiate between exclusively civilian and military cyber infrastructure. This is the case of military networks relying on cyber infrastructure, such as satellites or routers. Civilian vehicles or air traffic controls are equipped with navigation systems relying on GPS satellites, which are at the same time used by the military. A specific problem can arise if we apply the traditional criteria according to which the so-called "dual-use objects" (used for both civilian and military purposes) become military objectives. A strict application of this interpretation could lead to conclude that many objects of a cyberspace infrastructure would be considered military objectives not to be protected against attacks, both cyber and kinetic.

In any case, even if these attacks could be considered against lawful targets, they should fall under the general IHL prohibition of indiscriminate attacks and under the rules of proportionality and precautions in the attacks. The ICRC suggests that since IHL requires that the parties to a conflict "take all feasible measures to protect civilians and civilian objects under their control against the effects of hostilities", this obligation should already be implemented in peacetime, "especially with regard to fixed installations". Suggested measures are segregating military from civilian infrastructures and networks; segregating computer systems, upon which essential civilian infrastructure depends, from the internet; backing up important civilian data; using antivirus measures; making advanced arrangements to ensure the timely repair of important computer systems against cyber-attacks. Special care should be devoted to the protection of the cyber infrastructure and networks serving hospitals, and to study solutions like applying to the world of cyber space the protection reserved to demilitarized or protected zones.