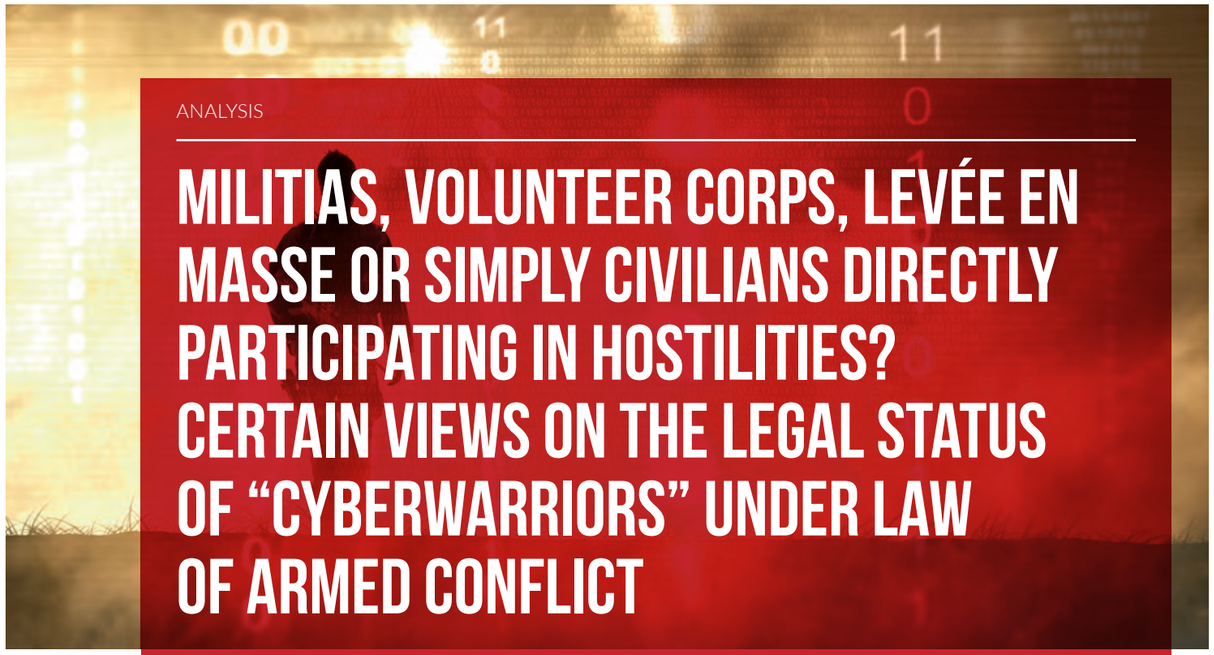
VOLUME 2 (2016) | ISSUE 2

CONTENTS



ANALYSIS

MILITIAS, VOLUNTEER CORPS, LEVÉE EN MASSE OR SIMPLY CIVILIANS DIRECTLY PARTICIPATING IN HOSTILITIES? CERTAIN VIEWS ON THE LEGAL STATUS OF "CYBERWARRIORS" UNDER LAW OF ARMED CONFLICT

WIESŁAW GOŹDZIEWICZ
Mr. Goździewicz is a Legal Adviser to the NATO Joint Force Training Centre in Bydgoszcz (Poland). He provides legal advice and training on the practicalities of the application of international humanitarian law and legal aspects of military operations. Mr. Goździewicz served at the Public International Law Division of the Legal Department of the Ministry of National Defence. Commander Goździewicz (Polish Navy) joined the Armed Forces as a junior legal officer, at the 43rd Naval Airbase in Gdynia. He is a graduate of the Faculty of Law and Administration of the University of Gdańsk.

1. Introduction

Growing „civilianisation" of contemporary armed conflicts is a fact. More and more civilians are present on or in vicinity of battlefields all over the world. Significant share of what used to be traditional military functions is nowadays being outsourced. This is caused mainly by two factors: gradual personnel reductions in most of the armies and growing reliance of the militaries on modern technology. Civilians (sometimes contractors) are hired to perform multiple functions from catering and logistics, through force protection, to providing actual combat force on the battlefield. Nowadays, it is not unusual to see civilian specialists operating or maintaining military equipment, weapon systems etc. for which highly specific knowledge, skillset and experience are required that the military lacks.

It is no secret that most militaries lack the expertise in cyberarea, thus it is highly likely that civilian specialists (most probably contractors) would become the "first choice cyberwarriors." Also, because cyber operations are relatively inexpensive, they may be considered particularly attractive by non-state actors engaged in asymmetric conflicts or hybrid warfare. Depending on multiple factors, such as the type of conflict, affiliation to state or non-state party, the nature of the relationship with the party to the conflict, the status of "cyberwarriors" under the law of armed conflict (LOAC) may vary. The purpose of this short article is to shed some light on the complicated, yet fascinating issue of the status of persons engaged in cyberwarfare and implications thereof. For the purpose of this

article, let us assume that cyberwarfare is either used in a broader armed conflict or independent cyber operations amount to armed attacks, thus trigger the initiation of an armed conflict.

Firstly, we will examine the matter of if and how Law of Armed Conflict (LOAC) applies to cyber hostilities (or cyberwarfare). Then, we will consider how the principal combatancy criteria as set forth in Geneva Convention 3 and Additional Protocol 1 to Geneva Conventions can be used in relation to "cyberwarriors." Next, the notion of direct participation in hostilities and organised armed groups will be assessed in the cyber context to culminate in an analysis of different possible options for legal status of persons involved in the conduct of cyber hostilities.

2. Applicability of LOAC to Cyberwarfare

There should be no doubt that international law applies to cyberspace and operations conducted therein. It has been recognised by the North Atlantic Treaty Organisation (NATO) in its Wales Summit Declaration[1] and confirmed by many scholars and legal experts, to include the drafters of the Tallinn Manual[2].

Undoubtedly, LOAC applies whenever an armed conflict exists, regardless of whether parties to the conflict recognise its existence and regardless of whether the conflict is of international or non-international character, as provided for in Articles 2 and 3 common to the four Geneva Conventions. From that perspective, if cyberactions cross the threshold of an armed attack, even if hostilities occurred only in cyberspace, without resort to conventional (or rather – traditional) means and methods of warfare, there will be an armed conflict, entailing the application of LOAC[3]. Modern means and methods of warfare do not evolve in a legal vacuum. Neither does legal vacuum exist in cyberspace[4]. To that end, it is worthwhile to quote the so called Martens Clause:

"Until a more complete code of the laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, as they result from the usages established among civilized peoples, from the laws of humanity, and the dictates of the public conscience[5]."

More recently, the Martens Clause was restated in Additional Protocol I, Art. 1(2): *"Recalling that, in cases not covered by the law in force, the human person remains under the protection of the principles of humanity and the dictates of the public conscience."*

In its commentary, the ICRC states that although the Martens Clause is considered to be part of customary international law[6], the plenipotentiaries considered its inclusion appropriate because:

"First, despite the considerable increase in the number of subjects covered by the law of armed conflicts, and despite the detail of its codification, it is not possible for any codification to be complete at any given moment; thus the Martens clause prevents the assumption that anything which is not explicitly prohibited by the relevant treaties is therefore permitted. Secondly, it should be seen as a dynamic factor proclaiming the applicability of the principles mentioned regardless of subsequent developments of types of situation or technology[7]."

Nowadays, the international community observes rapid development in military technology and also the means and methods of warfare. It is enough to mention the so called hybrid warfare, *"internationalised non-international armed conflicts"* (e.g. ISAF), development of autonomous weapon systems and, last but not least, the growing interest in examining the potential of offensive application of cybermeans and methods of warfare.

> "Apparently, there should be no doubt about LOAC applicability to cyberwarfare. The question is rather how LOAC applies to cyberwarfare, in particular whether (or when) it could be applied directly, or is there a need for mutatis mutandis application.

Drafting and adopting LOAC treaties obviously cannot keep the pace with technological and doctrinal developments in the area of modern warfare, thus the Martens Clause provides a "safety switch," recognised as customary international law that requires – should everything else fail – at least the application of the core four LOAC principles to all and any types of hostilities or means and methods of warfare.

In the author's view, this doesn't mean that only the core principles of LOAC apply to cyberwarfare. It just means that there can be no excuse to non-compliance with at least the core principles, even if it is recognised that there is no specific LOAC provisions governing for instance cyberwarfare, as opposed to explicit LOAC provisions restricting or prohibiting the use of certain conventional weapons, such as incendiary weapons, booby traps, laser weapons or expanding bullets.

Apparently, there should be no doubt about LOAC applicability to cyberwarfare. The question is rather how LOAC applies to cyberwarfare, in particular whether (or when) it could be applied directly, or is there a need for *mutatis mutandis* application. In the following section, this question will be answered with the example of combatancy criteria, as applicable to conduct of hostilities in cyberspace.

3. Cyberwarriors as Combatants

There is no simple definition of combatant. In fact, a number of IHL instruments contain different definitions of combatants. All of them are consistent when it comes to the obvious: granting combatant status to armed forces belonging to the party to the conflict. Differences (although perhaps not fundamental) occur with regards to other groups, militias, etc. belonging to the party to the conflict. Let us, however, start with defining the notion of armed forces.

Additional Protocol I to Geneva Conventions in its Article 43(2) provides perhaps the most comprehensive and widely adopted definition which states: *"The armed forces of a Party to a conflict consist of all organized armed forces, groups and units which are under a command responsible to that Party for the conduct of its subordinates, even if that Party is represented by a government or an authority not recognized by an adverse Party. Such armed forces shall be subject to an internal disciplinary system which,*

1 | Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, 5 September 2014, http://www.nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease, visited 18 January 2016.

2 | Tallinn Manual on the International Law Applicable to Cyber Warfare, general editor Michael N. Schmitt, Oxford University Press, 2013, p. 13.

3 | Knut Dörmann, 'The Applicability of the Additional Protocols to Computer Network Attacks: an ICRC Approach' in Karin Byström (ed.) International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law: Proceeding of the Conference (Stockholm: Swedish National Defence College, 2004), 142-143, http://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf, visited 24 Jan 2016.

4 | No legal vacuum in cyber space, 16-08-2011 Interview with Cordula Droege, ICRC legal adviser, https://www.icrc.org/eng/resources/documents/interview/2011/cyber-warfare-interview-2011-08-16.htm, visited 31 Jan 2016.

5 | Preamble to the Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907, https://www.icrc.org/applic/ihl/ihl.nsf/ART/195-200001?OpenDocument, visited 31 Jan 2016.

6 | Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC/Martinus Nijhoff Publishers, Dordrecht, 1987, p. 39, https://www.icrc.org/applic/ihl/ihl.nsf/Comment.xsp?action=openDocument&documentId=7125D4CBD57A70DDC12563CD0042F793 visited 03 Feb 2016.

7 | Ibidem, pp 38-39.

inter alia, shall enforce compliance with the rules of international law applicable in armed conflict." Militias and volunteer corps, if incorporated into the armed forces, are subject to the same requirements, as applicable to regular armed forces. It should be noted, however, that the legal regime and criteria governing membership or incorporation into the armed forces are generally contained in national legislation.

Members of other (i.e. those not forming part of armed forces) militias, volunteer corps, organised resistance movements, *levée en masse* can also be recognised as combatants, given they fulfil certain criteria that armed forces are considered to fulfil *ex lege*[8]. These criteria are formulated differently in Additional Protocol I, Geneva Convention III and the so called Hague Regulations[9], however can be reduced to the following:

1) being commanded by a person responsible for his subordinates;
2) having a fixed distinctive sign visible at a distance;
3) carrying arms openly;
4) conducting operations in accordance with the laws and customs of war.

If the four aforementioned criteria are fulfilled cumulatively, even members of irregular formations that do not constitute parts of armed forces, yet take part in hostilities, can enjoy the benefits of combatant status, to include combatant immunity, i.e. *"they shall not be called to account for their participation in lawful military operations[10]"* and should be granted prisoner of war status upon capture.

As criteria number one and four are rather uncontroversial (even in computer network operations), at least with regard to regular armed forces (who, by the way, will also always fulfil the requirement of *"belonging to a party to the conflict,"* thus simplify the issue of attribution if a cyberattack is conducted by members of regular armed forces), let us stop for a moment to analyse number 2 and 4 as crucial for compliance with the principle of distinction (between combatants as lawful military objective and civilians by default protected from attacks) and the obligation for combatants to distinguish themselves from civilians. Additional Protocol 1, Article 44(3) requires combatants to have a distinctive sign and carry arms openly while they are engaged in an attack or in a military operation preparatory to an attack. Yet, recognising certain specificities of guerrilla warfare, where "[…] *owing to the nature of the hostilities an armed combatant cannot so distinguish himself* […]," AP I provides that "[…] [such armed fighter] *shall retain his status as a combatant, provided that, in such situations, he carries his arms openly*:

a) during each military engagement, and
b) during such time as he is visible to the adversary while he is engaged in a military deployment preceding the launching of an attack in which he is to participate."

The reason for enforcing the obligation for belligerents to distinguish themselves from civilians is the obligation to protect civilians from direct attack, *"unless and for such time as they take a direct part in hostilities."* As will be discussed in more detail in the following section, the possibility to consider civilians as lawful military objectives is normally "conduct-based" (if they take direct part in hostilities), except for members of organised armed groups, who – similarly to members of armed forces – can be targeted by virtue of their status as members[11].

Today, modern means and methods allow remote conduct of hostilities. Computer network operations or cyberattacks are no different to that end from unmanned combat aerial vehicles (UCAVs) or stand-off weapons, that significantly reduce the prosper of capture of the person engaged in attack with the use of cybermeans, UCAV or stand-off weapons, yet make the attackers practically invisible to the enemy in the course of an attack. This makes some of the scholars to consider the four criteria less relevant for cyberwarriors than "conventional fighters," as opposed to the requirement to belong to a party to the conflict[12].

If a cyberattack is conducted by an entity that does not form a part of the armed forces, the issue of affiliation to a party to the conflict becomes somewhat challenging. Any governmental institution meets the requirement of belonging to a party to the conflict, but it is not so clear with respect to e.g. private enterprise, to which a state has turned to have carried out a network attack because of their knowledge, skills and technical capabilities. The requirement of affiliation may be met through a factual relationship, functional, which does not need to be formalised, but if such a link actually exists (e.g. in the form of a contract), it should be considered as satisfying the requirement of belonging to a party to the conflict.

Affiliation with a party to the conflict also involves state responsibility for the actions of armed groups carried out "at the request" of the state. One of the key principles of international law is that states (rather than individuals) bear liability for violation of obligations under international binding upon that state, if the breach is a consequence of actions that can be attributed to that state. State will bear the responsibility for the actions of their bodies and government institutions (including the armed forces) that constitute violations of international law, but would also be liable for the actions of private actors by order of state authorities, in accordance with the instructions of the state bodies under the direction or control of the State (criterion of effective control as in the case of *de facto* commanders)[13]. The principle applies to all military operations, conducted both by the regular armed forces and other organised groups meeting the criteria of Art. 43 of the first Additional Protocol, but is of particular importance in the context of operations in cyberspace that would be outsourced to private entities.

"Affiliation with a party to the conflict also involves state responsibility for the actions of armed groups carried out "at the request" of the state.

Even if the cyberattack qualifies as armed attack, that is, it is reasonable to assume that it would result in injuries to or death of persons or damage to or destruction of buildings, in most cases, such an attack will be carried out from a remote location, without direct contact between the attacker and the attacked. This may suggest that the requirement for combatants conducting a network attack to distinguish themselves from civilians by wearing fixed distinctive signs becomes less relevant,

8 | Leslie C. Green, The Contemporary Law of Armed Conflict, Juris Publishing, Manchester University Press, Manchester 2000, pp. 34-35; Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Law. Volume I: Rules., International Committee of the Red Cross, Cambridge University Press, Cambridge 2005, pp. 15-16.

9 | Regulations Respecting the Laws and Customs of War on Land annexed to Convention (IV) respecting the Laws and Customs of War, The Hague, 18 October 1907, https://www.icrc.org/ihl/INTRO/195 access 14 February 2016.

10 | Knut Ipsen, Combatants and non-combatants in: The Handbook of International Humanitarian Law, edited by Dieter Fleck, Oxford University Press, Oxford 2009, p. 95.

11 | Sean Watts, Combatant Status and Computer Network Attack, in: Virginia Journal of International Law, Vol. 50 – Issue 2, Virginia Journal of International Law Association, 2010, p. 420; Of note, even being considered a member of an organized armed group does not automatically entail combatant privileges or combatant immunity if the four combatant criteria prescribed above are not met.

12 | Ibidem, pp. 337-441.

13 | Guenael Mettraux, The Law of Command Reposnsibility, Oxford University Press, Oxford 2009, s. 100-102, 110-113, 122-123.

especially in situations in which the network attack is carried from within a military objective, for which there is a separate obligation to mark it (e.g. a warship or military aircraft)[14]. Nevertheless, in the author's view, the distinction requirement can be met by e.g. using IP addresses that are clearly different from those used by civilians or civilian entities or at least – when hiding the IP address from the objective of the cyberattack (as a mean to avoid or hamper counteractions) – using such tools that are specific to the military and leave no room for allegations of feigning civilian status which would be considered as perfidy in accordance with AP I Art. 37(1).c[15].

Similar approach could be adopted with regards to the criterion of carrying arms openly. Conventional (or "classical") weapons are not used in computer network operations. It would be hardware or software, both either specifically developed or adjusted to carry out cyberattacks. As it is difficult to expect "cyberwarriors" to carry their laptops marked as weapons with special stickers, especially if they are sitting thousands of miles away from their targets, perhaps the use of specific malware, not available "off the shelf" to any "hacker wannabe," or "weaponised" software clearly distinct from its civilian analogues, is the vehicle to ensure the weapons carrying criterion is met, except for cyber *levée en masse* (to be discussed in more detail in Section 5 of this article), for which spontaneous "taking up arms" might prevent the possibility to obtain militarised or weaponised information technology (hardware or software), but which – arguably – cannot exist in borderless cyberconflicts[16].

14 | Tallinn Manual, op. cit., pp. 99-100.

15 | Sean Watts, op. cit., p.442; see also Vijay M. Padmanabhan, Cyber Warriors and the Jus in Bello in: International Law Studies vol. 89 (2013), U.S. Naval War College, 2013, pp. 295-296.

16 | David Wallace, Shane R. Reeves, The Law of Armed Conflict's "Wicked" Problem: Levée en Masse in Cyber Warfare, in: International Law Studies vol. 89, op. cit, pp. 662-663.

4. Direct Participation in Hostilities (DPH) and Organised Armed Groups (OAGs) in the Cyber Context

Additional Protocol 1 Art. 51.(3) and Additional Protocol 2 Article 13.(3) provide that civilians are immune from direct attack unless and for such time as they take a direct part in hostilities. They lose this protection for the duration of each act amounting to direct participation, however, this conduct-based concept should only apply to civilians who are neither members of armed forces (to include militias and volunteer corps incorporated into the armed forces) or organised groups nor participate in *levée en masse*. For members, their membership alone is sufficient to determine their status as lawful military objectives (although criteria of membership will differ, as will be discussed below), regardless of whether they actually take direct part in hostilities at a given time. In an effort to define both the notion of DPH as well as membership in organised armed groups, International Committee of the Red Cross (ICRC) has issued its guidance[17] which, in fact, was the first comprehensive study on this topic. Although controversial in many aspects[18], it actually provides good overview of the issue and served as a catalyst for in-depth discussions of the practicalities of the DPH concept and its application in contemporary armed conflicts, most of which has been asymmetric over the last two decades.

a) DPH Criteria

What are the cumulative criteria that an act has to fulfil in order to be considered as amounting to DPH? In accordance with the ICRC guidance, these are: 1) threshold of harm, 2) direct causation and 3) belligerent nexus.

17 | Nils Melzer, Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law, International Committee of the Red Cross, Geneva 2009.

18 | See e.g. Michael Schmitt., The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis in: Harvard National Security Journal Vol. 1, May 5, Cambridge (Massachusetts) 2010; Kenneth Watkin, Opportunity Lost: Organised Armed Groups and the ICRC "Direct Participation in Hostilities" Interpretive Guidance, in: New York University School of Law Journal of International Law and Politics Vol. 42, No. 3, New York 2010.

1) **Threshold of harm** – the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack. Acting to the benefit of one's own party to the conflict the act has to result or be likely to result in negative consequences to the enemy's military effort[19]. It should be noted that adversely affecting military operations or capacity of the other party does not necessarily require causing physical damage. The ICRC guidance states that "[e]*lectronic interference with military computer networks could also suffice, whether through computer network attacks (CNA) or computer network exploitation (CNE).*"

2) **Direct causation** – there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part. For example, transporting weapons or other military equipment may be considered to be directly related to cause harm in military terms (and thus constitute DPH) only when it is executed as an integral part of a specific military operation, planned to inflict appropriate amount of damage (of sufficient degree of harm). Therefore, training or recruiting militants for organised armed groups, although it is essential to the military capabilities of the group, will not fulfil the direct causation criterion, unless it will be carried out in order to prepare a pre-planned specific military operation or hostile act. In this case, because the training or recruitment might be considered an integral part of the operation, and the causal link to the operation will be direct[20]. The guidance recognises that CNAs, despite their remoteness, will in most cases meet the direct causation test[21].

3) **Belligerent nexus** – an act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (carried out to gain definite military advantage). From that perspective, organised self-defence of the civilian populace against pillaging or other acts of violence towards the populace, even if resulting in hostile acts against the party to the conflict that fulfil the other two criteria, shall not be considered as DPH. Similarly, bank robbery (to include "cyber-robbery") committed by belligerents for their personal gain (not in support of the military operation of a party to the conflict) should be considered a criminal act rather than DPH[22].

The ICRC Guidance does not provide many examples of acts amounting to DPH in the cyber context. Nevertheless, if a cyberattack can amount to an armed attack, certain activities conducted in or through cyberspace will definitely fulfil criteria of direct participation in hostilities. The following three examples might be useful to illustrate the concept of DPH in the cyber domain.

Scholars tend to agree that designing malware (even for military purposes) would usually not fulfil the three criteria of DPH, unless such malware is specifically designed to exploit vulnerabilities of particular target or modified (customised) to be used in a specific cyberattack[23].

19 | Nils Melcer, op. cit., p. 47.

20 | Ibidem, p. 53. An example of training or recruitment that meets the direct causation test might be to select volunteers to conduct suicidal IED attack, and to train them on the topography of the object of attack, infiltration methods and vulnerabilities to be exploited in order to successfully execute the attack.

21 | Ibidem, p. 55.

22 | Ibidem, p. 62-63.

23 | Hanneke Piters, Cyber Warfare and the Concept of Direct Participation in Hostilities, in: NATO Legal Gazette Issue 35 (December 2014), p. 54, http://www.act.nato.int/images/stories/media/doclibrary/

Installation, servicing and maintenance of computer systems or software would normally not amount to DPH, especially if linked to passive (or reactive) cyberdefence. If, however, the system (or software) in question is being installed in preparation for launching a cyberattack at a specific target, it would amount to DPH, because "[measures] *preparatory to the execution of a specific act of direct participation in hostilities, as well as the deployment to and the return from the location of its execution, constitute an integral part of that act.*[24]"

Lastly, operation of a computer system or software in the course of a cyberattack (fulfilling the criteria of an armed attack, as assumed in the beginning of this article) would in most cases amount to DPH, regardless of whether the malware is to activate instantly or contains "delayed fuse" designed so that the malware took intended effects at a given point in time[25]. Exploring general vulnerabilities in software operated by the enemy would not amount to DPH, as opposed to exploiting such vulnerabilities in preparations for a cyberattack or in support of a conventional attack, just as collecting tactical intelligence would be considered DPH, whereas strategic intelligence activities would not[26].

b) Organised Armed Groups (OAGs)

Considerations on the subject of organised armed groups should be started with a statement that the concept of organised armed groups (OAGs) functions only in non-international armed conflicts (NIACs), where the state party to the conflict is represented by governmental security forces (to include regular armed forces) and the non-state party is fought for by either dissident armed forces (mutinied part of the armed forces) or OAGs. As the legal notion of combatants cannot be referred to with regard to persons engaged in hostilities on the non-state party to the conflict, the term "fighters" that encompasses both members of dissident armed forces and OAGs is being used despite not being reflected in LOAC treaties[27].

It should also be noted that in accordance with Article 3 common to all four Geneva conventions, applicability of Geneva conventions to NIAC is very limited, therefore provisions of Geneva Convention III (relative to the Treatment of Prisoners of War) dealing with combatancy and POW status will not apply, unless parties to the NIAC "[...] *bring into force, by means of special agreements, all or part of the other provisions* [...]" of the Convention. Neither will provisions of Additional Protocol I apply and thus there are no combatants or POWs in NIACs, although enemy fighters will constitute lawful military objectives.
As opposed to civilians who sporadically or spontaneously take direct part in hostilities and are considered "fighters" for the duration of each act amounting to DPH[28], persons who qualify as members of OAGs, become lawful military objectives for the duration of their membership, allegedly in a manner similar to members of regular armed forces. This means that as long as the membership exists, these persons can be targetable 24/7.

OAGs should belong to the non-state to the conflict (and the belonging could in fact mean even loose linkage materialised in following the directions and guidance of the non-state party) and fulfil the criteria laid down in Article 1(1) of Additional Protocol II, namely being under responsible command and exercising "[...] *such control over a part of [the state party's] territory as to enable them to carry out sustained and concerted military operations and to implement* [Additional Protocol II]." Putting aside the problematic question of territory in cyberspace, let's simplify the issue by adopting an assumption that there is an OAG fulfilling the aforementioned criteria and focus on the membership issue.

Membership in OAGs shall not be linked to a formalised joining or recruitment. There will be no formal relationship or bond, no formalised and common uniforms with distinctive signs and no identification cards serving the purposes of Geneva Convention III. In accordance with the ICRC Guidance, the only determining factor will be the so called continuous combat function constituting the foundation of the functional relationship with an OAG. Assumption of this continuous combat function is to be the objective indication of membership.

ICRC stated that continuous combat function requires lasting integration with an OAG and usually this function would be to take direct part in hostilities, although persons whose functions involve preparing, conducting or commanding operations or actions amounting to DPH is believed to have had continuous combat function. Persons, who within an OAG fulfil non-combat functions (administrative, political, logistic), in accordance with the ICRC guidance should not be considered members of that OAG, which has become a point of friction, as – in the opinions of some of the experts – it results in unequal treatment of regular armed forces and OAGs[29].

Also, a person who has been recruited, trained and equipped by an OAG to repeatedly take direct part in hostilities may be considered a member of this OAG (and thus a lawful military objective that may be subject of lethal targeting) even before committing the first act amounting to DPH, if upon completion of the training the person concerned does not "leave" the OAG. This is one more example of controversies behind the ICRC guidance: if there is no formalised joining criteria, how is it possible to determine if resignation took place?

Shifting to the cyberwarfare context, if the ICRC guidance was taken into account literally, only persons who joined an OAG in order to conduct cyberattacks crossing the threshold of armed attacks or in other manner amounting to DPH as illustrated above could be considered members and thus targetable throughout the duration of their membership (however the duration could be determined). Other persons affiliated with a cyber-OAG could only be targeted for the duration of each act amounting to DPH. Enjoying immunity from direct attack in military terms does not preclude facing criminal liability, though, as even Additional Protocol II, art. 6.(5) seems to recognise that taking part in a NIAC would violate criminal laws of the state party to the conflict and – as opposed to members of armed forces belonging to the state party – fighters on the non-state side would not enjoy combatant immunity.

From that perspective, hacktivists would normally face penal consequences of their actions, however members of hacker groups trained to conduct cyberattacks amounting to DPH or crossing the threshold of armed attack would fall within the category of lawful military objectives, whose *"partial or total destruction, capture or neutralisation"* would be lawful, if offering a definite military advantage in the circumstances ruling at the time[30].

5. Concluding Remarks – Lawful Options for Cyberwarrior Formations

A natural conclusion can be drawn from the considerations above: the optimal solution for cyberwarriors is to be members of the armed forces of a party to the conflict and there are

legal_gazette_35.pdf, access 16 February 2016.

24 | Nils Melzer, op. cit, p.17.

25 | Hanneke Piters, op. cit., pp. 55-56.

26 | Ibidem, pp. 34-35, 49, 52, 66-67.

27 | Michael N. Schmitt, Charles H.B. Garraway, Yoram Dinstein, The manual on the Law of Non-International Armed Conflict with Commentary, Martinus Nijhoff Publishers, Leiden/Boston 2006, pp. 4-5.

28 | This is one of the biggest controversies behind the ICRC Guidance, referred to by some scholars as the "revolving door concept" allowing fighters to regain protected civilian status after committing DPH, perfectly captured in the phrase "farmer by day, fighter by night". See e.g. Kenneth Watkin, Opportunity lost..., op. cit. pp. 686-690.

29 | Michael Schmitt, The Interpretive Guidance..., op. cit., pp. 15, 22-23.

30 | Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Law..., op. cit., p. 29.

several nations who have stood up their military organisations or units to deal with cyber operations (both defensive and offensive). Examples include U.S. Cyber Command (CYBERCOM), Chinese People's Liberation Army General Staff 3rd Department and Unit 61398, Israeli Defence Forces Unit 8200 or Democratic People's Republic of Korea Bureau 121[31].

> "the optimal solution for cyberwarriors is to be members of the armed forces of a party to the conflict

Members of armed forces are combatants, they are entitled to participate in hostilities and they enjoy combatant immunity for their actions in the course of hostilities, as long as these actions do not violate LOAC. Combatant immunity is of particular importance to those, who engage in offensive cyber operations or such cyberdefence activities that could be considered *"acts of violence against the enemy"*, as provided for in Article 49(1) of Additional Protocol I.

However, is it only military units and their personnel wearing uniforms that constitute armed forces? No, because as provided for in Article 43(1) of Additional Protocol 1, "[t]*he armed forces of a party to the conflict consist of all organised armed forces, groups and units which are under a command responsible to that party for the conduct of its subordinates*." The quoted provision is considered a reflection of customary international law, which state practice has confirmed over decades and is equally applicable to international and non-international armed conflicts. In countries where militia or volunteer corps (so-called "irregular" armed forces) constitute the army, or form part of it, they are included under the denomination "army". This definition is also used in Article 4 of the Third Geneva Convention, with the addition of organised resistance movements. Yet, with the privileges of combatant immunity and the right to engage in hostilities, come the obligations for the non-regular parts of the armed forces (i.e. militias, volunteer corps and organised resistance movements) to fulfil the four criteria of combatancy, as described in Section 3 above. It also requires incorporation into the armed forces that would enable the enforcement of command and control and disciplinary regime that ensures compliance with LOAC. The same requirement incorporation pertains to paramilitary organisations or armed law enforcement agencies that for the duration of an armed conflict may become parts of the armed forces (e.g. U.S. Coast Guard or Polish Border Guards).

Such incorporation would usually require a formal act, for example, an act of parliament that would define the membership criteria and requirements in a manner similar to the military. In the absence of formal incorporation, the status of such groups could be based on the facts and in the light of the criteria for defining armed forces[32].

This incorporation is a perfect vehicle to make voluntary defence organisations (defence leagues) specialised in cyberdefence or cyberwarfare more generally, comprised of talented specialists working as civilians on a daily basis, but undertaking certain military training similar to reservists, to fall under the protective umbrella of combatant status, should an armed conflict occur. Such cyber specialists wouldn't need to be mobilised as regular reservists, but the defence organisation to which they belong could be incorporated into the armed forces as a whole, with its organisational structure, personnel and equipment. Additional Protocol I requires a party to the conflict to notify such incorporation to the other parties to the conflict.

31 | Paul Walker, Organizing for Cyberspace Operations: Selected Issues, in: International Law Studies vol. 89, op. cit., pp. 342-343.

32 | Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Law..., op. cit., p. 17.

It is obvious that vast majority of expertise in cyber (defence) lies with the private (or civilian) sector. Some nations' militaries didn't develop their organic cyber capabilities, not to mention forming cyber-specialised units. Some nations, due to regulatory restrictions, cannot offer their uniformed personnel performing cyber duties emoluments that would be more attractive than those paid by big corporations, however they can either hire civilian employees or outsource such capabilities from the private sector, as the military does in many other areas previously belonging to the military (e.g. logistics). What would be the legal status of such civilian employees or contractors under LOAC?

Both civilians accompanying the force and contractors do not form part of the armed forces[33]. And though as a general rule, they are immune from direct attack, they share the risks and dangers of war alongside with the armed forces they accompany[34]. The ICRC Guidance provides that "[p]*rivate contractors and employees of a party to an armed conflict who are civilians* […] *are entitled to protection against direct attack unless and for such time as they take a direct part in hostilities. Their activities or location may, however, expose them to an increased risk of incidental death or injury even if they do not take a direct part in hostilities.*"[35] If, however, civilians are employed or contractors outsourced to perform combat function that fulfils DPH criteria, to include cyberattacks, they lose their protection from attack without gaining combatant privileges.

Moreover, in certain circumstances, as defined in Additional Protocol I, Art. 47(2)[36], civilian employees or contractors performing combat functions (taking direct part in hostilities, engaged in warfare), may be considered as mercenaries, especially if their wages in order to be competitive compared to those offered by private sector are significantly higher than those paid to the military. Persons determined mercenaries are not entitled to combatant privileges and thus – if captured – do not enjoy POW status and may be prosecuted for not only taking direct part in hostilities, but also for the fact of being mercenaries, which is penalised by many national criminal legislations.

With regard to other types of formations that may be considered combatants under LOAC, basically all of them raise significant questions to their applicability in the cyber context. Firstly, *levée en masse* defined as "*the inhabitants of a country which has not yet been occupied who, on the approach of the enemy, spontaneously take up arms to resist the invading troops without having time to form themselves into an armed force*." Although – as stated by some scholars[37] – due to the nature of cyberconflicts (no borders and no territories) – *levée en masse* would not exist in such conflicts, one could imagine spontaneous creation of a cyber *levée en masse* in reaction to an enemy invasion. It does, however raise an issue of carrying arms openly. Even the solution mentioned above, i.e. utilising unique IP addresses or non-civilian technologies to conceal the IP addresses, might be problematic, as it is impossible for the military to share the technologies with a spontaneously emerging group. Yet, there might be options for cyber *levée en masse* to distinguish themselves from civilian network users, by e.g. publically announcing that certain

33 | Jean-Marie Henckaerts, Louise Doswald-Beck, Customary International Law..., op. cit., p. 13.

34 | Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare, ed. by Yoram Dinstein and Bruno Demeyere, Program on Humanitarian Policy and Conflict Research at Harvard University, Version 2.1, Harvard University, Cambridge (Massachusetts) 2010, pp. 270-271.

35 | Nils Melzer, op. cit., p. 37.

36 | A mercenary is a person who: 1) is specially recruited locally or abroad in order to fight in an armed conflict; 2) does, in fact, take a direct part in the hostilities; 3) is motivated to take part in the hostilities essentially by the desire for private gain and, in fact, is promised, by or on behalf of a Party to the conflict, material compensation substantially in excess of that promised or paid to combatants of similar ranks and functions in the armed forces of that Party; 4) is neither a national of a Party to the conflict nor a resident of territory controlled by a Party to the conflict; 5) is not a member of the armed forces of a Party to the conflict; and 6) has not been sent by a State which is not a Party to the conflict on official duty as a member of its armed forces.

37 | See supra note 16.

sources of cyber actions or certain cyber tools are used solely by that cyber *levée en masse*.

Similar issues arise with other irregular groups: other (i.e. not belonging to nor incorporated into armed forces of a party to the conflict) militias and volunteer corps and organised resistance movements. As opposed to *levée en masse*, they are required to fulfil all the four combatancy criteria, as it assumes that they have sufficient time for organising themselves in a manner allowing to develop responsible command and disciplinary regime enabling to enforce compliance with LOAC, however fulfilment of the requirement to carry arms openly may become equally problematic without access to typically military cyber technologies.

6. Summary and a handful of recommendations

Full compliance with LOAC requirement in cyberwarfare might be challenging even for regular armed forces, which by definition are supposed to e.g. fulfil all the combatancy criteria. It gets even more challenging for irregular fighting groups, as hopefully has been proven above. Challenging doesn't mean impossible, though, and LOAC itself comes with assistance offered by the Martens Clause encouraging flexible approach to certain LOAC provisions. Adaptability of LOAC is its great advantage and – as stressed in recommendations from the First European Cybersecurity Forum – CYBERSEC.EU 2015, "[...] *legal framework governing the conduct of hostilities in cyberspace is sufficient* [...] *and the tendency to over-regulate should be avoided*[38]."

There are two principal ways of ensuring that "cyberwarriors" lawfully engage in hostilities: enrolment to the armed forces or becoming member of a militia or voluntary corps that complies with LOAC criteria of combatancy. One of the recommendations from CYBERSEC. EU 2015 was establishment of voluntary civic defence leagues composed of skilful and talented individuals capable of employing cybermeans and methods of warfare effectively. In order for such defence leagues to be entitled to lawfully take part in hostilities they could be either:

1) Offered and accepted up front to be incorporated into the armed forces upon commencement of an armed conflict; such defence leagues would have to lobby for their governments to introduce appropriate legislation (preferably before, not after the conflict has started); should circumstances require, military cyber technologies could be made available in advance to such civic defence leagues (to include appropriate training); or

2) If not incorporated into the armed forces, they would have to ensure on their own that they meet all the combatancy criteria; this might be more challenging, especially without access to military technologies clearly distinct from cybermeans and capabilities available to "regular" civilians.

> "There are two principal ways of ensuring that "cyberwarriors" lawfully engage in hostilities: enrolment to the armed forces or becoming member of a militia or voluntary corps that complies with LOAC criteria of combatancy.

The former option – although initially more formalised and requiring adoption of respective legislation – offers subsequent simplicity in implementation and execution, as well as full compliance with LOAC requirements and perhaps this is the option that should be pursued in order to enable talented individuals who are civilians in their regular life to become lawful cyberwarriors, should homeland call to arms. ■

38 | CYBERSEC 2015 Recommendations, p. 11, https://app.box.com/s/kb6zaq06v0uyhdh7pr13zk132uiwvu2u, access 21 February 2016.