Philos. Technol. (2015) 28:475–478
DOI 10.1007/s13347-015-0196-9

COMMENTARY

The Cyber Combatant: a New Status for a New Warrior

Maurizio D'Urso[1]

Received: 27 February 2015 / Accepted: 6 March 2015 / Published online: 31 March 2015

Cyber warfare differs from traditional forms of conflicts, both in the instruments used—computers—and in the environment in which it is conducted—the virtual world of the internet and other data communication networks.

The purpose of the commentary is to discuss whether, even in cyber warfare, the concept of 'direct participation in hostilities' is still operative, with special reference to the laws related to it, and to assess its consequences with regard to the law of armed conflict. In particular, I will consider whether in cyber warfare the distinction between lawful combatant and unprivileged combatant is still valid. Standing on the premises that this distinction does not apply to non-military combatants in the cyber domain and that any civilian who is taking part in cyber warfare takes direct part in the hostilities as an unlawful cyber combatant, this commentary dwells on the concept of continuous combat function and applies it to cyber combatants. This will offer the ground to address the question as to whether a virtual network, an online forum where members share methods on the way to conduct cyber attacks against a common enemy, could be assimilated to a terrorist organisation whose members have a continuous combat function.

1 The Cyber Combatant's Status

The status of lawful combatant is defined in Article 1 of the Regulations concerning the Laws and Customs of War on Land, The Hague, 18 October 1907:

'Article 1. The laws, rights, and duties of war apply not only to armies, but also to militia and volunteer corps fulfilling the following conditions:

1. To be commanded by a person responsible for his subordinates;
2. To have a fixed distinctive emblem recognisable at a distance;
3. To carry arms openly; and
4. To conduct their operations in accordance with the laws and customs of war'.

✉ Maurizio D'Urso
ugag.ue@smd.difesa.it

[1] Italian Defence General Staff, Legal Affairs General Office (SMD–UGAG), Rome, Italy

This rule is also reproduced in the Article 4 of the Convention (III) relative to the Treatment of Prisoners of War. G Geneva, 12 August 1949.

According to The Hague 'jus in bello' and Geneva Conventions, any combatant who does not match all four of the conditions set in Article 1 is considered an 'unlawful' combatant. Meaning that, in case of capture by the enemy, he is not entitled to claim the rights granted to prisoners of war by Convention III relative to the Treatment of Prisoners of War, Geneva, 12 August 1949.

The issue concerning the status is in itself quite complex. It becomes even more so when non-military cyber combatants are under consideration. Especially if cyber combatants operate using computers only, they lack a basic requirement to be considered as lawful combatants: a computer is not considered a weapon, and thus they do not carry arms openly, as is required to be distinguished from civilian population.

A civilian hacker, in order to be distinguished from a member of the civilian population, should also wear a fixed distinctive emblem recognisable at a distance. Nonetheless, in reality it is difficult to imagine civilian cyber combatants wearing a distinctive emblem when they operate from their computers inside civilian buildings. The problem of the distinction between cyber combatants and the general population is evident. The dual-use problem makes the matter even more complex, making indistinguishable computers used for civilian purposes and computers deployed to perpetrate cyber attacks.

On the basis of the above considerations, it can be affirmed that a non-military cyber combatant is an unlawful combatant in almost all cases, with consequent strict limitations on the prerogatives and rights that one may have against the enemy in the event of capture and detention. The current situation is thus paradoxical, as the combatant who uses conventional weapons and lethal force, and may cause severe physical damage and harm, is more protected by International Humanitarian Law than a cyber combatant.

2 Direct Participation in Cyber Hostilities by Virtual Communities

Assuming that members of non-military cyber organisations cannot be considered lawful combatants, they have to be regarded as unlawful and unprivileged combatants who take part in hostilities. Regarding participation in cyber hostilities, the Tallinn Manual (states in Rule 29 that 'Civilians are not prohibited from directly participating in cyber operations amounting to hostilities, but forfeit their protection form attacks for such time as they so participate').[1]

This rule derives from Article 51 AP1 93, 3rd paragraph:

'Civilians shall enjoy the protection afforded by this Section, unless and for such time as they take a direct part in hostilities'.

Therefore, those civilians who participate directly in hostilities lose their general protection against the dangers of military operations and may be attacked for such time as they do so.

[1] Schmitt, Tallinn Manual on the International Law applicable to Cyber Warfare, (CUP 2013), p. 104

According to the Guidance on Direct Participation in Hostilities provided by the International Committee of the Red Cross, the notion of direct participation requires the following three cumulative elements:

1. 'The act must cause harm to the military operations or military capacity of a party to an armed conflict or, alternatively, inflict death, injury, or destruction on persons or objects protected against direct attack (threshold of harm);
2. Here must be a direct causal link between the act and the harm (direct causation);
3. The act must cause harm in support of a party to the conflict and to the detriment of another (belligerent nexus)'.

Time and continuity are another elements, which play a decisive role in considering a civilian taking part to hostilities as lawful target.

Being a member of an organised armed group means that the person assumes a continuous function for the group involving his or her direct participation in hostilities ('continuous combat function'). The continuous combat function is the mission of irregular combatants groups, whose members aim to fight the enemy indefinitely until his/her defeat. This is the group's mission and it is permanent and unlimited as long as hostilities last. The continuous combat function requires lasting integration into an organised armed group. Resembling soldiers of regular armed forces, members of an organised armed group who have a continuous combat function may be attacked at any time.

Those conducting hostilities face the difficult task of distinguishing cyber combatants who are engaged in a specific hostile act (direct participation in hostilities) from members of organised armed groups (continuous combat function). This difficulty is evident when considering the issue of direct participation in hostilities of members belonging to virtual communities, like forums or chat rooms, or individuals who are members of groups inside popular social networks—e.g. Facebook, Google or Twitter, exchanging malware and tips on conducting cyber attacks.

Continuous combat function is ascribed to the following:

- The administrators of the community, those who have organised the community and who give its members permission to use its services
- The advisors and the supporting staff that provide services and technical support
- The so-called 'senior members or moderators'—members distinguished from the others by the quality and quantity of their contribution in the community

All the other members do not have this continuous combat function and could be attacked only if and when they take part in hostilities on the basis of the three parameters of threshold of harm, direct causation and belligerent nexus.

3 Conclusions

The existing rules of international law are not capable of countering cyber warfare activities. The current regulations posed by the International Humanitarian Law do not allow a civilian cyber combatant to be considered a lawful combat, causing a

tremendous disparity of treatment in the case of capture and detention when compared with a 'regular' lawful civilian combatant using conventional weapons. This is unfair in equity or in ethics. It raises a plethora of regulative as well as ethical issues that urgently need attention from both the academic and the non-academic world.

Another problematic disparity arises when considering that, according to the International Humanitarian Law, a cyber combatant can be neutralised not only by cyber attack but also by the use of kinetic force, even lethal force if necessary. The principle of proportionality usually refers to the use of the minimum force required to accomplish the mission and neutralise the combatant. In case of a fight between cyber combatants and conventional combatants, the disproportion between the means used by one side against the other is clear and cumbersome.

It would be worthwhile to consider amending the Geneva Conventions and Additional Protocols in order to fit this brand new genre of combatant, whose status remains uncertain.