Istituto Affari Internazionali

ISSN 22532-6570

IAI COMMENTARIES 18 | 35 - JUNE 2018

E-Emblems: Protective Emblems and the Legal Challenges of Cyber Warfare

by Adriano Iaria

The first rule governing armed conflicts is the strict distinction between civilians and combatants.[1] International humanitarian law (IHL) also provides special protection to certain objects such as medical units and their means of transport, cultural property, the natural environment and works and installations containing dangerous forces, "namely dams, dykes and nuclear electrical generating stations".[2]

To distinguish such objects, special emblems have been established and recognized in international treaties and customary law. The Red Cross, the Red Crescent and the Red Crystal are examples of such emblems, providing protection for military medical services and humanitarian aid workers.[3] The Blue Shield is instead applied to cultural property and archaeological heritage,[4] while the special emblem distinguishing works and installations containing dangerous forces is visualized by a sequence of three orange dots.[5] Finally, the yellow circle enclosing a blue triangle is applied to civil defence organizations, their personnel, buildings and material, as well as civilian shelters.[6]

[1] See IHL Database: *Practice Relating to Rule 1. The Principle of Distinction between Civilians and Combatants*, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule1.

[2] See IHL Database: *Practice Relating to Rule 42. Works and Installations Containing Dangerous Forces*, https://ihl-databases.icrc.org/customary-ihl/eng/docs/v2_rul_rule42.

[3] See the International Committee of the Red Cross (ICRC) website: *The Emblems*, https://www.icrc.org/en/war-and-law/emblem.

[4] Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, 1954, https://ihl-databases.icrc.org/ihl/INTRO/400.

[5] See IHL Database: *Practice Relating to Rule 42*, cit.

[6] See the International Civil Defence Organization website: *Emblem of Civil Defence*, http://www.icdo.org/en/about-icdo/icdo-symbols/emblem-civil-defence.

Adriano Iaria is a member of the Movement Support Group of the International Red Cross and Red Crescent Movement, for the 2018-2021 Action Plan on the Non-use, Prohibition and Elimination of Nuclear Weapons. In 2012, he supported the Permanent Mission of Italy to the United Nations in the context of negotiations for the Arms Trade Treaty (ATT).

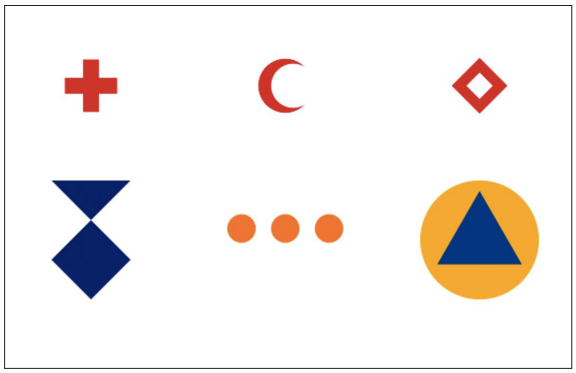
© 2018 IAI
ISSN 2532-6570
IAI COMMENTARIES 18 | 35 - JUNE 2018

Today, objects enjoying special protection can also be found in cyberspace, on the Internet, but they lack identifiable emblems. Examples include the websites and servers of hospitals, of museums and critical civilian technological infrastructure.

How can one strengthen international protection mechanisms for immaterial objects, virtual networks and infrastructure? How can states respond to new threats and should special provisions, including the definition of special emblems, be made for websites, networks and servers related to these objects, mirroring those that already exist for physical objects?

Cyberspace is heralding a new era of international relations, not only for international law, but also for the ethical implications that these new technologies pose. IHL places strict limits on the means and methods of warfare and these also apply to new weapons and technologies.[7] As argued by the International Committee of the Red Cross (ICRC) last October, new technologies such as cyber capabilities – and most recently even autonomous weapons systems – lend urgency to international efforts aimed at updating and expanding legal requirements for the use of such technologies and their compliance with IHL.[8]

Figure 1 | Internationally recognized protective emblems



Source: Author's elaboration

Cybersecurity has assumed increasing visibility due to new advancements in offensive technologies and the growing connectivity of objects and devises in cyberspace. Nowadays, the protection of critical infrastructures – both material and immaterial – is a priority for all state and non-state actors, extending potential threats beyond the traditional land, air and sea domains.[9]

Like these other domains, cyberspace is increasingly recognized as a potential "battlespace", an arena where states and non-state actors can engage and compete for power and influence. The conduct of hostilities between states is regulated by IHL – synonymous with *jus in bello*. By contrast, the *jus ad bellum* "refers to the conditions under which states may resort to war or to the

[7] See Article 36, Additional Protocol (I) to the Geneva Conventions, 1977, https://ihl-databases.icrc.org/ihl/INTRO/470.

[8] International Committee of the Red Cross (ICRC), *Weapons: Statement of the ICRC to the United Nations, 2017*, Statement at the General Debate on All Disarmament and International Security Agenda Items, First Committee (Disarmament and International Security), United Nations General Assembly, 72nd session, 10 October 2017, https://www.icrc.org/en/document/weapons-statement-icrc-united-nations-unag-2017.

[9] European Commission, *A New Approach to the European Programme for Critical Infrastructure Protection. Making European Critical Infrastructures More Secure* (SWD/2013/318), 28 August 2013. https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf.

use of armed force in general".[10]

Over the years, a number of states have engaged in operations that can be considered cyber warfare. Some, due to their low intensity, did not fall under IHL. Others, largely due to them taking place between states presently engaged in armed conflict, have generally been regarded to fall within the scope of IHL.[11]

With cyberspace acquiring a growing role in hostilities between states, a pool of legal experts began collecting and codifying IHL rules applicable in cyberspace. After three years work, in 2012 the group of law experts within the NATO Cooperative Cyber Defence Centre of Excellence approved the Tallinn Manual on International Law Applicable to Cyber Warfare. Most recently reviewed in 2017, the Tallinn Manual is not legally binding, but is the first and best attempt made so far to create order in the applicability of IHL to cyberspace.[12] While touching on various domains, the Tallinn Manual does not provide much clarity as to the potential use of protective emblems in cyberspace.[13]

In this respect, states need to identify and protect virtual infrastructure that is strictly connected to those objects that are protected by IHL, as well as extending such protection to servers and critical technological infrastructure from conventional attacks. Such protection poses big challenges, not only in applying the principle of distinction but also the principle of precaution. In order to protect essential civilian infrastructure that relies on cyberspace, it is also crucial to protect the infrastructure of cyberspace itself.

Major problems regarding cyber attacks and the protection of civilian infrastructure relate to the interconnectedness of civilian and military networks and the difficulty to attribute responsibility for an attack. As noted by ICRC in 2015;

"Most military networks rely on civilian cyber infrastructure, such as undersea fibre-optic cables, satellites, routers or nodes. Conversely, civilian vehicles, shipping, and air traffic controls are increasingly equipped with navigation systems that rely on global positioning system (GPS) satellites, which are also used by the military. Civilian logistical supply chains (for food and medical supplies) and other businesses use the same web and communication networks through which some military communications pass. Thus, it is to a large extent impossible to differentiate between purely civilian and purely military cyber infrastructures".[14]

[10] International Committee of the Red Cross (ICRC), *International Humanitarian Law. Answers to Your Questions*, Geneva, ICRC, 2016, p. 8, https://www.icrc.org/en/publication/0703-international-humanitarian-law-answers-your-questions.

[11] See the cases of Estonia and Georgia in 2007 and 2008.

[12] Michael N. Schmitt, "Rewired Warfare: Rethinking the Law of Cyber Attack", in *International Review of the Red Cross*, Vol. 86, No. 893 (Spring 2014), p. 189-206, https://www.icrc.org/en/international-review/article/rewired-warfare-rethinking-law-cyber-attack.

[13] Iain Sutherland et al., "The Geneva Conventions and Cyber-Warfare. A Technical Approach", in *The RUSI Journal*, Vol. 160, No. 4 (August 2015), p. 30-39.

[14] International Committee of the Red Cross (ICRC), "International Humanitarian Law and the Challenges of Contemporary Armed

ISSN 2532-6570

This difficulty, among many, has undermined recent efforts to regulate cyber operations. The non-binding confidence building measures (CBMs) proposed, for example, within the framework of the Organization for the Security and Co-operation in Europe (OSCE) in 2013 and 2016,[15] did not prevent attacks against specific infrastructure included under these measures.

In 1977, with the approval of the Additional Protocol I to the Geneva Conventions and its annex, states found an agreement to codify light and radio signals to protect the operations of medical units and other objects protected by internationally recognized emblems.[16] By doing so, states effectively extended protection to those non-physical infrastructures related to protected physical objects.

Building on this example, all states should today redouble their efforts to provide legal protection to certain cyber infrastructures by marking them with distinctive emblems. States may seek to extend similar protection to websites, networks and servers by marking them through electronic emblems or simply by using the emblems mentioned above and reproducing them on the Internet and in cyberspace. Another possibility would be that of developing special codes and coding that highlight the protection of such networks and servers under IHL.

It is time for states to move towards a better regulation of cyberspace. If states start to mark the websites and servers of hospitals or museums with such emblems, two immediate goals would be reached: in peacetime, states could promote familiarization on the special protection accorded to certain objects; in wartime, states would gradually be more prone to accord protection to these objects, limiting the adverse effects of cyber warfare and reinforce the central legal regulation pertaining to the distinction between combatants and civilians in war.

18 June 2018

Conflicts", in *International Review of the Red Cross*, Vol. 97, No. 900 (December 2015), p. 1477, https://www.icrc.org/en/international-review/article/international-humanitarian-law-and-challenges-contemporary-armed-0.

[15] Organization for the Security and Co-operation in Europe (OSCE), *OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, 10 March 2016, https://www.osce.org/pc/227281.

[16] Regulations Concerning Identification, as amended on 30 November 1993. See Additional Protocol (I) to the Geneva Conventions, 1977, cit., https://ihl-databases.icrc.org/ihl/INTRO/471.

© 2018 IAI
ISSN 2532-6570
IAI COMMENTARIES 18 | 35 - JUNE 2018

Istituto Affari Internazionali (IAI)
Founded by Altiero Spinelli in 1965, IAI does research in the fields of foreign policy, political economy and international security. A non-profit organisation, IAI aims to further and disseminate knowledge through research studies, conferences and publications. To that end, it cooperates with other research institutes, universities and foundations in Italy and abroad and is a member of various international networks. More specifically, the main research sectors are: European institutions and policies; Italian foreign policy; trends in the global economy and internationalisation processes in Italy; the Mediterranean and the Middle East; defence economy and policy; and transatlantic relations. IAI publishes an English-language quarterly (*The International Spectator*), an online webzine (*Affarinternazionali*), two book series (*Quaderni IAI* and *IAI Research Studies*) and some papers' series related to IAI research projects (*Documenti IAI*, *IAI Papers*, etc.).

Via Angelo Brunetti, 9 - I-00186 Rome, Italy
T +39 06 3224360
F + 39 06 3224363
iai@iai.it
www.iai.it

Latest IAI COMMENTARIES

ISSN 2532-6570