Artigo recebido em agosto de 2013 e aceite para publicação em outubro de 2013

'NOVAS ARMAS, NOVA LEI?': ENSAIO SOBRE A APLICAÇÃO DO DIREITO INTERNACIONAL HUMANITÁRIO À 'GUERRA CIBERNÉTICA'

A Problemática do Princípio da Distinção num Mundo Interconectado

'NEW WEAPONS, NEW LAW?': ESSAY ON THE APPLICATION OF IHL TO CYBER WARFARE AND THE PROBLEMATIC OF THE PRINCIPLE OF DISTINCTION

The Problematic of the Principle of Distinction in an Interconnected World

Joana Oliveira Rodrigues de Freitas
Licenciada e Mestre em Direito pela Universidade Católica do Porto
Lisboa, Portugal
f_joana@hotmail.com

Resumo

A questão iminente da segurança cibernética levanta relevantes problemáticas legais cuja solução urge. Tendo por objeto a regulação de ataques cibernéticos levados a cabo por forças governamentais durante um conflito armado internacional (e como tal, deixando de parte questões relevantes como a da atribuição, atores não estaduais e criminalidade cibernética, em tempo de paz) o presente artigo propõe demonstrar, à luz do basilar princípio da distinção e os princípios corolários da discriminação, proporcionalidade e precaução, que o atual Direito Internacional Humanitário é passível de ser aplicado aos ataques cibernéticos, através da analogia e das normas de interpretação. No que toca ao princípio da distinção e seus corolários, a aplicação do DIH é problemática surgindo questões complexas relacionadas com, inter alia, a problemática dos civis que tomam parte nas hostilidades, os ataques a objetos com uma função concomitantemente civil e militar e a objetos que contêm forças perigosas (e.g., barragens, centrais nucleares, etc.). Defende-se, porém, neste artigo, que mesmo estes problemas podem ser resolvidos pela lei atualmente existente, sem necessidade de se criar nova lei. Ainda, o presente artigo faz uma análise comparativa das normas convencionais existentes com o recente Manual de Tallinn sobre a regulação dos ataques cibernéticos.

Palavras-chave: direito internacional humanitário; ataques cibernéticos; princípio da distinção; ataques indiscriminados; proporcionalidade; Manual de Tallinn.

Como citar este artigo: Freitas, J., 2013. "Novas Armas. Nova Lei?": Ensaio sobre a Aplicação do Direito Internacional Humanitário à Guerra Cibernética. Revista de Ciências Militares [em linha], Vol. I, N.º 2, novembro 2013, pp 49-67. Disponível em: http://www.iesm.pt/s/index.php?option=com_content&view=article&id=719&Itemid=164

Abstract

The imminent concern for cyber security raises relevant legal issues urging for a solution. The object of the present article is the regulation of cyber-attacks perpetrated by governmental forces during an international armed conflict (and thus leaving aside relevant questions relating to attribution, non-state actors, cyber operations that stand below the violence threshold and cyber criminality during peace-time) and its goal is to demonstrate how, in light of the principle of distinction (and its corollary principles of discrimination, proportionality and precaution), the current IHL might well apply through analogy and the rules of interpretation, to cyber-attacks. However, the application of current IHL raises distinction-related difficulties, such as the definition of civilians taking a direct part in the hostilities, dual-use objects, and objects containing dangerous forces (such as dams and nuclear reactors). Nevertheless, it is argued that current IHL is capable of tackling these more problematic issues and hence there is no need to attend the calls for lege ferenda. Finally, the present article puts forward a comparative analysis of the existing treaty law with the recently released Tallinn Manual addressing cyber security.

Keywords: International Humanitarian Law; cyber-attacks; principle of distinction; indiscriminate attacks; proportionality; Tallinn Manual.

I. Introduction

'So cyberspace is real. And so are the risks that come with it'. The words of the incumbent US President Barack Obama, and the language of several General Assembly resolutions, alerting for the risks that the misuse of information technology may pose to international peace and security, clearly reflect today's concern about cyber security[1].

The present article, dealing with both the risks and the benefits of the increasing number of cyber operations during an international armed conflict[2], will probe how the existing International Humanitarian Law (IHL)[3], in particular the principle of distinction and its corollaries, the principle of proportionality and the principle of precaution, apply to the reality of cyber warfare, rejecting the calls of lege ferenda. In other words, the present article will probe how the current body of IHL, by way of analogy and interpretation, is adequate to regulate cyber-attacks during an armed conflict and provide guidance to practitioners in the conduct of military operations, rejecting the calls for the drafting of a comprehensive treaty to regulate cyber warfare, on the one hand, and for the development of the law through custom, on the other.

---

[1] See for example the Preamble of the Resolution A/RES/55/63 of 4 December 2000, and the Resolutions A/RES/56/12 of 18 December 2001, A/RES/58/32 of 8 December 2003, A/RES/63/37 of 2 December 2008, A/RES/64/25 of 2 December 2009.

[2] One can think of cyber operations (whose qualification as attack, for the purposes of IHL, needs further analysis) perpetrated during the former 1999 Yugoslavia NATO's intervention; the recent (2008) Georgia-Russia war; the second Chechen war with Russia; and the targeting of Israeli governmental websites during the 2009 Operation Cast Lead. Other operations such as the recent alleged Chinese attacks on US cyber facilities fall out of the scope of the present article since they were perpetrated outside the context of an armed conflict.

[3] IHL, also known as the Law of Armed Conflict or jus in bello, is the branch of law that regulates international and non-international armed conflicts.

Cyber warfare raises several jus ad bellum (i.e., the right to engage in war, which is regulated in the Charter of the United Nations) questions that will not be dealt with here, such as whether an act may be considered an attack capable of commencing a war. Nevertheless, one should not forget that the application of IHL to cyber warfare depends on those jus ad bellum considerations, namely, whether a cyber-attack constitutes an armed attack for the purposes of the UN Charter or whether an exclusively cyber war exists at all.

Thereby, after a semantic clarification and an assessment of the applicable body of law, in Part I (sections A and B, respectively), the present article will analyse when a cyber-operation constitutes an 'attack', i.e., generally, when does a cyber-operation reach the necessary threshold to trigger the application of IHL. Subsequently, in Part II, this article will inspect the particular application of the fundamental principle of distinction to cyber warfare, and the questions it entails: the definition of military objectives and the problematic of dual-use objects; the definition of civilians and the problematic of civilians taking direct part in (cyber) hostilities; the prohibition of indiscriminate cyber-attacks and the concomitant principle of proportionality.

Finally, throughout the present article reference will be made to the recently released draft manual on the applicable law to cyber warfare. The Tallinn Manual on the International Law Applicable to Cyber Warfare was prepared at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). This work is "intended to lead to a restatement and manual on the international law applicable to cyber warfare"[4], and means to reflect customary international law, which is to say law applicable to all states[5]. Notably, the Manual does not address cyber operations below the use of force threshold nor cyber criminality (cf. the Manual's Introduction, 4) in peace-time. Further, its focus is on armed conflicts proper, i.e., 'armed hostilities that may include or be limited to cyber operations' (Rules 22 and 23).

Despite its undeniable importance – the 'teachings of the most highly qualified publicists' constitute a secondary source of International Law as stated in Article 38(d) of the Statute of the International Court of Justice (ICJ), which, as commonly accepted, enumerates the sources of international law – to commit to paper more than a perfunctory reference to the Manual is, in our view, superfluous due to its precocity and the consequent lack of official comments, on which to rely. Finally, it is worth mentioning that the Tallinn Manual does not reflect NATO's or any State's position (although it was sponsored by NATO): it is 'an expression solely of the

[4] Cf. a version of the Tallinn Manual available at http://www.ccdcoe.org/249.html (last visit 20 October 2013). Also, for a critical view of the Manual see D. Fleck, "Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual", (2013) available at http://jcsl.oxfordjournals.org.ezproxy.leidenuniv.nl:2048/content/18/2/331.full.pdf (last visit 20 October 2013).

[5] The question of whether or not customary international law applies to non-state actors, like terrorist groups, private security forces, autonomous regions, etc., will not be dealt in the present article due to the lack of space although we recognize its imminent importance since the ability of these smaller and less organized groups to use cyber weapons and perpetrate cyber-attacks whose graveness might trigger the application of IHL is just a matter of time. For literature dealing with the problematic of non-state actors see, inter alia, T. Meron, "Improving Compliance by Non-State Actors with Obligations in International Humanitarian Law: A Global Responsibility" (2011); G. S. Corn, "Thinking the unthinkable: has the time come to offer combatant immunity to non-state actors?" (2011); C. Waxman, "Temporality and Terrorism in International Humanitarian Law" (2011). For a critical overview of the difficulties of ascertaining customary international humanitarian law see H. Parks, "Perspective and the Importance of History" (2011).

opinions of the International Group of Experts, all acting in their private capacity' (cf. The Manual's Introduction, p. 11 and Fleck, 2013, p. 336).

A. Semantic Clarification

Thus far, as it can be easily demonstrated, International Law has not yet provided for an authoritative definition of cyber war, cyber warfare or cyber-attacks (Melzer 2011b, p. 22). These terms – all related to the conduct of armed conflict – come under the chapeau of a much broader concept, i.e., cyber operations or information operations. These operations are the 'integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security (…) to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own.' (US National Military Strategy for Cyberspace Operations, 2006). Within this concept, highlight must be made to 'computer network operations' (CNO), which entail, inter alia, 'computer network attacks' (CNA) – the object of the present article[6].

Generally, there is a CNA whenever a CNO aims at the destruction or modification of information contained in the adversary's computer network, in order to weaken the adversary's communication system and/or causing damage that extrapolates from the targeted network. The most common means of such performance are Trojan horses, viruses, worms and logic bombs, which can cause the disruption of software, hardware or simply a denial of service (by overloading the network with information), in the adversary's computers or computer networks (cf. Roscini, 2010, pp. 91-3). Notably, the Manual on International Law Applicable to Air and Missile Warfare elaborated within the Program on Humanitarian Policy and Conflict Research of Harvard University adds to this definition of CNA the manipulation of computer information and the aim to 'gain control over the computer or computer network' (HPCR, 2009, p. 3)[7].

B. Applicable Law

IHL is the body of law applicable to (international and non-international) armed conflicts, aiming to regulate the conduct of hostilities between the belligerent parties and concomitantly to protect the ones in need. Today's most relevant rules of IHL, are the 1907 IV Hague Convention: Respecting the Laws and Customs of War on Land, and its Annex: Regulations concerning the Laws and Customs of War on Land, the four 1949 Geneva Conventions and their two Additional Protocols, relating to the protection of victims in international and non-international armed conflicts, respectively[8]. Furthermore, there are several treaties regulating the use of certain

[6] For a more detailed and technical explanation of the different cyber and information operations see Roscini 2010; Melzer 2011b.

[7] Available at http://ihlresearch.org/amw/HPCR%20Manual.pdf, (last visit in 20 October 2013).

[8] International Committee of the Red Cross (ICRC): Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (First Geneva Convention), 12 August 1949, 75 UNTS 31,
Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (Second Geneva Convention), 12 August 1949, 75 UNTS 85; Geneva Convention Relative to the Treatment of Prisoners of War (Third Geneva Convention), 12 August 1949, 75 UNTS 135; Geneva Convention Relative to the Protection of Civilian Persons in Time of War (Fourth Geneva Convention), 12 August 1949, 75 UNTS 287. Also, the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol

weapons, such as the 1995 Protocol on Blinding Laser Weapons, the 1997 Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, the 1993 Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction. To complete the picture, there is a vast set of rules of customary IHL that have developed along the centuries of warfare[9].

The preliminary question of the present article is whether the existing legal framework suffices to accommodate and provide guidance to the new trends in warfare, in particular the recourse to high technological means, namely, cyber weapons. In the existing body of International Law, there is still no specific provision regarding cyber warfare, cyber operations or cyber-attacks, the simple reason being that, when those rules were drafted these concepts did not come to the mind of the drafters, for they were either irrelevant or inexistent (cf. Kodar, 2012, p. 109). However, this absence of specific provisions regarding cyber warfare is not tantamount to anarchy: from the Martens Clause (both the original and the modern versions)[10], the supra mentioned 1907 IV Hague Convention to the Protocol I, not only the belligerent parties have limited discretion to choose the methods or means of warfare (cf. the 1996 International Court of Justice Nuclear Weapons Advisory Opinion (paragraph 77), and article 22 of the IV Hague Convention and article 35 of Protocol I, stating that the right of the parties to choose methods or means of warfare is not unlimited), as they are also obliged to ascertain whether the use of a new weapon complies with the applicable existing IHL (cf. article 36 of Protocol I). This obligation is confirmed in Rule 48(a) of the Tallinn Manual. In other words, the existing rules may well be analogically applied to cyber warfare (for the same opinion see Kodar, 2012).

Some argue however that the absence of rules regulating cyber warfare works as a blank cheque for the belligerent parties to freely use cyber weapons (on this divergence cf. Kodar, 2012, pp. 109-110). The 'blank cheque' argument is similar to the one brought to the ICJ in Nuclear Weapons Advisory Opinion, which the Court ultimately rejected, by analogical recourse to the Martens Clause (cf. paragraphs 87 and 226-67).

Thus, most scholars[11] and some State representatives[12] defend that the existing legal framework, if applied by analogy, suffices to regulate and limit the use of cyber means and methods of warfare, which by no means exist in a legal void.

I), 8 June 1977, 1125 UNTS 3; and the 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, 1125 UNTS 609.

[9] Cf. the 2009 ICRC Study: Customary International Humanitarian Law, Volume I: Rules.

[10] The modern version of the Martens Clause is provisioned in Art. 1(2) of the Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), entered into force in 7 December 1978, 1125 UNTS 3, and states that whenever a situation is not covered by the laws of armed conflict *'civilians and combatants remain under the protection and authority of the principles of international law, derived from established custom, from the principles of humanity, and from the dictates of public conscience.'* The Martens Clause was written in the Preamble of the 1899 Hague Convention (II) with Respect to the Laws and Customs of War on Land (entered into force in 4 September 1900) and 1907 Hague Convention (IV) respecting the Laws and Customs of War on Land (entered into force in 1 January 1910). According to this Clause, there cannot exist a lacuna in IHL.

[11] Cf. Doswald-Beck, 2002, p. 176; Schmitt, 2002, pp. 368-70; Kodar, 2012, p. 110; Dinstein, 2012, p. 264; and Kelsey, 2007-2008, p. 1430.

[12] Cf. Kodar, 2012, p. 111, stating that in the past 2009 ICRC Conference on new challenges for IHL the majority of State representatives agreed that IHL 'is a sufficiently flexible tool that can overcome abstract challenges', including cyber warfare. Kodar writes that in the mentioned Conference the Permanent Representative of the Federal Republic of Germany to the United Nations, Ambassador Reinhard Schweppe, expressed the view that cyber warfare is a real issue, but LOAC can be applied to the problem and it can address the challenge.

Be that as it may, the complete lack of jurisprudence and opinio juris (Roscini 2010, p. 90; Fleck, 2013, p. 332) on the subject due to its early stage (although there is little State practice, as demonstrated by the examples provided throughout the present article) makes the study of cyber warfare regulation a very difficult exercise.

II. Cyber Warfare and IHL

A. Are CNA 'attacks' under IHL?

Having established that IHL applies to cyber warfare, the question now is when does it apply. Certainly, not in every case of cyber espionage, propaganda, or intrusions that, despite causing inconveniences, fall outside the scope of IHL. Hence, a graver threshold ought to be met, i.e., the attack threshold, for IHL to kick in.

Thereby, article 49(1) of Protocol I states that 'attack' is an 'act of violence against the adversary, whether in offence or in defence.' Nowadays, it is commonly accepted that a CNA, although non-kinetic in nature, may amount to an act of violence under the scope of IHL. According to Professor Schmitt's argument, the concept of attack should be read from the perspective of its consequences (Schmitt, 2002, pp. 374-5; 2011, p. 93). Accordingly, if a CNA is intended to, or it can foreseeably result either in death, injury or destruction, then it is considered an attack, pursuant to article 49(1), for its consequences meet the violence requirement (Schmitt, 2002, pp. 374-5; 2011, p. 93)[13]. Hence, below this threshold cyber operations against civilian networks are lawful. On the contrary, some authors (Dinniss, 2011, p. 196; Dörmann (ICRC), 2004, pp. 5-6) adduce different arguments leading to the idea that even cyber operations against civilian networks that do not reach the above mentioned violence requirement might be unlawful (on this divergence, cf. Fleck, 2013, pp. 340-1). These doctrinal divergences are contemplated in the Tallinn Manual (cf. Introduction, 7 and Rule 30, commentary 10-12), which unfortunately was unable to take a firm position on the issue. Thus, the Group of Experts defined cyber-attacks as 'a cyber-operation, whether offensive or defensive, that is reasonably expected [emphasis added] to cause injury or death to persons or damage or destruction to objects' (Rule 30) (Fleck, 2013, p. 342). It is worth noting that in jus in bello, contrary to the jus ad bellum, the motives behind the attack are irrelevant (Schmitt, 2002, p. 373).

On the other hand, the definition of 'military objectives', as provided in article 52(2) of Protocol I, entails the neutralization of an object as offering a definite military advantage. Thus, for authors like Dörmann (2004, p. 4; also, Melzer, 2011a, p. 7), shutting down an electricity grid (i.e., preventing it from continuing working) without any destruction involved is also considered an attack for the purposes of IHL. This view is compatible with that of the Tallinn Manual's Experts to whom 'attack' may include those CNAs interfering with the 'functionality of the object', when its reparation involves 'replacement of physical components' (cf. Rule 30).

As an example of a cyber-attack, one could think of the 2010 attack against an Iranian

[13] Schmitt offers some examples of what can amount to violent consequences: significant human physical or mental suffering is logically included in the concept of injury; permanent loss of assets, for instance money, stock, etc., directly transferable into tangible property (377).

nuclear facility called Natanz, by a potent virus known as Stuxnet, had it been committed during an armed conflict[14]. In this concrete case, the malware manipulated the operation of the gas centrifuges in a manner that eventually destroyed a significant part of their uranium enrichment equipment, setting it back several years. Therefore, it did cause physical destruction of the object (Richardson, 2011, p. 17).

Apropos this consequence-oriented notion of attack, it is argued that the use of cyber warfare broadens the ambit of legitimate operations vis-à-vis civilian objects, which if perpetrated by conventional kinetic warfare would reach the violence threshold and thus would be unlawful (Schmitt, 2002, p. 378; 382). As the former do not amount to an 'attack', they fall out of the scope of IHL. Using Professor Schmitt's example, if the NATO 1999 bomb attack on the Serbian State TV station had been carried out by a CNA instead, possibly resulting in no death, injury or destruction, it would not have been considered an attack, and thus it would have been lawful. (Schmitt, 2002, p. 378; see also Kelsey, 2008, p. 1440). Professor Schmitt argues that this expansion of legitimate targets is just a feature of the new battlefields and by no means weakens the existing legal framework (Schmitt, 2002, p. 378).

B. The Principle of Distinction and Cyber Warfare

Although the era of increased technological weaponry has blurred the application of the fundamental IHL principle of distinction, it is unanimously acknowledged that CNAs undertaken in the context of an armed conflict, must distinguish between military and non-military objectives (Koh, 2012). In addition, the Tallinn Manual reaffirms this obligation to distinguish between civilian population and property and military targets when perpetrating cyber-attacks (Rule 31). Nevertheless, this distinction is not without difficulties, as will be seen.

The principle of distinction, whose rationale is the protection of civilian population and property is, as stated by the ICJ in Nuclear Weapons Advisory Opinion, one of the 'cardinal principles contained in the texts constituting the fabric of humanitarian law'[15]. The principle was first codified in the 1863 Lieber Code[16], and makes part of customary international humanitarian law (ICRC Customary Law Study, Rule 1). In modern IHL, the principle is provisioned in articles 48, 51 and 52 of Protocol I.

Thereby, pursuant to the principle of distinction, only combatants and military objectives can be targeted, rendering the intentional attack on civilians or civilian objects absolutely prohibited. The classic example of a cyber-attack on civilians is the disrupting of the computer system of a civilian air control tower, causing civilian airplanes with civilians aboard to crash (Dinstein, 2012, p. 265).

Corollary to the principle of distinction, are the prohibition of indiscriminate attacks,

[14] One shall not over-simplify, since this case triggers a lot of controversial ad *bellum* questions, namely, whether the Stuxnet attack could have amounted to a use of force according to the Charter of the UN and thus initiate an armed conflict, in order for IHL to apply (since there was no on-going armed conflict between the state that allegedly perpetrated the attack and Iran).

[15] The other cardinal principle the Court made reference to is the prohibition of causing unnecessary suffering.

[16] Headquarters, Department of Army, General Orders No. 100, Instructions for the Government of Armies of the United States in the Field (1863), art. 22, available at http://www.loc.gov/rr/frd/Military_Law/pdf/Instructions-gov-armies.pdf (last visit 20 October 2013).

i.e., attacks that do not distinguish between civilian and military targets, either because the belligerent is unwilling to do so, or because the means or method used are inherently indiscriminate[17], and the principle of proportionality, which deals with permissible collateral damage arising from the attack of a military target, when the former is not excessive while compared to the concrete and direct military advantage anticipated.[18] Therefore, in order to be lawful cyber-attacks must be able to discriminate and target military objectives only, and not to cause excessive collateral damage in relation to the military advantage anticipated (cf. articles 48, 51 and 52 of Protocol I).

Although the law seems clear, in practice some vexata questions arise as regards the definition of civilian and military targets, dual-use objects and the classification of civilian experts who engender the sophisticated cyber-attacks. These questions will be dealt with below.

1. Civilian and Military Targets

IHL defines civilians and civilian objects in the negative: civilians are those who are not combatants, and civilian objects are those, which are not military objectives. In case of doubt, the presumption goes for the civilian status[19]. Therefore, it is imperative to define both combatants and military objectives[20].

According to Professor Dinstein, combatants are the 'members of the armed forces of a Belligerent Party, whether regular or irregular, including paramilitary units incorporated de facto in the armed forces' (2010, p. 33). On the other hand, military objectives are those 'objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'[21]. Thus, for the purposes of the present study, computers installed in military facilities, computers that function as weapons or within weapon systems, and computers that keep military information or perform military administrative tasks, are military objects (hence, they are in abstract lawful targets). Using Professor Schmitt's example, attacking the military air traffic control causing military planes to crash is permissible (2002, p. 380). Moreover, to use the same example, one could argue that the Iranian nuclear facility attacked by Stuxnet is a lawful military target, if it was made clear that it was being used to enrich uranium in order to produce nuclear weapons (or that that was a likely purpose). The question whether this attack was nonetheless indiscriminate, is dealt with below.

Beyond clear examples of military targets rests the grey area. Therefore, in order to

[17] Cf. arts. 51(4) and (5) of Protocol I. This is also a norm of customary humanitarian law: see ICRC Customary Law Study, Rules 11-13.

[18]Arts. 57(2)(a)(iii) and (b) of Protocol I. Moreover, intentionally directing attacks against civilians (not taking direct part in hostilities) or civilian objects is a war crime under art. 8(2)(b)(i)–(ii) of the Rome Statute of the International Criminal Court. (Rome Statute).

[19] Arts. 50(1) and 52(1) of Protocol I.

[20] Arts. 43(2) and 52(2) of Protocol I, respectively.

[21]Note that Art. 52(3) of Protocol I states, in case of doubt the object must be considered civilian. Furthermore, the distinction must be made in concrete terms, i.e., if an object, which is normally civilian, is being exclusively used for military purposes, then it becomes a military target.

ascertain the military nature of a target, one has to find the nexus between the target and the on-going armed conflict, taking into account the target's location, its purpose and use. In other words, the target's destruction/ neutralization must offer an effective contribution and a definite military advantage (Schmitt, 2002, p. 380). The crux thus lays in defining 'effective' and 'definite'. A civilian protection-oriented approach like that of the ICRC would define these terms narrowly, whereas a more military-oriented approach is likely to call for a broader meaning of 'effective' and 'definite' (Schmitt, 2002, p. 380). But how far can one go in ascertaining such contribution or advantage? In regard to cyber warfare, Kelsey proposes to broaden the concept of 'military objectives' susceptible of being targeted by a cyber-attack, to include those offering an indirect contribution or providing for 'an effective war-sustaining capability', since cyber weapons have a non-lethal potential (2007, p. 1448). This approach, which would allow for the targeting of economic targets[22], is criticized by the ICRC whose view is that there should not be different notions of military objectives, depending on the weapon used (Dörmann, 2004, p. 6). Finally, it is worth noting that the Group of Experts rejected the inclusion in the Tallinn Manual of 'war-sustaining' objects in their definition of military objectives (Schmitt, 2012, p. 27).

a) Dual-use Targets

'Dual-use objects' are those objects serving both a military and a civilian function, namely, petroleum and power distribution networks, computer information exchange networks, air traffic control networks, power plants, telecommunications and transports infrastructures, to name just a few common-knowledge examples. The problematic of targeting dual-use objects is especially challenging in the context of cyber-attacks, colouring the legal application of the principle of distinction, due to the highly interconnected nature of the military and civilian networks, which renders much of the Internet a dual-use target (Kelsey, 2008, p. 1439).

In theory, if these dual-use objects serve an effective contribution to the military action, they can lawfully be attacked for they become a military target as well (cf. the already mentioned article 52(2) of Protocol I). In practice though, cyber-attacks against dual-use objects are controversial as they normally encompass a larger risk for civilians surrounding the object, and arguably a too remote military advantage. The Tallinn Manual states that when it is not possible to identify the military parts of a dual-use network, then the whole network is considered to be a military objective (Rule 39, commentary 3). It then continues to analyze the legitimacy of targeting social networks such as Facebook. Thus, where these social networks are used to transmit military information, they become military objectives (at least the network's facets being used for that purpose). Nevertheless, should this be the case, the social network would be protected by the principle of proportionality and the obligation to take precautionary measures since if we take into account the enormous number of civilian Facebook users that could be

[22] Notably, this is also the position of the US: '(t)he United States, unlike most other States, takes the position that the aforementioned definition of military objectives encompasses not only objects that are "war-fighting and war-supporting," but also those that are "war-sustaining", such as oil-production facilities in a country that relies on oil export profits to finance its war effort.'

affected, the collateral damage would most likely be excessive). It is important to remind that these questions only arise in case the consequences of the attack reach the 'violence threshold'.

In spite of the above, cyber warfare can play an important role in targeting dual-use objects, for they are likely to cause less harm to civilians than kinetic attacks. For example, it is less disruptive to shut down the flight control system of an airport than to bomb the runway and the airport facilities (Schmitt, 2002, p. 394). This question is related to the question of collateral damage and proportionality (Schmitt, 2002, p. 394) and thus will be dealt in more detail below.

b) Civilians Taking a Direct Part in Hostilities

According to article 51(3) of Protocol I and to customary law (ICRC Customary Law Study, Rule 6), civilian population and civilian objects are immune from attack 'unless and for such time as they take a direct part in hostilities.' The same is provisioned in the recent Tallinn Manual (Rule 35)[23]. Moreover, the ICRC has developed guidelines in order to define and apply the concept of civilians taking direct part in hostilities, as will be seen below[24]. Notably, this rule does not apply to members of organized armed groups or participants of a levée en masse, considered to be military personnel.

In practice, the meaning of taking 'direct part in hostilities' is a matter of controversy among scholars and practitioners, and one difficult to ascertain. The Commentary to the Protocol I describes the standard as 'acts of war which by their nature or purpose are likely to cause actual harm to the personnel or equipment of the enemy armed forces' (Sandoz et al, eds, 1987, paragraph 1944).

In general terms, this is an extremely relevant question because those civilians taking direct part in hostilities lose their civilian protection and become legitimate targets, and will not be counted as collateral damage, nor will they be given the status of prisoner of war if captured (however, they will still be under the protection of Article 75 of the Protocol I). Furthermore, they can be prosecuted for their unlawful participation in hostilities. It is worth noting that, according to the ICRC, the civilian status of these persons maintains. However, some authors like Professor Dinstein argue that by engaging in the hostilities civilians become combatants (more precisely, unlawful combatants) and therefore lose their status as civilians (2010, p. 147).

On the other hand, the particular case of CNA poses some challenges in determining when and for what time civilians contracted to program and maintain software, and to plan and perpetrate cyber-attacks, are taking direct part in hostilities.

Determining the scope of application of the exception of taking part in the hostilities to the protection of civilians involves defining the notions of 'direct', 'hostilities' and 'for such time'. The meaning of direct participation can be interpreted by recourse to the three cumulative criteria proposed by the ICRC guidelines, which are generally accepted (Turns, 2012, p. 286)

[23] Moreover, Article 8(2)(b)(i) of the Rome Statute also refers to the war crime of attacking civilians 'not taking direct part in hostilities'. Note that entering this equation are also medical and religious personnel embedded with the belligerent parties.
[24] Cf. *Interpretive Guidance on the Notion of Direct Participation in Hostilities under IHL*, ICRC, 2009 (available at http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf). For a detailed analysis of the guidelines see Dörmann, pp. 8-11.

and acknowledged in the Tallinn Manual (Rule 35): (1) the act must be likely to adversely affect the military operations or the military capacity of a Belligerent Party or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack; (2) the act (or the military operation in which the act is integrated) has to be the direct cause of the harm likely to occur; and (3) the act must be designed to, directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another (thus, an attack in view of a private gain is not considered as direct participation). Professor Dinstein adds that, regardless of the location of the person, every use of weapons in combat is considered as direct participation in the hostilities. Thus, whoever sends an email with a virus likely to reach the violence threshold is taking direct part in the hostilities and is consequently a lawful target, no matter how far from the hostilities this person is (2010, p. 149). One could question, however, the relevance of a civilian becoming a lawful target when he or she is acting sometimes thousands of kilometres away, on the other side of the world, perpetrating a cyber-attack, for instance.

In addition, it is consensual that the meaning of engaging in hostilities is both narrower than that of contributing to the effort of war, and broader than that of the concrete acts of violence, i.e. attacks, as defined above (Kalshoven, 2011, p. 102; Dinstein, 2010, p. 150). Hence, although a virus does not cause a direct harm itself, it triggers situations that will cause the said harm. Thus, perpetrating cyber-attacks in the context of an armed conflict, finding vulnerabilities in a system that can thus be attacked, designing malware to attack a particular target, and gathering intelligence through cyber means and passing it to the armed forces, are 'unambiguous' examples of cyber-attacks, according to the Tallinn Manual (Rule 35). On the other hand, providing software maintenance to the armed forces[25], or designing malware generally, are not acts integral to a military operation and as such do not entail the loss of civilian protection[26]. The problem here will be distinguishing these 'embedded' civilians from the military forces.

Finally, it is accepted that civilian scientists and weapon's experts are protected civilians, although doubts remain as to those scientists whose expertise in the field is so unique 'and potentially decisive for the outcome of the armed conflict', that some consider legitimate to uphold their protection (ICRC Guidelines, 2009, p. 102).

Although the time-factor is one difficult to assess, some argue that the duration of direct participation in hostilities should encompass the preparatory measures to the act itself and what is required to 'both "upstream" and "downstream" from the actual engagement' (Dinstein, 2010, p. 148). This would entail a broader engagement than the more consensual one including the acts existing immediately before and after the attack. What this interpretation means for CNA remains to be seen in practice: the former interpretation would include the process of identifying vulnerabilities in a target system and the damage assessment period in

[25] This seems not to be the view of the US National Research Council which states that civilians that accompany the military forces even if they are not the ones who press the button, should be a legitimate target (Turns, 2012, p. 290).
[26] There is no consensus as to designing malware that most likely will be used for military purposes, but the precise target is unknown to the designer and supplier of the malware. In this case, the required direct causal link between the designer at and the attack is difficult to fulfill (Turns, 2012, p. 290).

order to evaluate the need to re-attack; on the other hand, acts immediately before and after the attack would include travelling to and from the computer base. This example is taken from Rule 35 of the Tallinn Manual.

The problem of the 'delayed effects' of a 'smart virus' regarding the time-period of direct participation can be solved with the 'active role in the attack' threshold (cf. Rule 35, commentary 8 of the Tallinn Manual). Thus, even if the effects of the attack are to happen somewhere in the future, the direct participation will cease when the active role ceases and not when the effects are felt. Nevertheless, this question is debatable, as one can extract from the Tallinn Manual (cf. commentary 8). Still unresolved time-factor questions, in the Tallinn Manual, are: (1) the case of intermittent attacks: is an individual who, in the period of one month engages in several different attacks (against the same target or a different one), taking direct participation (and thus becoming a legitimate target) for the whole month or intermittently during each attack? (2) In case of doubt, should the non-direct participation be presumed? (on these divergences, cf. Rule 35, commentaries 10 to 12).

Generally, there are other unsolved questions, namely the ignorance of the attackers themselves, when their computers are being used to conduct denial of services without their knowing it; and the case of 'patriotic hacking', where civilians voluntarily engage in the hostilities after a government call (Kodar, 2012, pp. 126-7). As seen above, if these attacks reach the improbable level of causing death, injury or destruction, or cause military harm, then these civilians lose their immunity with all its consequences. The easiness with which these attacks can be triggered (Kodar talks about the 'playstation mentality', 2012, p. 125) and the lack of the attackers' conscience and ignorance of the consequences, may spur abuses of power, and constitutes a real problem that has to be legally dealt with (cf. the Human Rights Council Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions, 2010, p. 84). Whether the existing framework will be able to do it in practice remains to be seen.

From the above, there is clearly still a lot of legal uncertainty in this field. A broad interpretation of the concept of direct part in hostilities is dangerous, whereas a too narrow one might be unrealistic. Thereby, Kodar proposes that it should be for the military forces to engage in cyber warfare, and not for civilians (2012, p. 125). Notwithstanding, cyber operations exclusively operated by military personnel does not seem to be the reality so far. Moreover, as seen above, this increasing dependence of military forces on civilian experts makes the application of the principle of distinction even more difficult.

2. Indiscriminate Attacks

Also as a corollary of the principle of distinction, there is the principle of discrimination. Article 51 (4) and (5) of Protocol I and customary international humanitarian law (ICRC Customary Law Study, Rules 11-13) prohibit attacks that do not distinguish between civilian and military targets either because the belligerent is unwilling to do so, or because the means or methods used (or their effects) are inherently indiscriminate.

To put it bluntly, the Internet is everywhere and every computer is inter-connected. Therefore, a high degree of expertise and sophistication is required to engender a cyber-attack that is capable to, on the one hand, distinguish between military and civilian targets, and on the other, avoid 'knock-on effects' into civilian networks and computers. This is not to say that all cyber-attacks are inherently indiscriminate, for it is still possible to target a specific military object. However, in some cases if perpetrated without additional sophisticated measures and precautions, the risk of indiscriminate effects of such attack is considerably high. The paradigmatic example is the launch of a virus in order to target a military/ governmental computer network: this virus is most likely to spread to other networks and systems (civilian or military, from the State attacked or from a neighbouring State), without any possible control by the attacker or the attacked (Dörmann, 2004, p. 5). One could think of the cyber-attack to the Estonian governmental and civilian systems, in May 2007. The attack not only disrupted the governmental cyber facilities but also hit the websites of banks, newspapers, telephone and broadcast systems, and most importantly, the emergency call centre was unavailable for more than one hour, causing harm to the civilian population (Kelsey, 2007, pp. 1428-9). Note that David Turns does not consider this attack to have reached the 'attack' threshold. (2012, p. 287) Apart from jus ad bellum considerations, should this attack have been perpetrated during an armed conflict between Estonia and Russia (who was allegedly the perpetrator of the attack), it would have violated the prohibition of indiscriminate attacks, for the perpetrator could not prevent civilian harm to occur. Proportionality considerations regarding this type of attack will be dealt with below.

In addition, the Stuxnet attack can be a useful and exceptional example. It seems from the information provided that Stuxnet was created to specifically target Natanz: its malware was designed to detect Siemens software, sabotaging the power supplies used to control the speed of a device, such as the motor. It does not however sabotage any power supply, but only the ones that run a specific frequency. In other words, Stuxnet is a very accurate virus, capable of pinpointing its target. Although the virus spread likewise to civilian systems across the world, it caused mere inconveniences to these other targets, not differently than any other lawful attack that necessarily causes disruptions in the daily life of a civilian (for a more detailed and technical analysis of the Stuxnet attack see Richardson, 2011, p. 10).

3.The Principle of Proportionality

The protection afforded to civilians by the principle of distinction extends to attacks on military targets that are likely to cause excessive collateral damage, i.e., incidental death, injury or destruction to civilians and/or civilian objects. The principle of proportionality states that collateral damage is legitimate if not excessive in relation to the concrete and direct military advantage anticipated. This principle is provisioned in articles 51 (5) (b) and 57 (2) (a) (iii) of the Protocol I. Furthermore, '(i)ntentionally launching an attack in the knowledge that it will cause collateral damage to civilians or civilian objects', which would be clearly excessive in relation to the concrete and direct overall military advantage anticipated, is a war crime

under article 8 (2) (b) (iv) of the Rome Statute. According to the Commentary to the Additional Protocols, the 'concrete' and 'direct' advantage has to be 'substantial and relatively close (…) advantages which are hardly perceptible and those which would only appear in the long term should be disregarded' (Sandoz et al, eds, 1987, paragraph 2209). Also, the advantage assessed is that of the overall operation, and not that of the individual attack itself (Schmitt, 2002, p. 391). Thereby, a CNA against a military target that inadvertently causes collateral damage (i.e., that reaches the violence threshold), which is not excessive in relation to the concrete and direct military advantage anticipated, is still a lawful attack.

Corollary to the principle of proportionality is the obligation to take all feasible precautions on attack to protect civilians from harm, namely issuing warnings of attacks, choosing less harmful weapons, so on and so forth. This obligation is stated in article 57 of Protocol I, and is part of customary humanitarian law (ICRC Customary Law Study, 2009, Rules 15-21).

As mentioned above, mere inconveniences to the civilian population (like blackouts, goods shortage, lack of transports, and so forth) will not be taken into account as collateral damage, since these are accepted secondary effects of an armed conflict. Notwithstanding, the line between mere inconveniences and collateral damage is a thin and ambiguous one. While Dörmann and other authors consider some inconveniences, e.g. disrupting a TV broadcast, as being collateral damage, other authors like Schmitt qualify them as a legitimate consequence of an armed conflict (for a comparison between these two approaches see Niels, p. 7). Finally, it is worth noting that the Group of Experts of the Tallinn Manual accepted that causing loss of data does not amount to collateral damage unless it interferes with the 'functionality of the civilian network' (Rules 52-8).

The high interconnectivity of the cyber infrastructure highlights the question whether the 'knock-on effects' of a cyber-attack count as collateral damage. According to Jensen, 'knock-on effects', are 'known as second and third tier effects that were not accounted for in the planning stages of the attack, but occur due to some unexpected agent or circumstance' (2002, p. 1177).

The indirect consequences of a CNA are more often than not difficult to predict, for there is insufficient knowledge of what exactly is being attacked due to the target's virtual nature, and lack of accuracy in targeting (Schmitt, 2002, pp. 392-3). Thus, there is a high likelihood that cyber-attacks against military objectives will likewise affect civilian computer networks. In addition, the Group of Experts of the Tallinn Manual agreed that both foreseeable direct and 'knock-on effects' count as collateral damage in a collateral damage assessment (Schmitt, 2012, p. 29).

Having said that, it must be acknowledged that cyber-attacks might be a laudable alternative to kinetic attacks that will most likely be disproportionate, as long as the necessary means exist to safely predict collateral damage and knock-on effects throughout the planning of the attack (Schmitt, 2002, p. 393). To use a paradigmatic example, launching a CNA against a military air control tower, causing the military air traffic to disrupt, is a legitimate alternative to bombing it, as this could amount to disproportionate collateral damage among the civilian workers.

a) Works or installations containing dangerous forces

Still under the auspices of the principle of distinction, article 56 of the Protocol I establishes that works or installations containing dangerous forces, namely dams, dykes and nuclear electric generating stations, regardless of their nature as military, civilian or dual-use objects, shall be protected from attack, 'if such attack may cause the release of dangerous forces and consequent severe losses among the civilian population'. This rule of protection applies even if the anticipated proportionality test of the attack is achieved, i.e., even if the collateral damage is not excessive in relation to the military advantage anticipated. However, the protection may cease if the dyke, dam or nuclear station is used in 'regular, significant and direct support of military operations' (article 56 (2) of Protocol I). Although setting a very high standard, and calling for all precautionary measures to avoid the release of dangerous forces, this exception creates difficulties to the fulfilment of the raison d'être of article 56, which is the protection of civilians from catastrophic damage.

Notably, the customary rule (relevant for non-Parties to the Protocol I) differs from its correspondent rule entailed in Protocol I (ICRC Customary Law Study, 2009, Rule 42). Accordingly, the customary norm states that these objects can be attacked if particular care is taken to avoid expected severe losses to civilian population. Thus, standing under the principle of proportionality auspices, this rule does not outright the attack to dams, dykes or nuclear stations, even if the anticipated collateral damage thereof is 'severe', provided it is not 'excessive' (Dinstein, 2010, pp. 194-5). The Group of Experts agreed with the ICRC Rule 42 stating that it reflects a more limited prohibition than the corresponding norms of Protocol I, which do not reflect customary IHL contrary to the former (cf. Rule 80, commentary 1).

In what CNA is concerned, this prohibition is relevant, since more and more works and installations containing dangerous forces, are controlled by computers and thus are more vulnerable to a cyber-attack. Some authors like Kodar (2012, p. 121) and Schmitt (2002, p. 385) argue that cyber-attacks against these critical infrastructures (provided they are military objectives, i.e., that they serve a military use or purpose) are able to neutralise the possible release of dangerous forces, thus widening the ambit of legitimate targets of this nature. The already mentioned Stuxnet attack on Iranian nuclear facilities, which arguably did not result in the release of nuclear radiation, could be a fair example of a lawful attack against a nuclear station, provided the Natanz facilities may be classified as a 'nuclear electrical generating station'[27]. This is not oblivious to concerns, especially from the part of the ICRC (Dörmann, 2004, p. 7): how certain of the probability of releasing such dangerous forces can the attacker be, especially when these facilities are dependent on computer systems not entirely known by the enemy? Without this certainty, the attack could still be lawful pursuant to the exception of article 56 (2) (b), if it could be proved that these facilities were being used to develop nuclear weapons. Finally, the corresponding norm in the Tallinn Manual is Rule 80.

[27] Of course, the question of attribution of the attack to a State, and consequently the customary character of art. 56 of Protocol I, would have to be the subject of a preliminary discussion.

Conclusions

The present article addresses the application of traditional IHL and the principle of distinction to the relatively new and crescent reality of cyber-attacks perpetrated by governmental forces during an international armed conflict.

Yet, to commit to paper a study on the application of the principle of distinction to cyber warfare, it is necessary to first of all define the concept of 'attack' for the purposes of IHL. Hence, attack is defined in regard to its consequences: if a CNA intends to, or its foreseeable result is to cause death, injury or destruction, then it is considered an attack. As to the consequences of such a definition, the doctrine is divergent. Hence, on the one hand a military-oriented approach lead by Professor Schmitt states that cyber operations against civilians that do not reach the violence threshold are lawful and thus the use of cyber operations ultimately expands the ambit of permissible targets, on the other, a civilian-oriented approach lead by the ICRC naturally rejects this argument as being incorrect: attacks directed against civilians can never be lawful, even if they do not reach the violence threshold. The Tallinn Manual reflects this divergence without firmly leaning towards one of the arguments.

Further, the 'cardinal' principle of distinction and, concomitantly, its corollary principles of discrimination and proportionality are a fundamental tool to any military conducting the hostilities. Discriminating the military targets from civilian population and civilian objects and, likewise, assessing the proportionality of any attack are fundamental and constant exercises that are nevertheless coloured by the subtleties of defining civilian and military targets. Firstly, the problematic of dual-use objects is prominent in cyber warfare, since air control towers, oil and gas pipelines, transport and telecommunications infrastructures, and many other dual-use objects, are mainly controlled by computer networks, obliging the military to ascertain what is the use being given to the targeted object in order to decide whether or not to attack. Cyber warfare can play an important role in targeting dual-use objects, when these serve a military purpose and thus become a military target, for they are likely to cause less harm to civilians than kinetic attacks.

Secondly, the reality of civilians taking part in the hostilities is a challenge for any discrimination and proportionality assessment, which is especially difficult in cyber warfare. Many (if not the most) are the civilians managing and operating cyber operations, either because they are contracted to do so by the military, or because they engage in 'patriotic hacking', answering to government calls. The doctrinal divergence regarding when and for what time civilians participate actively in the hostilities reflect the difficulties for the military to know whether and when they can be targeted. On the one, it can be said that clear examples of civilians participating in the hostilities, for the purposes of this article, are perpetrating cyber-attacks in the context of an armed conflict, finding vulnerabilities in a system that can thus be attacked, designing malware to attack a particular target, and gathering intelligence through cyber means and passing it to the armed forces. Yet, when exactly these civilians loose the civilian status and therefore the inherent protection from being attacked is still controversial. This and many other questions are still unsolved and State practice is required

to see how the law interpretation will develop. To conclude, it should be for the military forces to engage in cyber warfare, and not for civilians, in order to avoid uncertainty.

Subsequently, it is argued that although very difficult in practice cyber-attacks are not inherently indiscriminate, as it can be demonstrated through the Stuxnet example. On the contrary, in regard to the proportionality of cyber-attacks collateral damage (that reaches the harm threshold) and 'knock-on effects' are more difficult to predict and control due to the high interconnectivity between civilian and military computer networks and its virtual nature, leading to insufficient knowledge of what exactly is being targeted and lack of accuracy in targeting. This complicates further the proportionality assessment. Moreover, the principle of precaution urges the military not to target (for the present purposes, through cyber-attacks) works or installations that may contain dangerous forces such as dams, dykes and nuclear generating stations (article 56 of Protocol I). In regard to CNAs, this prohibition is relevant, since more and more works and installations containing dangerous forces, are controlled by computers and thus are more vulnerable to a cyber-attack. The question whether these may notwithstanding be targeted if the result is the neutralization of the work or installation has yet to be solved. Notably, the ICRC corresponding norm provides, under the auspices of the principle of proportionality, a more protective norm, seconded by the Group of Experts of the Tallinn Manual, who considered the former and not the latter as customary.

Despite the fact that some vexata questions remain unsolved and some remain in a legal void, this article shows that by recourse to analogy and interpretation, it is possible to conclude that the existing legal framework suffices to provide adequate protection to those it seeks to protect, i.e., the civilian population and objects. Nevertheless, the most part of cyber operations fall short of the notion of 'attack' and thus are not regulated by IHL or by the recently released Tallinn Manual that chose not to address these questions. This is unfortunate since it opens the Manual to the criticism that it contains but black letter for the time being (cf. Fleck, 2013), despite its undeniable value as a step forward in the discussion around cyber security that paves the way towards legal certainty.

Finally, considering that cyber-attacks may achieve comparable military gains with less collateral damage and suffering than conventional kinetic attacks, their (regulated) use must be encouraged. Thus, efforts to create a cyber-department within States' armed forces, where computer experts can properly assess the effects of an attack, are to be welcomed.

Bibliography

Alston, P, 2010. *Human Rights Council Report of the Special Rapporteur on Extrajudicial, Summary, or Arbitrary Executions*. A/HRC/14/24/Add.6. [On-line]. Available in: http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.24.Add6.pdf, (Consult. Apr. 3, 2013).

Dinstein, Y, 2010. *The Conduct of Hostilities under the Law of International Armed Conflict*. Cambridge: Cambridge University Press.

Dinstein, Y, 2012. Principle of Distinction and Cyber War in International Armed Conflicts. *Journal of Conflict & Security Law,* 17 (2).

Dörmann, K, 2004. *Applicability of the Additional Protocols to Computer Network Attacks*. [On-line]. Available in: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm, (Consult. Mar. 14, 2013).

Doswald-Beck, L, 2002. Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. In: SCHMITT, MN *et al*, 2002. *Computer Network Attack and International Law*. International Law Studies, 76.

Fleck, D, 2013. Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual. *Journal of Conflict & Security Law,* 18 (2).

Henckaerts, J *et al*, 2009. *Customary International Humanitarian Law, Volume I: Rules*. Geneva: ICRC.

International Court of Justice, 1996. *Legality of the Threat or Use of Nuclear Weapons*. ICJ Reports.

Jensen, M, 2002-2003. Unexpected Consequences from Knock-on Effects: a Different Standard for Computer Network Operation?. *American University International Law Review*, 18.

Kalshoven, F, et al, 2011. *Constraints on the Waging of War*. Cambridge: Cambridge University Press.

Kelsey, J, 2007-2008. Hacking into International Humanitarian Law: the Principles of Distinction and Neutrality in the Age of Cyber Warfare. *Michigan Law Review,* 106.

Kodar, E, 2012. Applying the Law of Armed Conflict to Cyber Attacks: From the Martens Clause to Additional Protocol I. *Estonian National Defence College Proceedings,* 15.

Koh, HH, 2012. *Address to the USCYBERCOM Inter-Agency Legal Conference*. [On-line]. Available in: http://www.state.gov/s/l/releases/remarks/197924.htm, (Consult. Mar. 14, 2013).

Melzer, N, 2009. *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*. [On-line]. Geneva: ICRC. Available in: http://www.icrc.org/eng/assets/files/other/icrc-002-0990.pdf, (Consult. Apr. 3, 2013).

Melzer, N, 2011a. Cyber Operations and *Jus in Bello*. *UNIDIR*. [On-line]. Available in: http://www.isn.ethz.ch/isn/Digital-Library/Publications/Detail/?lng=en&id=143275, (Consult. Mar. 14, 2013).

Melzer, N, 2011b. Cyberwarfare and International Law. *UNIDIR Resources*. Program on Humanitarian Policy and Conflict Research, 2009. *Manual on International Law Applicable to Air and Missile Warfare*. [On-line]. Harvard: Harvard University. Available in: http://ihlresearch.org/amw/HPCR%20Manual.pdf, (Consult. Apr. 3, 2013).

Richarson, J, 2011. *Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield*. [On-line]. Available in: http://ssrn.com/abstract=1892888, (Consult. Mar. 14, 2013).

Roscini, M, 2010. World Wire Warfare *Jus ad Bellum* and the Use of Cyber Force. *Max Planck UNYB*, 14.

Sandoz, Y, et al, 1987. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*. Geneva: ICRC.

Schmitt, MN, 2002. Wired Warfare: Computer Network Attack and Jus in Bello. *International Review of the Red Cross*, 84 (846).

Schmitt, MN, 2011. Cyber Operations and the Jus in Bello: Key Issues. *International Law and the Changing Character of War*, Naval War College.

Schmitt, MN, 2012. International Law in Cyberspace: the Kohl Speech and Tallinn Manual Juxtaposition. *Harvard International Law Journal*, 54.

Schmitt, MN, gen. ed, 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. [On-line]. Available in: http://www.ccdcoe.org/249.html, (Consult. Mar. 14, 2013).

Turns, D, 2012. Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict & Security*, 17 (2).

US National Military Strategy for Cyberspace Operations, 2006, *GL-2*. [On-line]. Available in: http://www.dod.mil/pubs/foi/joint_staff/jointStaff_jointOperations/07-F-2105doc1.pdf, (Consult. Feb.19, 2013).