MEANS AND METHODS OF CYBER WARFARE

Dan-Iulian VOITAȘEC*

Abstract

According to the Declaration of Saint Petersburg of 1868 "the only legitimate object which States should endeavor to accomplish during war is to weaken the military forces of the enemy". Thus, International Humanitarian Law prohibits or limits the use of certain means and methods of warfare. The rapid development of technology has led to the emergence of a new dimension of warfare. The cyber aspect of armed conflict has led to the development of new means and methods of warfare. The purpose of this paper is to study how the norms of international humanitarian law apply to the means and methods of cyber warfare.

Keywords: *cyber warfare, means and methods, international humanitarian law, Tallinn manual, armed conflict.*

1. Introduction

International Humanitarian Law (IHL) limits the way in which hostilities are being conducted by limiting or prohibiting certain means and methods of warfare. According to Article 22 of The Hague Regulations of 1907 "the right of belligerents to adopt means of injuring the enemy is not unlimited."[1] The limitation is reiterated in Article 35(1) of Additional Protocol I (AP I) to the Geneva Conventions of 1949 and in the preamble of the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons. The norms of IHL that limit or prohibit the use of certain means and methods of warfare are also known as the law of weaponry. The law of weaponry contains both general principles and specific rules. The general principles refer to the prohibition of weapons that are by nature indiscriminate or cause unnecessary suffering while the specific rules refer to the limitation or prohibition of certain means and methods of warfare.[2] The norms of IHL that limit or prohibit the usage of certain means and methods of warfare were adopted before the development of cyber capabilities, some of the norms were adopted before the invention of the television set. The modern battle space presents more dimensions, is more complex to manage and employs a larger number of weapons and tools. Due to the rapid development of cyber capabilities, cyberspace has been recognized as one of the five domains of warfare. Although no IHL norms deal directly with situation of cyber warfare, the growing importance of cyber operations has led to the publication, in 2013, of the Tallinn Manual on the International Law applicable to cyber warfare. The Manual was prepared by an international group of experts at the invitation of the NATO Cooperative Cyber Defence Centre of Excellence. The Tallinn Manual is a non-binding document that has the scope of examining the international law governing cyber warfare. The scope of this article is to study how the law of weaponry will apply to cyber means and methods of warfare.

2. Content

Rule 41 of the Tallinn Manual distinguishes between means of cyber warfare and methods of cyber warfare stating that the means of cyber warfare are "cyber weapons and their associated cyber systems" while cyber methods of warfare include the "tactics, techniques and procedures by which hostilities are being conducted."[3] These definitions will apply in both situations of international and non-international armed conflict.[4]

In the commentary on Rule 41, the group of experts state that cyber weapons are "by design, use, or intended use capable of causing either (i) injury to, or death of, persons; or (ii) damage to, or destruction of objects, that is, causing the consequences required for qualification of a cyber operation as an attack" [5] The cyber infrastructure that is used to launch a cyber attack (in this case the internet) is not viewed as a means of warfare because it is not under the control of the attacking party.[6] The definition of methods of cyber warfare does not include communication between allies but it is intended to "denote more than those operations that

* PhD candidate, Faculty of Law, "Nicolae Titulescu" University of Bucharest (e-mail: **dan.voitasec@gmail.com**).

[1] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land. The Hague, 18 October 1907. - Art. 22.

[2] Heather Harrison Dinniss - Cyber Warfare and the Laws of War (Cambridge University Press, 2012) – p. 252.

[3] Michael N. Schmitt et al., Tallinn Manual on the International Law Applicable to Cyber Warfare – Cambridge University Press, Cambridge, 2013 p. 118.

[4] Idem – p. 119.

[5] Idem.

[6] Idem.

rise to the level of an attack"[7]. Even though communications between friendly forces are not viewed as methods of cyber warfare, interfering with the enemy's communication using a Denial of Service (DoS) attack that does not reach the threshold necessary to be considered a cyber attack[8] would constitute a method of warfare.

The development of new means and methods of warfare is not prohibited by international law but the same norms that apply to conventional means and methods of warfare will also apply to the newly developed ones. In a 2011 report the International Committee of the Red Cross (ICRC) stated that IHL will apply to "means and methods of warfare which resort to cyber technology"[9]. The same view is shared by the international group of experts that developed the Tallinn Manual. All new technologies, including cyber capabilities, used in a situation of armed conflict fall under the scope of article 36 of AP I to the Geneva Conventions of 1949 that states: "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." [10]

Although article 36 is not considered customary IHL even some states that are not party to AP I to the Geneva Conventions of 1949, like the United States of America, apply the review of new means and methods of warfare.[11]

The use of new means and methods of warfare is unlawful if they are of a nature to cause superfluous injury or unnecessary suffering[12], their effects are indiscriminate[13] or are intended or expected to cause long-term and severe damage to the natural environment.[14]

Superfluous injury or unnecessary suffering

Rule 42 of the Tallinn Manual states that: *"It is prohibited to employ means or methods of cyber warfare that are of a nature to cause superfluous injury or unnecessary suffering."*[15] This rule reflects both treaty law[16] and customary IHL and is applicable in both international and non-international armed conflict[17]. Unnecessary suffering was defined by the International Court of Justice (ICJ) in the Nuclear Weapons case as "harm greater than that unavoidable to achieve legitimate military objectives."[18]

Article 35(2) of AP I to the Geneva Conventions presents a test for new means a methods of warfare. The effects of the new means and methods must be judged in relation to their military utility. The test is "only valid for weapons designed exclusively for antipersonnel purposes" inasmuch as weapons designed to destroy, for example, military materiel "may be expected to cause injuries to personnel in the vicinity of the target which would be more severe than necessary to render these combatants hors de combat."[19] It is accepted that anti-personnel weapons and weapons used to destroy enemy materiel or fortifications differ in effect and character and that the latter ones will cause more serious injury or lead to the death of more personnel. Their use is not unlawful and does not violate article 35(2) because the military advantage that they offer means that the additional suffering cannot be characterized as unnecessary.[20] In the opinion of Yoram Dinstein "the injunction against superfluous injury or unnecessary suffering hangs on a distinction between injury/suffering that is avoidable and unavoidable."[21] A test of the weapon in question and other available options is required in order to see whether there is an alternative weapon that causes less injury and suffering and if its effects are

[7] Idem.

[8] Rule 30 of the Tallinn Manual - A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects.

[9] ICRC - International Humanitarian Law and the challenges of contemporary armed conflicts (2011) – p. 37. Accessed on 10.03.2016. Available at: https://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf

[10] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts of 8 June 1977 – article 36.

[11] Marco Roscini - Cyber Operations and the Use of Force in International Law (Oxford University Press, 2014) – p. 171.

[12] AP I to Geneva Conventions – art. 35 (2).

[13] Idem – art. 51(4).

[14] Idem – art. 35(3).

[15] Tallin Manual – p. 119.

[16] Article 35(2) of AP I to the Geneva Convention and Article 23 (e) of Hague Convention IV of 1907.

[17] ICRC Customary IHL Database – Rule 70 – Accessed on 10.03.2015. Available at: https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule70.

[18] International Court of Justice - Legality of the threat or use of Nuclear Weapons, Advisory Opinion (1996) – p. 66. Accessed on 11.03.2016. Available at: http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4&case=95.

[19] Bothe et al. – New Rules for Victims of Armed Conflicts – Commentary on the two 1977 Protocols Additional to the Geneva Conventions of 1949, 2nd edition (Brill | Nijhoff, 2013) p. 226. Accessed on 11.03.2016. Excerpts, including page 226, available at: https://books.google.ro/books?id=rVy2AgAAQBAJ&pg; Yoram Dinstein - The Conduct of Hostilities under the Law of International Armed Conflict 1st edition (Cambridge University Press, 2004).

[20] Bothe – p. 226; Christopher Greenwood - The Law of Weaponry at the Start of the New Millennium (International Law Studies – Vol. 71, 1998) – p. 196.

[21] Y. Dinstein – p. 60.

sufficiently effective in neutralizing enemy personnel.[22]

Regarding cyber means and methods of warfare, the Tallinn Manual states that Rule 42 applies only to injury or suffering caused to combatants, civilians directly participating in hostiles and members of organized armed groups while any incidental harm caused, during a military operation, to persons protected against attack would be governed by the principle of proportionality and the requirement to take precautions in attack.[23]

Given the nature of the test it could be argued that the usage of means or methods of cyber warfare, against certain targets, could be more effective than conventional means or methods. Most cyber attacks tend to neutralize or destroy a target while causing fewer casualties. However, the test is not limited just to the immediate effects of the two weapons (or methods of warfare); other factors should be taken in consideration before choosing between the two such as: the availability (including the expense) of both types of weapon, the logistics of supplying the weapon and its ammunition at the place where it is to be used and the security of the troops which employ it.[24] All these factors tend to be in favor of increasing the usage of cyber means and methods in certain situations. It should be noted that most means and methods of cyber warfare are not directed against individuals but against military materiel. As stated in the Tallinn Manual most means and methods of cyber warfare will rarely violate Rule 42[25] but there are some situations in which lawful means and methods of cyber warfare could cause unnecessary suffering. In the example given in the Tallinn Manual a state takes control of the pacemaker of an individual in order to kill him or render him hors de combat by stopping his hart. This action is lawful and does not cause unnecessary suffering to the individual. The act of controlling the peacemaker of the individual, stopping his heart, reviving him multiple times before finally killing him serves no military purpose and would violate rule 42.[26] It may sound like science fiction to take control of an individual's pacemaker but in 2011, Jerome Radcliffe, a security consultant and researcher, hacked his insulin pump and suspended the delivery of insulin[27]

Indiscriminate Means or Methods

The prohibition of indiscriminate attacks can be found in article 51(4) of AP I to the Geneva Conventions of 1949. In subparagraph (b) it is stated that indiscriminate attacks employ means or methods of combat which cannot be directed against a specific military objective; subparagraph (c) prohibits attacks that employ means or methods of combat the effects of which cannot be limited as required under the Protocol and "consequently, in each such case, are of a nature to strike military objects and civilians or civilian objects without distinction." [28] The rule that indiscriminate means or methods of warfare are prohibited also reflects customary IHL and applies to both situations of international and non-international armed conflict[29]. Rule 43 of the Tallinn Manual is based on article 51(4)(b) and (c) and stated that:

"It is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means or methods of cyber warfare are indiscriminate by nature when they cannot be:

a) directed at a specific military objective, or

b) limited in their effects as required by the law of armed conflict

and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction."[30]

It is stated in the commentary accompanying the Tallinn Manual that Rule 43 deals only with means and methods of cyber warfare that are inherently discriminate. Subparagraph (a) prohibits those means and methods of cyber warfare whose effects are impossible to predict.[31] For example the launch of a malware, designed without any specific safeguards, that will infect and deploy the payload component[32] to all computer systems infected without distinguishing between military computer systems and computer systems protected by IHL. Subparagraph (b) prohibits the usage of means and methods of cyber warfare that are capable of being directed against a specific target but also will cause harmful effects on civilians or civilian objects. The rule does not prohibit the use of means and methods of cyber warfare that only cause effects that are "inconvenient or annoying". [33] For example, the Stuxnet virus spread indiscriminately but created effects only on computer systems that had a specific component structure. In this case, the weapon is not

[22] Idem.
[23] Tallin Manual – p. 120.
[24] C.Greenwood – p. 198.
[25] Tallin Manual – p. 120.
[26] Idem – p. 121.
[27] Jerome Radcliffe – Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System (Black Hat USA, 2011).
[28] AP I to the G.C – art. 51(4).
[29] ICRC Customary Database – rule 12, 71.
[30] Tallinn Manual –rule 43, p. 121.
[31] Idem.
[32] The part of the packet, message or code that carries the data. In information security, the term payload generally refers to the part of malicious code that performs the destructive operation.- http://www.securityfocus.com/glossary/P
[33] Tallinn Manual, p. 121.

prohibited under Protocol I and Rule 43 of the Tallinn Manual because even though the spread was indiscriminate the effects were limited to specific computer systems.

In the Manual it is also stated that all indiscriminate effects caused by means or methods of warfare, during a particular attack, will not violate rule 43 if they were caused by an unforeseeable system malfunction or reconfiguration.[34] Even though that is the case, states are required to ensure that new means and methods of warfare that they develop comply with the rule of IHL that bind the state. This requirement is found in article 36 of A.P. I to the Geneva Conventions and is also reflected in Rule 48 of the Tallinn Manual[35].

The International Group of Experts that worked on the Tallinn Manual found it difficult to identify means and methods of cyber warfare that might violate Rule 43[36]. Indeed, given the rapid development in the field of IT&C it is hard to believe that states could not create a cyber weapon capable of targeting certain military objectives without causing harm to objects and individuals protected by IHL. Stuxnet, discovered in 2010 was capable of targeting only Siemens supervisory control and data acquisition (SCADA) systems[37]. Given the amount of time that has passed since the discovery of the malware it is plausible to believe that state have the capability to develop even more powerful and precise cyber weapons. Having that in mind, the application of this norm of international law on all means and methods of cyber warfare is important for the safeguard of civilians and civilian objects.

Cyber booby traps

The usage of conventional weapons is generally not prohibited by IHL but a series of treaties were adopted that limit or prohibit the usage of certain conventional weapons that do not respect the norms of IHL[38]. Although, at this time, there is no norm of IHL that limits or prohibits the usage of cyber capabilities, some means and methods of cyber warfare could be the subject of definitions of other weapons conventions[39]. The usage of cyber booby traps fall under such definition. Protocol II and Amended Protocol II of the Conventional Weapons Convention define booby traps as "any device or material which is designed, constructed or adapted to kill or injure, and which functions unexpectedly when a person disturbs or approaches an apparently harmless object or performs an apparently safe act. " [40] Rule 44 of the Tallinn Manual states that "it is forbidden to employ cyber booby traps associated with certain objects specified in the law of armed conflict."[41] The rule is based on the definition of booby traps found in the Conventional Weapons Convention; it reflects customary international law in both international and non-international armed conflict.[42]

According to the International Groups of Experts for a cyber booby trap to fall under the scope of this rule it must include the following factors[43]:

- the cyber booby traps should be deliberately designed to operate unexpectedly
- it must be "designed, constructed or adapted to kill or injure"
- the act that triggers the cyber booby trap should appear harmless.

The cyber weapon should be associated with specific objects defined in art. 7 of Amended Protocol II to the CWC[44]

Perfidy

Perfidy is defined in article 37 of AP I to the Geneva Conventions of 1949 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."[45] The Tallinn Manual states in Rule 60 that "in the conduct of hostilities

[34] Idem, p. 122.

[35] Tallinn Manual – Rule 48: a. All States are required to ensure that the cyber means of warfare that they acquire or use comply with the rules of the law of armed conflict that bind the State.

b. States that are Party to Additional Protocol I are required in the study, development, acquisition, or adoption of a new means or method of cyber warfare to determine whether its employment would, in some or all circumstances, be prohibited by that Protocol or by any other rule of international law applicable to that State.

[36] Tallinn Manual, p. 122.

[37] Nicolas Falliere - Stuxnet Introduces the First Known Rootkit for Industrial Control Systems. Available at: http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scada-devices

[38] Beatrice Onica Jarka – Drept International Umanitar (Universul Juridic, 2010) – p.99.

[39] H.H Dinniss – p. 258.

[40] Protocol II to the 1980 CCW Convention as amended on 3 May 1996 – art. 2(4).

[41] Tallinn Manual – Rule 44, p. 122.

[42] ICRC Customary IHL Database – Rule 80.

[43] Tallinn Manual, p.123.

[44] Protocol II to the 1980 CCW Convention as amended on 3 May 1996, Article 7(1) […] (a) internationally recognized protective emblems, signs or signals; (b) sick, wounded or dead persons; (c) burial or cremation sites or graves; (d) medical facilities, medical equipment, medical supplies or medical transportation; (e) children's toys or other portable objects or products specially designed for the feeding, health, hygiene, clothing or education of children; (f) food or drink; (g) kitchen utensils or appliances except in military establishments, military locations or military supply depots; (h) objects clearly of a religious nature; (i) historic monuments, works of art or places of worship which constitute the cultural or spiritual heritage of peoples; or (j) animals or their carcasses; 2. It is prohibited to use booby-traps or other devices in the form of apparently harmless portable objects which are specifically designed and constructed to contain explosive material.

[45] AP I to the Geneva Conventions – article 37.

involving cyber operations, it is prohibited to kill or injure an adversary by resort to perfidy."[46] The definition of perfidy found in Rule 60 of the Tallinn Manual mimics the definitions found in AP I. The norm applies in both international and non-international armed conflicts and is considered customary international law[47]

According to the International Group of Experts, customary international law includes perfidious acts intended to result in the injury or death of an adversary while article 37 includes acts that also result in the capture of the adversary.[48] Temporal proximity is not required for an act to violate rule 60[49]. An example of cyber perfidy is sending the enemy an email inviting them to meet with a representative of the ICRC. The email will be sent from a genuine but hacked ICRC email address. Several days later, when the enemy arrives at the location they are "greeted" by an explosion causing injury or death to several of them.

The confidence of cyber systems was a topic of debate for the International Group of Experts. In the example given in the Manual, a malware is created that will disrupt the rhythm of an enemy commander's pacemaker. In order to cause the heart attack, the malware will falsely authenticate itself as being generated by a legitimate medical source. The majority of experts considered that in this situation the confidence of an adversary's computer system was betrayed and that Rule 60 was violated while others consider that the notion of confidence presupposes human involvement.[50] Perfidy does not extend to perfidious acts that cause damage or destruction of property, as stated above, the acts should result in the injury or death of the adversary.[51]

The usage of ruse of war is not prohibited by international law. Article 37(2) states that "ruses of war are not prohibited. Such ruses are 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 because they do not invite the confidence of an adversary with respect to protection under that law. The following are examples of such ruses: the use of camouflage, decoys, mock operations and misinformation."

The Tallinn Manual states in Rule 61 that "cyber operations that qualify as ruses of war are permitted."[52] Examples of ruses used during cyber operation include: "(a) creation of a 'dummy' computer system simulating non-existent forces; (b) transmission of false information causing an opponent erroneously to believe operations are about to occur or are underway; (c) use of false computer identifiers, computer networks (e.g., honeynets or honeypots), or computer transmissions; (d) feigned cyber attacks that do not violate Rule 36; (e) bogus orders purported to have been issued by the enemy commander; (f) psychological warfare activities; (g) transmitting false intelligence information intended for interception; and (h) use of enemy codes, signals, and passwords."[53]

Improper use of protective symbols

According to article 38 of AP I to the Geneva Conventions it is prohibited to make improper use the distinctive protection emblems used by the Red Cross, the flag of truce, the protective emblem of cultural property and the emblem of the United Nations without authorization from the Organization. A similar provision can be found in article 12 of AP II to the Geneva Convention, in this case the prohibition is against the misuse of the Red Cross protective symbols. Article 6(1) of AP III to the Geneva Conventions of 1949 and article 23(f) of the Hague Regulations of 1907 contain similar provisions. This prohibition is absolute, the misuse does not have to be linked to actions that result in death, injury or capture of an adversary.[54]

Rule 62 of the Tallinn Manual states that: "it is prohibited to make improper use of the protective emblems, signs, or signals that are set forth in the law of armed conflict." The Rule is based on treaty provisions and customary international law and applies in both situations of international and non-international conflict.[55] The International Group of Experts had split opinions regarding the improper usage of protective symbols in a cyber context. Some considered that using a fake @icrc.org or UN email to send malware to the adversary is not prohibited because the symbol of protections was not misused while others considered that the action violated Rule 62 because the domain name invites confidence as to the affiliation of the originator[56]. I believe that hacking the ICRC database to create a fake email address or hack the private e-mail address of an ICRC employ to send malware to the adversary could violate Rule 62, while using similar domain

[46] Tallinn Manual – p. 149.
[47] ICRC Customary Database – rule 65.
[48] Tallinn Manual – p. 149.
[49] Idem – p. 150.
[50] Idem – p. 151.
[51] Idem.
[52] Idem – p. 152.
[53] Idem.
[54] H.H Dinniss – p. 265.
[55] ICRC Customary IHL Database – Rules 58 to 60.
[56] Tallinn Manual – p. 154.

names, for example @ierc.org, @ic-rc.org etc. would not violate rule 62.

Belligerent reprisals

Belligerent reprisals "consist of action which would normally be contrary to the laws governing the conduct of armed conflict (the ius in bello) but which is justified because it is taken by one party to an armed conflict against another party in response to the latter's violation of the ius in bello."[57]

According to the ICRC Customary IHL Study, five conditions must be met before belligerent reprisals could be launched: reprisals may only be taken in reactions to a prior serious violation of IHL, reprisals may only be carried as a measure of last resort, they must be proportionate to the violation, the decision to resort to reprisals must be taken at the highest level of government, the reprisal action must cease as soon as the adversary complies with the law.[58]

Reprisals launched against the wounded, sick, medical personnel, medical buildings and equipment[59], prisoners of war[60], shipwrecked persons[61], civilians and their property[62] and cultural property are prohibited[63]. The notion of belligerent reprisals applies only in situations of international armed conflict.

Rule 46 of the Tallinn Manual states that Belligerent reprisals by way of cyber operations against:

(a) prisoners of war;

(b) interned civilians, civilians in occupied territory or otherwise in the hands of an adverse party to the conflict, and their property;

(c) those hors de combat; and

(d) medical personnel, facilities, vehicles, and equipment are prohibited.

Where not prohibited by international law, belligerent reprisals are subject to stringent conditions.

Due to the fact that there is no condition stating that reprisals should be in kind, a state could resort to cyber operations in response to kinetic violations of IHL.

3. Conclusions

The world is more connected and we rely more on computer systems than ever before. This situation can be seen even in the field of military development. The newest development in the field of conducting hostilities is represented by means and methods of cyber warfare. As is the case with conventional means and methods of warfare, the same limitations and prohibitions apply to means and methods of cyber warfare. It may prove difficult to apply some norms of IHL to means and methods of cyber warfare but states that are party to AP I have an obligation to determine if the employment of newly acquired means and methods of warfare are prohibited by international law. In the future we could see more states deciding to resort to means and methods of cyber warfare due to the fact that, in certain situations, they could be more effective and lead to fewer casualties.

References:

- Michael N. Schmitt et al., Tallinn Manual on the International Law Applicable to Cyber Warfare – Cambridge University Press, Cambridge, ISBN 978-1-107-02443-4 Hardback;
- Roscini, M. (2014) - Cyber Operations and the Use of Force in International Law, Oxford University Press, Oxford, ISBN 978–0–19–965501–4;
- Onica-Jarka, B. (2010). Drept internațional umanitar, Universul Juridic, București, ISBN 978-973-127-698-4 1;
- Dinstein, Y. (2004). The conduct of hostilities under the law of international armed conflict, Cambridge University Press, Cambridge;
- Dinnis, H.H. (2012) - Cyber Warfare and the Laws of War, Cambridge University Press, Cambridge, ISBN 978-1-107-01108-3 Hardback;
- Bothe et al. – New Rules for Victims of Armed Conflicts – Commentary on the two 1977 Protocols Additional to the Geneva Conventions of 1949, 2nd edition (Brill | Nijhoff, 2013) Accessed on 11.03.2016. Excerpts available at: https://books.google.ro/books?id=rVy2AgAAQBAJ&pg
- Jerome Radcliffe – Hacking Medical Devices for Fun and Insulin: Breaking the Human SCADA System (Black Hat USA, 2011);

[57] Y. Dinstein – p. 220.

[58] ICRC – Customary IHL Databaste – Rule 145. Accessed on 13.03.2016. Available at: https://www.icrc.org/customary-ihl/eng/docs/v1_rul_rule145

[59] Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field– article 46.

[60] Geneva Convention (III) relative to the Treatment of Prisoners of War – article 13.

[61] Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea – article 47.

[62] Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War – article 33.

[63] Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict– article 4(4).

- ICRC - International Humanitarian Law and the challenges of contemporary armed conflicts (2011) – p. 37. Available at: https://www.icrc.org/eng/assets/files/red-cross-crescent-movement/31st-international-conference/31-int-conference-ihl-challenges-report-11-5-1-2-en.pdf
- Christopher Greenwood - The Law of Weaponry at the Start of the New Millennium, International Law Studies – Vol. 71, 1998;
- ICRC Customary IHL Database - Available at: https://www.icrc.org/customary-ihl/eng/docs/home
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts of 8 June 1977;
- Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts, 8 June 1977;
- Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Adoption of an Additional Distinctive Emblem, 8 December 2005;
- Geneva Convention (I) for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Fiel, 12 August 1949;
- Geneva Convention (II) for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 12 August 1949;
- Geneva Convention (III) relative to the Treatment of Prisoners of War, 12 August 1949;
- Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12 August 1949;
- Hague Convention for the Protection of Cultural Property in the Event of Armed Conflict, 14 May 1954;
- Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects, 1980;
- International Court of Justice - Legality of the threat or use of Nuclear Weapons, Advisory Opinion (1996) – p. 66. Available at: http://www.icj-cij.org/docket/index.php?p1=3&p2=4&k=e1&p3=4& case=95
- Nicolas Falliere - Stuxnet Introduces the First Known Rootkit for Industrial Control Systems. Available at: http://www.symantec.com/connect/blogs/stuxnet-introduces-first-known-rootkit-scad a-devices
- http://www.securityfocus.com/glossary