Applicability of the Additional Protocols to Computer Network Attacks

Knut Dörmann*

1. Introductory remarks

The purpose of this contribution is to explore whether international humanitarian law (IHL) in general applies to computer network attacks (CNA) and what specific prohibitions or limitations on the use of computer network attacks follow from international humanitarian law, in particular from the Additional Protocols. This will be done from an ICRC perspective, but not exclusively.

To date the ICRC has not publicly stated a position in this regard. This contribution will outline aspects of ICRC's ongoing thinking. It is therefore only preliminary stock-taking and subject to further internal reflection.

Given that the mandate of the ICRC with regard to its legal activities is confined to the implementation and development of IHL, its reflection does not extend to other important legal questions related to, for example, whether or not CNA represent a permissible use of force under the Charter of the United Nations or whether space or telecommunications law impose specific restrictions on computer network attacks.

Michael Schmitt's contribution[1] provides a detailed overview of the many legal challenges posed by CNA under existing *ius in bello*, with a specific focus on the consequences arising from the principle of distinction. Since the views of this author relating to CNA and the principle of distinction do not differ much from the views expressed by Michael Schmitt, the remarks thereon will be limited to a few comments. These will then be followed by an elaboration of other issues subject to reflection by the ICRC – focussing essentially on international armed conflicts,[2] i.e.

- What prohibitions or limitations to CNA follow from rules giving special protection to certain objects?
- What activities of civilians relating to CNA constitute direct participation in hostilities and cause them to lose their protection against direct attack?
- Must the defender fulfil specific requirements in order to comply with its obligation to take precautions against attacks?
- Do specific prohibitions of methods of warfare, such as the prohibition of perfidy or of improper use of protected emblems, signs and signals, apply to CNA and, if so, in which way?

The core provisions of IHL are found in the 1949 Geneva Conventions,[3] the 1977 Additional Protocols to the Geneva Conventions[4] and customary international law. None of these address

---

* Dr. Knut Dörmann is Deputy Head of the Legal Division, International Committee of the Red Cross (ICRC), Geneva.

[1] Michael N. Schmitt, Computer Network Attack and the Law of International Armed Conflict, published in this volume.

[2] This contribution will not cover issues related to combatant and prisoner of war status. This has been done by Heather A. Harrison-Dinniss in the volume.

[3] Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, Geneva, 12 August 1949 (hereinafter GC I); Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, Geneva, 12 August 1949 (hereinafter GC II);

explicitly CNA. The Geneva Conventions with their focus on the protection of persons in enemy hands are only of limited relevance to CNA. Without reference to specific weapons, the two Additional Protocols address various methods and means of warfare in general terms. Thus the APs are most likely to present a framework for the use of CNA. The fact that CNA developed only after the adoption of the Protocols does not preclude their applicability. The very existence of Art. 36 of Additional Protocol I (AP I) is a strong indicator that the drafters of AP I anticipated the application of its rules to new developments of methods and means of warfare.[5] It requires that:

> *"In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."*

Consequently, the fact that a particular military activity constituting a method of warfare is not specifically regulated, does not mean that it can be used without restrictions. Based on that, nothing precludes to assume that the more recent forms of CNA, which do not involve the use of traditional weapons, are subject to IHL just as any new weapon or delivery system has been so far when used in an armed conflict.[6] One of the fundamental rules of IHL states that the right of the Parties to the conflict to choose methods or means of warfare is not unlimited.[7] If a computer network attack is directed against an enemy in order to cause damage, such as manipulation of an air traffic control system, which causes the crash of civilian aircraft, it can hardly be disputed that such a CNA is in fact a method of warfare and is subject to limitations under IHL.

There is no doubt that an armed conflict exists and IHL applies, once traditional kinetic weapons are used in combination with new methods of CNA. The most difficult situation, as far as applicability of IHL is concerned, would be the one where the first, or the only "hostile" acts are conducted by CNA.[8] Can this be qualified as constituting an *armed* conflict within the meaning of the 1949 Geneva Conventions and other IHL treaties? Does it depend on the type of CNA, i.e. would the manipulation or deletion of data suffice or is physical damage as the result of a manipulation required? As to the temporal element, the ICRC Commentary to the 1949 Geneva Conventions takes the view that in the case of a cross-border operation, the first

---

Convention (III) relative to the Treatment of Prisoners of War. Geneva, 12 August 1949 (hereinafter GC III); Convention (IV) relative to the Protection of Civilian Persons in Time of War, Geneva, 12 August 1949 (hereinafter GC IV).

[4] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 (hereinafter AP I); Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II), 8 June 1977 (hereinafter AP II).

[5] See also Emily Haslam, Information warfare: Technological Changes and International Law, Journal of Conflict and Security Law (2000), Vol. 5 No. 2, p. 160, Wolff Heintschel von Heinegg, Informationskrieg und Völkerrecht, Volker Epping/Horst Fischer/Wolff Heintschel von Heinegg (eds.), Brücken bauen und begehen, Festschrift für Knut Ipsen zum 65. Geburtstag, 2000, pp. 132, 147.

[6] Louise Doswald-Beck, Some Thoughts on Computer Network Attack and the International Law of Armed Conflict, in: Michael N. Schmitt/Brian T. O'Donnell (eds.), Computer Network Attack and International Law, International law Studies, Vol. 76, 2002, p. 164; von Heinegg, op. cit., p. 147. See also Haslam, op. cit., p. 171.

[7] A recent restatement in treaty law is to be found in Art. 35 (1) of AP I.

[8] For a description of different approaches see Haslam, op. cit., pp. 166 et seq.; Michael N. Schmitt, Wired Warfare: Computer network attack and jus in bello, International Review of the Red Cross, No. 846, 2002, pp. 370 et seq.

shot suffices to trigger an *international armed conflict.* Such conflict can therefore be of very short duration.[9] This view is however not generally shared. Some require a minimum threshold of intensity or time.[10] The latter approach may lead to the need for evaluations and result in inevitable uncertainties which would be detrimental to the protection of victims of conflicts.[11]

Whether CNA alone will ever be seen as amounting to an armed conflict will probably be determined in a definite manner only through future state practice. There are strong arguments in favour of the applicability of IHL in situations when a CNA is intended to or does result in physical injury to persons, or damage to objects that goes beyond the computer program or data attacked. It might also depend on the degree of damage that a computer network attack causes - the greater the damage, the more likely the situation will be treated as an armed conflict.[12] In the case of IHL, the motivation for the application of the law is to limit the damage and provide care for the casualties. This would militate in favour of an expansive interpretation of when IHL begins to apply.

In any case, it is required that a CNA is undertaken by state organs or can otherwise be attributed to a State in accordance with international rules on State responsibility. This cannot be limited to acts committed by members of the State armed forces but must apply also to conduct of other persons acting on behalf or as agents of a State (for example civilians acting instead of the State armed forces).[13]

2. Do the rules giving effect to the principle of distinction apply to CNA and how should they be applied?

The definition of the term “attack” is of decisive importance for the application of the various rules giving effect to the principle of distinction and for most of the rules providing special protection for certain objects. It should be borne in mind that AP I and customary IHL contain a specific definition of the term which is not identical to that provided for in other branches of law.

In accordance with Art. 49 (1) of AP I "Attacks" means acts of violence against the adversary, whether in offence or in defence.

---

[9] Jean S. Pictet (ed.), Commentary: IV Geneva Convention relative to the Protection of Civilian Persons in Time of War, ICRC, 1958, pp. 20 et seq., 59 ("as soon as the first acts of violence were committed, even if the armed struggle did not continue"). If one follows the case law of the ICTY and ICTR, a different standard would apply to non-international armed conflicts: a non-international armed conflict "exists whenever there is [...] *protracted* armed violence between governmental authorities and organized armed groups or between such groups within a State" (emphasis added), ICTY Appeals Chamber, Decision on the defence motion for interlocutory appeal on jurisdiction, *The Prosecutor v. Dusko Tadic*, IT-94-1-AR72, para. 70. This finding is also cited in ICTR, Judgement, *The Prosecutor v. Jean Paul Akayesu*, ICTR-96-4-T, para. 619.

[10] Michael N. Schmitt, Wired Warfare, op. cit., p. 372 with further references.

[11] Doswald-Beck, op. cit., p. 164. See also Haslam, op. cit., p. 171.

[12] Doswald-Beck, op. cit., p. 165. See also Michael N. Schmitt, Wired Warfare, op. cit., pp. 373-375; Greenberg/Goodman/Soo Hoo, op. cit., p. 15.

[13] See also Michael N. Schmitt/Heather A. Harrison Dinniss/Thomas C. Wingfield, Computers and War: The Legal Battlespace, http://www.ihlresearch.org/ihl/pdfs/schmittetal.pdf, p. 4.

Bothe/Partsch/Solf in their commentary to AP I point out that the term "acts of violence" denotes physical force. Thus, the concept of "attacks" excludes dissemination of propaganda, embargoes or other non-physical means of psychological, political or economic warfare.[14]

Based on that understanding and distinction, CNA through viruses, worms, logic bombs etc. that result in physical damage to persons, or damage to objects that goes beyond the computer program or data attacked can be qualified as "acts of violence" and thus as an attack in the sense of IHL.[15] Given that elsewhere in the same section of AP I, namely in the definition of a military objective, reference is made to neutralization of an object as a possible result of an attack, one may conclude that the mere disabling of an object, such as shutting down of the electricity grid, without destroying it should be qualified as an attack as well.[16]

It is also helpful to look at how the concept of attack is applied to other means and methods of warfare. There is general agreement that, for example, the employment of biological or chemical agents that does not cause a physical explosion, such as the use of asphyxiating or poisonous gases, would constitute an attack.[17]

If one admits that CNA constitute an attack, AP I imposes

- the obligation to direct attacks only against "military objectives"; and not to attack civilians or civilian objects;[18]
- the prohibition of indiscriminate attacks, including attacks that may be expected to cause excessive incidental civilian casualties or damages;[19]
- the requirement to take the necessary precautions to ensure that the previous two rules are respected,[20] in particular the requirement to minimise incidental civilian damage and the obligation to abstain from attacks if such damage is likely to be excessive to the value of the military objective to be attacked;[21]

---

[14] Michael Bothe/Karl Josef Partsch/Waldemar A. Solf, New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949, 1982, p. 289. Busutil uses as a criterion that actions are taken against the will of the 'target' and concludes that a CNA would qualify as an attack in the sense of AP I, James A. Busutil, A Taste of Armageddon: The Law of Armed Conflict as Applied to Cyberwar, in: The Reality of International Law, p. 48.

[15] Torsten Stein/Thilo Marauhn, Völkerrechtliche Aspekte von Informationsoperationen, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht, 69/1, 2000, p. 35, requiring that the use of CNA is not limited to causing inconveniences, but causes danger for life and limb. Michael N. Schmitt, Wired Warfare, op. cit., pp. 377 et seq. See also Department of Defense, Office of General Council, An Assessment of International Legal Issues in Information Operations, May 1999, www.infowar.com/info_ops/info_ops_061599a_j.shtml (last checked 9.11.1999), under B. Application to Information Operations, pp. 10 et seq., stating however: "The extent to which force can be used for purely psychological purposes, such as shutting down a civilian radio station for the sole purpose of undermining the morale of the civilian population, is an issue that has yet to be addressed authoritatively by the international community."

[16] See also Bothe/Partsch/Solf, op. cit., p. 289: "denying the use of an object to the enemy without necessarily destroying it"; this points into the direction that no further consequences are required.

[17] See also Haslam, op. cit., p. 170; Michael N. Schmitt, Wired Warfare, op. cit., pp. 374 et seq., both in the context of analysing the use of which type of weapons would constitute an international armed conflict.

[18] Arts. 48, 51 (2), 52 of AP I.

[19] Art. 51 (4), (5) of AP I.

[20] Art. 57 of AP I.

[21] Arts. 51 (5)(b), 57 (2)(a)(ii) and (iii) of AP I.

These rules operate in exactly the same way whether the attack is carried out using traditional weapons or through CNA.[22] Problems that arise in applying these rules are therefore not necessarily unique to CNA. They are more related to the interpretation of, for example, what constitutes a military objective or which collateral damage would be excessive.

Some points merit to be emphasised:

a) The prohibition of indiscriminate attacks

IHL prohibits indiscriminate attacks. In accordance with Art. 51 (4) of AP I, an indiscriminate attack is defined as one which is either not aimed at a specific military objective (through carelessness or use of weapons that are by nature not capable of being so directed)[23] or because the effects of an attack on a military objective are uncontrollable and unpredictable.[24]

Based on what has been made public so far on CNA, this might potentially be the most serious problem.[25] The question arises immediately how a CNA could be aimed accurately at the intended target and, even if one is capable of doing this, not at the same time create a magnitude of unforeseen and unforeseeable effects upon civilian infrastructure? An obvious example would be the release of a virus or a range of viruses into the computer systems of a target State. Even if introduced only into the military network of a State, if the virus is virulent enough, it would soon seep out of that network and into civilian systems of the targeted State or even beyond to neutral or friendly States.[26] This problem is due to the fact that civilian and military computer networks are in practice highly interconnected. Such viruses must most likely be considered as indiscriminate because they cannot be directed against a specific military objective, and they would be a means or method of combat the effects of which cannot be limited as required by AP I.[27]

b) Does CNA allow the targeting of a broader range of objects?

In literature it is sometimes claimed that the use of CNA expands the range of legitimate targets because it enables attacks with reversible effects against otherwise prohibited objects.[28] If this claim implies that an attack against a civilian object may be considered lawful if the attack does not result in destruction or if its effects are reversible, this claim is unfounded under existing law.[29]

Attacks may only be directed at military objectives.[30] Objects not fulfilling the definition of a military objective are civilian and may not be attacked. The definition of military objectives is not dependent on the method of warfare used. It applies in the same way to kinetic and non-

---

[22] Stein/Marauhn, op. cit., p. 35; Haslam, op. cit., p. 172; Department of Defense, Office of General Council, op. cit., under B. Application to Information Operations, pp. 10 et seq.
[23] Art. 51 (4)(a) and (b) of AP I.
[24] Art. 51 (4)(c) of AP I.
[25] For example Lawrence T. Greenberg/Seymour E. Goodman/Kevin J. Soo Hoo, Information Warfare and International Law, 1998, p. 12.
[26] Busutil, op. cit., p. 52. See also Department of Defense, Office of General Council, op. cit., under B. Application to Information Operations, pp. 10 et seq.
[27] Busutil, op. cit., p. 52; Michael N. Schmitt, Wired Warfare, op. cit., p. 389.
[28] For example, Mark R. Shulman, Discrimination in the Laws of Information Warfare, Columbia Journal of Transnational Law 1999, pp. 961, 963, 964.
[29] See also Haslam, op. cit., pp. 173 et seq.
[30] See Art. 52 (2) of AP I: "Attacks shall be limited strictly to military objectives."

kinetic means. The fact that CNA does not lead to the destruction of the object attacked is irrelevant. In accordance with Art. 52 (2) of AP I only those objects, which make an effective contribution to military action and whose total or partial destruction, capture or neutralization offers a definite military advantage, may be attacked. By referring not only to destruction or capture of the object but also to its neutralization the definition implies that it is irrelevant whether an object is disabled through destruction or in any other way.

However, certain attacks against military targets executed with kinetic weapons, which would be unlawful because they may be expected to cause excessive incidental civilian damage or casualties, may be lawful if conducted by way of CNA. If a CNA is capable of avoiding or minimizing civilian death or injury inside of or in the vicinity of a military objective, the incidental damage or casualties may under the circumstances not outweigh the military advantage anticipated from the attack.[31]

c) Precautions in attack

The availability of the option to use CNA may also have some implication on one specific precaution that Art. 57 of AP I requires to be taken in case of an attack, namely the obligation to take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental civilian casualties and damages.[32] This rule would require that a commander should consider whether he or she can achieve the same military advantage by using CNA if this is practicable and would cause less civilian casualties or damage compared to a use of more conventional weapons. However, it may be difficult in practice to anticipate all the reverberating consequences/knock-on effects of CNA.

3. What prohibitions or limitations to CNA follow from rules giving special protection to certain objects?

IHL contains special protections against attacks for particular objects, which today can be highly dependent on computer control.

Medical facilities and establishments are protected by various provisions of the GC and the two APs. For example, Art. 19 of GC I covers military medical units and establishments, such as hospitals; Art. 18 of GC IV specifically addresses civilian hospitals, and Art 12 of AP I applies to civilian and military medical units, again including hospitals.

These facilities may in no circumstances be attacked and must at all times be respected and protected. The notion of attack has been discussed before. Under this term, shutting down of an electricity generating system exclusively used by a hospital through CNA would be prohibited as well as corruption of a medical database, for example, causing civilians or wounded soldiers to receive transfusions of an incorrect blood type.[33] As pointed out in the ICRC Commentary to these provisions the obligation "to respect" the mentioned facilities means, first of all, not to attack them or harm them in any way. To respect such units means, secondly, not to interfere with their work. It is not enough for the enemy simply to refrain from taking action against them; he must also allow them to continue to give treatment to the

[31] See also Shulman, op. cit., pp. 961 et seq.
[32] Art. 57 (2)(a)(ii) of AP I.
[33] Greenberg/Goodman/Soo Hoo, op. cit., p. 12. A similar example is given by William Church, Information Warfare, International Review of the Red Cross, No. 837, 2000, p. 212.

wounded in their care, as long as this is necessary.[34] The term “to respect” thus prohibits a broader range of manipulations of data than what is implied by the prohibition of attacks. One could imagine manipulation of patients' data, which would render more difficult their treatment. It should be stressed that protection of these facilities only ceases if they are used to commit, outside their humanitarian activities, acts harmful to the enemy.[35]

The rules on the protection of medical aircraft[36] and hospital ships[37] as well are drafted in a way as to be applicable to CNA. We find again the terms “not be attacked” and “must at all times be respected and protected”.

Among targets, which are likely to be object of CNA, are installations such as drinking water pipeline systems, purification plants and crop irrigation systems. CNA against these objects might involve giving incorrect commands as to the length of the purification cycle, the amounts and composition of chemicals to add to the water supply.[38] Such CNA may fall under the scope of Art. 54 of AP I. This provision prohibits to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as food-stuffs, agricultural areas for the production of food-stuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for their sustenance value to the civilian population or to the adverse Party, whatever the motive, whether in order to starve out civilians, to cause them to move away, or for any other motive.

The term “attack” as contained in this provision has the same meaning as described before. The term “render useless” is even more encompassing and may cover a broader range of manipulating activities than those described by the term “attack”.[39] Whether a particular CNA has violated the rule depends on whether the further conditions of that Article are met.

Dams and power plants, sometimes also dykes are highly dependent on computer control. Manipulation of these systems by way of CNA may cause the release of dangerous forces and cause severe damage to the civilian population. Such a scenario is specifically addressed in Art. 56 of AP I. It states in its essential part that:

> *"Works or installations containing dangerous forces, namely dams, dykes and nuclear electrical generating stations, shall not be made the object of attack, even where these objects are military objectives, if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population."*

This prohibition is independent of the type of weapons or methods of warfare used. It would therefore also cover attacks effected by means of CNA, for example manipulation of the computer system of a dam which leads to opening the floodgates, if this may cause severe losses among the civilian population.

---

[34] Jean S. Pictet (ed.), *Commentary: I Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field*, ICRC, Geneva, 1952, p. 196.
[35] E.g. Art. 21 of GC I, Art. 19 of GC IV.
[36] Art. 36 of GC I, Art. 24 of AP I.
[37] Art. 22 of GC II, Art. 22 of AP I.
[38] Busutil, op. cit., p. 53, with further examples.
[39] Claude Pilloud/Jean S. Pictet, in Yves Sandoz/Christophe Swinarski/Bruno Zimmermann (eds), Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, ICRC, Geneva, 1987, no. 2101.

In the case when a nuclear electrical generating station constitutes a military objective, it could be attacked by means of CNA if the CNA only neutralizes the object without releasing dangerous forces in a way described by AP I.[40] However, if the nuclear electrical generating station does not constitute a military objective in the sense of Art. 52 (2) of AP I, it may not even be the object of a CNA which only disables – even temporarily – without causing the release of dangerous forces.[41]

For the sake of completeness, but without going into the details, it should be kept in mind that Art. 56 of AP I also provides for loss of protection against attack of these objects under very specific circumstances, but requires as well that all practical precautions must be taken to avoid the release of the dangerous forces.

A last rule of protection that may be relevant to CNA is Art. 55 of AP I, which provides that

> *"Care shall be taken in warfare to protect the natural environment against widespread, long-term and severe damage. This protection includes a prohibition of the use of methods or means of warfare which are intended or may be expected to cause such damage to the natural environment and thereby to prejudice the health or survival of the population."*

It is not inconceivable that, for example, a CNA on a control system of a chemical factory may cause the release of poisonous gases and cause important damage to the environment; or an attack on pharmaceutical plants or oil refineries could release toxic substances into the atmosphere. However, while it cannot be excluded, the high threshold of "widespread, long-term and severe damage" will not bring the vast majority of CNA within the scope of the prohibition under Art. 55 of AP I.

4. What activities of civilians relating to CNA constitute direct participation in hostilities and cause them to lose their protection against direct attack?

The concept of direct participation in hostilities determines under which circumstances civilians lose their protection against attack.[42] This concept is of particular importance also in the context of CNA. There is a strong likelihood that civilians will be involved in CNA often due to their specific technical expertise, which members of the armed forces may not necessarily have. This involvement can take a variety of forms: for example civilians may be those who launch a CNA or they are used to maintain the computers or computer network from which a CNA is or may be launched. The question therefore arises what conduct would qualify as direct participation in hostilities and make these persons lose protection from attack. Unfortunately, the interpretation of the concept of direct participation is not entirely clear. Therefore, the ICRC decided in 2003 to start a process of clarification of that concept through both meetings of experts and independent research by the ICRC and selected experts.

---

[40] See also Stein/ Marauhn, op. cit., p. 35; Busutil, op. cit., p. 54; Michael N. Schmitt, Wired Warfare, op. cit., p. 385. For a similar example see Shulman, op. cit., p. 962.

[41] Pilloud/Pictet, in Sandoz/Swinarski/Zimmermann (eds), op. cit., no. 2153; Bothe/Partsch/Solf, op. cit., p. 353.

[42] Such persons remain civilians as evidenced by the interplay between Arts. 50 (1) and 51 (3) of AP I. In addition, the loss of protection is limited to attacks for the time of their direct participation. Once in the hands of the enemy, such person are protected as civilians under GC IV, to the extent that they fulfil the conditions as set out in Art. 4 of that Convention, and/or the fundamental guarantees as contained in Art. 75 of AP I, which reflects customary international law. For further detail see Knut Dörmann, The legal situation of "unlawful/unprivileged combatants", International Review of the Red Cross No. 849, pp. 45-74.

The two expert meetings held so far were co-organized with the TMC Asser Institute in The Hague. The primary aim of this process is to try to formulate guidelines for the interpretation or even a generic definition of the notion of ‘direct participation in hostilities’. As many participants expressed the opinion during the first meeting that further clarification of the notion of "direct participation" would be facilitated by a discussion of concrete examples, the ICRC submitted a questionnaire to the participants for the second expert meeting in October 2004. While not addressing all aspects of CNA, some examples chosen for the questionnaire had a direct link to the use of CNA.

First, we asked whether the causing of damage to or interfering with a computer network by way of a CNA as a form of "direct application of electronic or other means of destruction or injury with the aim of diminishing the military capacity of an adversary" would constitute a direct participation.

A clear majority of experts considered the use of electronic means, as well as CAN, to constitute direct participation in hostilities (14 experts "yes", 1 "no"; 4 "n/a"). One expert required that computer network attacks qualifying as direct participation in hostilities must *result* in death, injury or physical damage, whereas another expert required that the CNA be carried out deliberately. Finally, one expert contended that the question of qualification of CNA as direct participation in hostilities was not settled at this time and depended on the situation.

Second, with regard to "delayed, indirect or remote controlled application of electronic means of destruction or injury with the aim of diminishing the military capacity of an adversary", the electronic interference with weapons systems, means of communication, means and ways of transportation, electronic networks used by the adversary for military operations was considered to constitute direct participation in hostilities by almost all experts responding. One expert contended the contrary and there were between three and four abstentions. One expert required that direct participation in hostilities through "electronic" or "any other" means must result in death, injury or physical damage.

Gathering intelligence through an unauthorized access to a computer network used by an adversary, which is probably not covered by the definition of CNA, was a rather controversial example. Nine experts considered such activity to constitute direct participation in hostilities (with 6 "no"; 4 "n/a").

On the other end of the spectrum covering support activities, maintenance of military computer programs was considered by a clear majority of experts as not constituting direct participation in hostilities (12 "no", 2 "yes", 5 "n/a").

The responses received demonstrate certain tendencies, sometimes very clear ones: while executing CNA is widely considered as constituting direct participation in hostilities, maintenance work for computer networks, even of military nature, was not. It must be noted however that not all experts responded and no substantive discussion of these specific situations took place during the last meeting. It is our intention to continue this work at least over the next two years.

5. Must the defender fulfil specific requirements in order to comply with its obligation to take precautions against attacks?

It is evident that the dual-use of many telecommunications networks may further exacerbate the difficulty in distinguishing between military and civilian systems and, consequently, between military targets, which are lawful targets, and civilian targets, which may not be the object of an attack. In this context, one might question whether the obligation of States parties to AP I under its Art. 58 to remove, to the maximum extent feasible, civilian objects under their control from the vicinity of military objectives and to take the other necessary precautions to protect the civilian population and civilian objects under their control against the dangers resulting from military operations, would require that military and civilian computer networks are separated, if technically feasible.[43] The actual trend goes however in the opposite direction.[44] In any case, military planners should not forget that use of civilian networks for military purposes may render such networks lawful targets[45] – not just by CNA, but also by more conventional means.

6. Do specific prohibitions of methods of warfare, such as the prohibition of perfidy or of improper use of protected emblems, signs and signals, apply to CNA and, if so, in which way?

The use of computers provides new avenues for practising ruses of war,[46] which are lawful tactics under IHL. Ruses are defined as acts which are intended to mislead an adversary or to induce him to act recklessly but which infringe no rule of international law applicable in armed conflict and which are not perfidious. Examples of ruses are the use of camouflage, decoys, mock operations and misinformation.[47] The more cyber counterintelligence or, as it was previously called, computer network exploitation is undertaken, the more likely it is that misinformation will be deliberately planted to confuse the adversary. Such misinformation about one's own military plans is lawful and is no different in principle to any other vehicle for misinformation.[48] Planting inaccurate information into the enemy's data in order to mislead him would be no different. As follows from traditional sources, ruses of war need not be limited to creating misinformation about oneself.[49]

As with all ruses of war, misinformation or deception must not cross the line into perfidy. Perfidy is defined as "acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence".[50] AP I mentions the following acts as examples of perfidy:

> (a) the feigning of an intent to negotiate under a flag of truce or of a surrender;
> (b) the feigning of an incapacitation by wounds or sickness;
> (c) the feigning of civilian, non-combatant status; and
> (d) the feigning of protected status by the use of signs, emblems or uniforms of the United Nations or of neutral or other States not Parties to the conflict.

---

[43] Von Heinegg, op. cit., p. 147.
[44] Shulman, op. cit., p. 963; Greenberg/Goodman/Soo Hoo, op. cit., p. 12.
[45] Stein/Marauhn, op. cit., p. 35; Department of Defense, Office of General Council, op. cit., under B. Application to Information Operations, pp. 10 et seq.
[46] Doswald-Beck, op. cit., p. 171; Michael N. Schmitt, Wired Warfare, op. cit., p. 395.
[47] Art. 37 (2) of AP I.
[48] Michael N. Schmitt, Wired Warfare, op. cit., p. 395.
[49] Doswald-Beck, op. cit., p. 171.
[50] Art. 37 (1) AP I.

Therefore, misinformation implicating protected persons or objects would be unlawful. For example, manipulating enemy visual, sensing, or other information systems so that enemy forces wrongly believe that the forces of the opponent are surrendering would be perfidious,[51] as would causing them to believe that combat vehicles of the opponent were medical vehicles or those of neutrals.[52] Manipulating the enemy's targeting database so that it is believed that one's own division headquarters were a hospital could also constitute perfidious behaviour.[53] Another example would be “morphing” techniques to create an image of the enemy’s chief of state informing his troops that an armistice or cease-fire agreement had been signed.[54]

In terms of AP I, only the killing, injuring or capturing of an adversary by resort to perfidy is prohibited.

It is questionable whether intrusion of a computer network system through, for example, a firewall could qualify as feigning non-combatant status if the origin of the data is not identifiable by the firewall as a military source or if the impression is created that the data comes from a civilian institution. While one may be inclined to assimilate this with perfidy, at first sight the definition of perfidy in AP I seems to exclude such an interpretation since the act itself does not betray the confidence of a person. First, it is rather the system protecting a computer and not a person that will be "betrayed".[55] However, one could also focus on the person that controls or develops the system. Second, the system probably does not allow entrance based on international legal protections that must be granted.[56] However, what about a situation, where a virus is sent with an email from a seemingly "innocent" sender to a military headquarters and the recipient opens the mail because he or she believes that it does not come from an enemy military source and as consequence the virus seeps into the network? This scenario looks much more like perfidy in the traditional sense.

Feigning an identity through electronic means may be prohibited under other provisions of AP I. A few examples are provided:

Art. 38 of AP I prohibits *inter alia* to make improper use of the distinctive emblem of the red cross, red crescent or red lion and sun or of other emblems, signs or signals provided for by the Geneva Conventions or by Additional Protocol I.

The term signals refers to technical means of identification for medical transports and units as contained in Annex I to Additional Protocol I, such as radio codes and signals or the Secondary Surveillance Radar system, the use of which is regulated by the International Telecommunication Union, the International Civil Aviation Organization and the International Maritime Organization. If such signals are used for other purposes than those foreseen under IHL that would constitute an improper use and is absolutely prohibited. Albeit technically not falling under the definition of CNA, feigning protected status as medical transports and units by transmitting false signals to the enemy even without fulfilling the additional conditions of perfidy would therefore be in violation of Art. 38 of AP I.

---

[51] Greenberg/Goodman/Soo Hoo, op. cit., p. 13; Stein/ Marauhn, op. cit., p. 34.
[52] Greenberg/Goodman/Soo Hoo, op. cit., p. 13. A similar example is given in Department of Defense, Office of General Council, op. cit., under B. Application to Information Operations, pp. 10 et seq.
[53] Greenberg/Goodman/Soo Hoo, op. cit., p. 13.
[54] Department of Defense, Office of General Council, op. cit., under B. Application to Information Operations, pp. 10 et seq.; Michael N. Schmitt, Wired Warfare, op. cit., pp. 395 et seq.
[55] Busutil, op. cit., p. 49.
[56] Busutil, op. cit., p. 49.

It is debatable whether intrusion into an enemy computer system by feigning that the intrusion or the data sent emanates from, for example, a medical unit or the ICRC would fall under this prohibition. The argument that it does could be made, in particular since the prohibition does not require the betrayal of confidence of a person.

Similar considerations[57] may be made as to the prohibition

- to make use of the distinctive emblem of the United Nations, except as authorized by that Organization.
- to make use in an armed conflict of the flags or military emblems, insignia or uniforms of neutral or other States not Parties to the conflict.
- to make use of the flags or military emblems, insignia or uniforms of adverse Parties while engaging in attacks or in order to shield, favour, protect or impede military operations.

The ordinary meaning of these provisions could preclude that improper use of other means of identification than the uniform, insignia or emblem would fall under the prohibitions.

Despite the narrow wording it has been suggested in literature that any computer-generated attack cannot be undertaken whilst giving the impression that it is coming from the adversary's own side. This would be the equivalent to attacking wearing the enemy's uniform, which is clearly unlawful under existing IHL.[58] While the rationale of this reasoning is very convincing, some doubts remain.[59]

7. Conclusions

Despite the newness of both the technology of Computer Network Attacks and the evolving concepts for its employment, legal constraints apply to it. There is no provision of IHL that explicitly outlaws computer network attacks. It is clear however that CNA may only be undertaken to the degree and in a way which respects existing law. The most relevant provisions are based on and are a consequence of the principle of distinction. Rules providing special protection to certain objects impose important limitations as well. Certain uses, such as CNA directed at civilian objects, would not only be violations of IHL, but also amount to war crimes.[60]

After technical analysis, it must be properly assessed, whether certain types of actions (for example, the introduction of worm viruses) would be inherently indiscriminate. If so, such techniques would be automatically illegal weapons and thus be banned as such. In this context it should be remembered that in accordance with AP I in the study, development or adoption of a new weapon or method of warfare, States are under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by any rule of international law applicable to the State. Given that the formulation of the rules in AP I on the conduct of hostilities are crafted in rather general terms, this has to be done very meticulously.

[57] See for example Busutil, op. cit., p. 49.
[58] Doswald-Beck, op. cit., p. 171; Church, op. cit., p. 212.
[59] Greenberg/ Goodman/Soo Hoo, op. cit., p. 13. Stein/Marauhn, op. cit., p. 34, qualifying such conduct as a lawful ruse or psychological warfare.
[60] See Art. 8 (2)(b)(ii) of the ICC Statute.