APPLYING THE LAW OF ARMED CONFLICT TO CYBER ATTACKS: FROM THE MARTENS CLAUSE TO ADDITIONAL PROTOCOL I

Erki Kodar

1. Introduction

The operational environment is in a state of flux, presenting operators, lawyers and soldiers with new challenges on the battlefield. The legal tools applicable to the changing environment have often been created before modern advancements in the methods and means of warfare. The technological leaps of the past three or four decades create unique challenges for lawyers as the applicable norms predate the inventions. Nevertheless, numerous international and non-international conflicts and international disputes have shown that the "old law" is capable of answering new questions. The adaptability of the Law of Armed Conflict (LOAC) is a core characteristic of this, providing analytical tools for unforeseen circumstances and enabling the provision of sound legal advice to commanders.

The Martens Clause is an apt starting point for the discussion of one of the challenges facing LOAC: cyber attacks.[1] Public international law as a whole is struggling to come to grips with cyber attacks as this phenomenon presents complex questions.[2] Cyber attacks – or Computer Network Attacks (CNAs) – are, according to the US definition, "actions taken through the

[1] See **D. Hollis.** 2007. Why States Need an International Law for Information Operations. – Lewis & Clark Law Review, Vol. 11, p. 1023; **M. Schmitt.** 2002. Wired Warfare: Computer Network Attack and Jus In Bello. – International Review of the Red Cross, Vol 84, No 846, p. 367; **K. Dörmann.** 2001. Computer Network Attack and International Law – Extract from The Cambridge Review of International Affairs "Internet and State Security Forum". Trinity College, Cambridge, UK, 19 May. <www.icrc.org/eng/resources/documents/misc/5p2alj.htm>; **ICRC**. 2003. Direct Participation in Hostilities under International Humanitarian Law. Report. September. <www.icrc.org/ara/assets/files/other/direct_participation_in_hostilities_sept_2003_eng.pdf >.

[2] See **E. Kodar.** 2009. Computer Network Attacks in the Grey Areas of Jus ad Bellum and Jus in Bello. – Baltic Yearbook of International Law, Vol. 9; **M. Benatar.** 2009. The Use of Cyber Force: Need for Legal Justification? – Goettingen Journal of International Law, Vol. 1, pp. 375–396; **S. J. Shackelford.** 2009. From Nuclear War to Net War: Analogizing

use of computer networks to disrupt, deny, degrade or destroy information resident in computers and computer networks, or the computers and the networks themselves."[3] Rain Ottis, a scientist at the Cooperative Cyber Defence Centre of Excellence, defines cyber attacks as "the malicious use of information systems in order to influence the information, systems, processes, actions or decisions of the target without their consent."[4] The scope of cyber attacks is thus extensive and, by whichever definition, encompasses a range of actions available to military planners.

Under which circumstances can a cyber attack be attributed to a state? Can a cyber attack exceed the threshold of use of force established in the UN Charter? Can a cyber attack constitute an armed attack that would justify the right of self-defence? As the Internet is not a centralised networking system, is there a way to defend against cyber attacks that overlap different jurisdictions? Perhaps there are no easy answers, but existing law most definitely provides guidance on these issues. Whether the answers provided are adequate or sufficient is up for debate. Nevertheless the need to comprehend these issues is urgent as even the Group of Experts on NATO's new Strategic Concept foresee cyber attacks as one of the most probable threats to the Alliance in the next decade.[5]

Cyber attacks turn the attention of LOAC to a set of pressing questions. Many of these questions are fundamental to the law – are there concrete and precise restrictions regarding the employment of cyber attacks? Can LOAC, a body of law mostly regulating international conflicts and conventional weapons, provide workable solutions? As cyber attacks require a high level of knowledge of information technology and are thus more likely to be executed by civilian experts, are the perpetrators of cyber attacks then entitled to combatant privilege or is it a case of direct participation in hostilities? Can cyber attacks be regarded as a means of warfare? Are cyber attacks in compliance with the requirements of neutrality? What restrictions and modalities arise during targeting? Can cyber attacks be construed as constituting perfidy or

---

Cyber Attacks in International Law. – Berkley Journal of International Law, Vol. 25, No. 3, pp. 191–250.

[3] **Department of Defense.** 2009. Dictionary of Military and Associated Terms. – Joint Publication 1–02. 12 April 2001, as amended through 31 October 2009, p. 111.

[4] **R. Ottis.** 2009. On Definitions. 14 July. <conflictsincyberspace.blogspot.com/2009/07/on-definitions.html>.

[5] **North Atlantic Treaty Organisation.** 2010. NATO 2020: Assured Security; Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO. <www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf>.

other prohibited methods of warfare? The field for legal research is ripe for practitioners and academics.

The aim of this article is to describe, in general, the interaction between the current norms of LOAC and cyber attacks, whether they be state-coordinated or perpetrated by individuals. The focus is on *jus in bello* and on the practical problems that the use, or defence against the use, of cyber attacks brings forth. The article will try to provide indicative answers to the questions posed above and argue that the current body of LOAC applies to cyber attacks by way of fundamental principles or norms, and that the law is capable of providing guidance to operators and practitioners in the conduct of military operations.

2. Prerequisites for the Application of LOAC: Invoking the Spirit of Martens

Applying LOAC norms to cyber attacks is only possible in the event of an armed conflict (mostly in international armed conflicts, possibly in non-international armed conflicts). The current article is based on the presumption of an established armed conflict governed by LOAC. When and in cases where cyber attacks fall under the purview of LOAC, the legal restrictions regulating the means and methods of warfare will apply to cyber attacks as well. These restrictions limit the freedom of permissible actions either in defence (actions taken whilst defending a cyber attack) or offence (actions taken whilst conducting cyber attacks against a belligerent).

LOAC contains no explicit treaty provision or custom regulating conduct in relation to cyber attacks. To date, there has been no international arms control treaty that would either ban or place restrictions on cyber weapons. This *lacuna* has bred two differing viewpoints. One school of thought plays the devil's advocate by stating that the absence of a treaty should be interpreted to mean that the law does not apply to cyber attacks and states are free to conduct actions in this field. A similar argument was put forward to the International Court of Justice (ICJ) in the *Legality of the Threat or Use of Nuclear Weapons* advisory opinion,[6] but ultimately rejected. The ICJ's approach in the case created the basis for the second school of thought, which

[6] *Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion)*, ICJ Reports (1996), pp. 226–267 (hereinafter *Nuclear Weapons*).

takes the more balanced view and tries to avoid the legal gap by way of interpretation and analogy.[7]

The ICJ invoked "the Martens Clause, whose continuing existence and applicability is not to be doubted, as an affirmation that the principles and rules of humanitarian law apply to nuclear weapons".[8] Hence, in the absence of explicit norms, one can turn to the Martens Clause to ascertain the limits of freedom of action. The clause states that

> in cases not included in the [Hague] Regulations … populations and belligerents remain under the protection and empire of the principles of international law, as they result from the usages established between civilised nations, from the laws of humanity and the requirements of the public conscience.[9]

The aim of the clause is to specify that the belligerents' choice of methods or means of warfare is not unlimited, and to either eliminate or minimise any incidents in armed conflicts that are not covered by treaty regulation or customary law. This principle reaffirms that even without the explicit mention of cyber attacks in modern treaties or customs, certain fundamental restrictions derived from LOAC still apply.

A more modern sentiment regarding the application of LOAC to cyber attacks can be ascertained from the statements of the states themselves. In November 2009, the International Committee of the Red Cross (ICRC) organised the conference "60 Years of the Geneva Conventions and the Decades Ahead" in Geneva, Switzerland.[10] The conference focused on the challenges

---

[7] It has been argued that "[i]t is perfectly reasonable to assume that also the new forms of CNA, which do not involve the use of traditional weapons, are subject to IHL just as any new weapon or delivery system has been so far when used in an armed conflict". **Dörmann** 2001, para. 7.

[8] *Nuclear Weapons*, para. 87.

[9] Preamble of the 1899 Hague Convention (II) with Respect to the Laws and Customs of War on Land (entered into force 4 September 1900) and 1907 Hague Convention (IV) Respecting the Laws and Customs of War on Land (entered into force 1 January 1910). The modernised Martens Clause is contained in Article 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 7 December 1978, 1125 UNTS 3 (hereinafter AP I) which states that "[i]n cases not covered by this Protocol or by other international agreements, 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".

[10] **J. Kellenberger.** 2009. Statement by ICRC president Jakob Kellenberger. 9 November. <www.icrc.org/eng/resources/documents/statement/geneva-convention-statement-091109.htm>.

to LOAC, new threats, new actors, and new means and methods of war. The main discussion was about whether LOAC applies to the new actors, threats and means and methods of war. Most of the representatives agreed that LOAC is a sufficiently flexible tool that can overcome abstract challenges and the main issue is actually the enforcement of LOAC. Nevertheless, one of the issues under discussion was cyber attacks wherein the majority view was that the Geneva and Hague laws provide guidance on these matters. In his official statement, 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.[11]

If, by way of the Martens Clause, cyber attacks are not beyond the pale of law, it is possible to agree that LOAC applies to cyber attacks. If cyber attacks are perceived as a means of warfare, then discerning between different types of cyber attacks is a must, as not all attacks would be regulated by LOAC. The question to be asked is: does a cyber attack constitute the use of violence in an attack? The Geneva Conventions of 1949 and especially the Additional Protocol I of 1977 (AP I) define violence through attacks – attacks are acts of violence against the adversary in offence or defence.[12] The picture is blurred with regard to cyber attacks as some types of attacks or intrusions might only cause inconvenience – disruption of a commerical or military intranet, downloading financial or personal information, temporary loss of access to Internet or to some websites. To this list it is possible to add cyber espionage which is more concerned with intelligence gathering and would usually breach the computer systems but might not cause any tangible or harmful effects. On the other hand there exist cyber attacks that can cause, directly or indirectly, damage or injury to persons or objects in a manner similar to kinetic weapons.

Thus it can be argued that the effects of cyber attacks do not always constitute violence in the strict sense of Article 49(1) of AP I, as it would be counterproductive and even dangerous to regard in every case everyday hacking and espionage as an attack under LOAC. But where can one draw the line? The Commentary on AP I states that Article 49(1) has been constructed with the civilian population in mind and as such has been intended to be interpreted in a broad and generic manner, as the attacks (or combat actions, as the Commentary suggests) and the effects of these attacks

[11] **R. Schweppe.** Statement by H. E. Ambassador Reinhard Schweppe. 9 November.

[12] AP I, Article 49(1).

may affect the civilian population.[13] According to Article 49(1) "violence" is defined in terms of the consequence of physical (in case of objects and physical persons) or mental (in case of physical persons only)[14] damage.

Schmitt proposes an effects-based approach to distinguish between cyber nuisances and cyber attacks proper under LOAC. Deriving from the interpretation of Article 49(1) of AP I, the term "violence" is "prescriptive shorthand intended to address specific consequences" and "it must be considered in the sense of violent consequences rather than violent acts".[15] Thus, cyber attacks fulfil the requirements of Article 49(1) when the consequences of such attacks are not sporadic, isolated cases of inoconvenience, and are intended to cause injuries, death, damage and destruction, and where such consequences are predictable or desired. This approach gives better guidance when discerning whether operators are dealing with a common nuisance or a full-fledged cyber attack under LOAC.

If LOAC wants to impose rules on cyber attacks, the effects of cyber attacks in most cases cannot be intangible and they need to be the source of, or contribute to the physical destruction of a military target. Nevertheless, even under this approach some grey areas will remain – it is debatable whether the remote formatting of an adversary's command and control database and corrupting the hard-drive concerned is an act of physical destruction. *Prima facie* the act brings forth destruction of data and such an outcome is desired by the attacker but the hard-drive would still exist unharmed in its physical state.

3. Specific LOAC Issues Related to Cyber Attacks

The aim of the following section is to give a brief, and by no means comprehensive or exhaustive overview of LOAC issues that must be assessed when conducting offensive or defensive cyber attacks. The issues at hand are the law of neutrality, cyber attacks as weapons systems, targeting challenges (conventional, economic, dual-use targets and facilities containing dangerous forces), indiscriminate attacks, direct participation in hostilities and the question of perfidy.

---

[13] **C. Pilloud & J. Pictet.** 1987. Article 49. Definition of Attacks and Scope of Application. – Y. Sandoz *et al.* (eds). Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Geneva: Martinus Nijhoff, pp. 602–603.

[14] For example, spreading terror among the civilian population is prohibited per AP I, Article 51(2).

[15] **Schmitt** 2002, p. 377.

3.1. Cyber Attacks and the Law of Neutrality

The law of neutrality under LOAC could be the main obstacle impeding the conduct of either offensive or defensive cyber attacks. Most of the body of law regulating the law of neutrality is contained in the 1907 Hague Convention V, which predates the existence of Internet and cyber weaponry by more than a half a century. Neutrality is the right of the State to have relations with other belligerents. This right is counterbalanced with the obligation to refrain from assisting the belligerents' war efforts.

If a state declares itself neutral, it is entitled to immunity from attack, and the territory of the neutral state is inviolable. Per Article 2 of the Convention, "[b]elligerents are forbidden to move troops or convoys of either munitions of war or supplies across the territory of a neutral Power". It is also prohibited to conduct hostilities within neutral states' territory; and Article 3 prohibits the belligerents from using communications installations on the territory of the neutral State purely for military purposes. Korns and Kastenberg define cyber neutrality as "the right of any nation to maintain relations with all parties engaged in a cyber conflict", and postulate that "to remain neutral in a cyber conflict a nation cannot originate a cyber attack, and it also has to take action to prevent a cyber attack from transiting its Internet nodes."[16]

Articles 2 and 3 of the Hague Convention create peculiar legal outcomes when applied to Internet communications and cyber attacks. Cyber attacks challenge neutrality on two levels. Firstly, can cyber attacks be construed as troop movements? If the effects of the attack cause death or damage, the author of this article would be inclined to give an affirmative answer. Secondly, the exclusion of military use of communications installations might have been reasonable in 1907 when such a ban could have been easily enforced.

Unfortunately, the architecture of Internet does not facilitate neutrality. The internet is a global network of networks encompassing the private and public sector. Network connections are not restricted to one territory as the transmitted information transcends jurisdictions. For example, an email sent from the jurisdiction of State A could pass through the networks of States C, D and E before reaching the recipient in State B.[17]

---

[16] **S. W. Korns & J. E. Kastenberg.** 2008–2009. Georgia's Cyber Left Hook. – Parameters, Winter, p. 62. The article gives an overview of problems of cyber neutrality in relation to the Georgia–Russia conflict of 2008.

[17] Cloud computing will create even more peculiar situations. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS), thus creating possible scenarios where a

As the Internet is not a "series of tubes", as infamously proclaimed by US Senator Ted Stevens,[18] self-contained military networks are not viable because they would go against the general architecture of Internet. Such networks could be built but their efficiency would most probably be hampered without a connection to the Internet and difficult to maintain in military operations that go beyond the physical restrictions of peacetime infrastructure. The military would most probably want to use the Internet as a backup communications system in case of an armed conflict. In the remote possibility of a cyber war, the belligerents' military action would not be confined to military networks but would most likely also be conducted in "civilian networks".

It would seem that cyber attacks are in conflict with the law of neutrality and raise the question of whether cyber attacks can be conducted with such precision and sophistication that neutral states would not be maliciously affected. The risks for a neutral state are high: it could be facilitating the war effort of belligerents by use of its networks unbeknownst to itself.

3.2. Cyber Attacks as Weapons Systems and Related Restrictions

A feasible solution could be the equation of cyber attacks or such capabilities with weaponry, in which case the norms applicable to the means of warfare could be applied to cyber attacks. The US Operational Law Handbook eloquently states that the "use of various forms of information operations generally requires the same legal analysis as any other method or means of warfare."[19] Use of weapons is subject to concrete restrictions under LOAC. The ICJ has opined that two fundamental customary law restrictions apply to weapons. First of all, "[s]tates must never make civilians the object of attack and must consequently never use weapons that are incapable

person is in the jurisdiction of State A, but uses either infrastructure, a platform or software that is located in the jurisdiction of State B. This creates a possibility where a cyber attack by an individual in State A against State C is prima facie attributed automatically to State B and even in this scenario the attack data could cross different jurisdictions before reaching its target. **SearchCloudComputing.com.** 2010. Definitions – Cloud Computing. 5 April. <searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html>.

[18] **K. Belson.** 2006. Senator's Slip of the Tongue Keeps on Truckin' Over the Web. – New York Times. 17 July. <www.nytimes.com/2006/07/17/business/media/17stevens.html>.

[19] **The Judge Advocate General's Legal Center & School, International and Operational Law Department**. 2008. Operational Law Handbook. Charlottesville, VA: US Army, p. 149 (**JAG School** 2008).

of distinguishing between civilian and military targets".[20] Secondly, "it is prohibited to cause unnecessary suffering to combatants; it is accordingly prohibited to use weapons causing them such harm or uselessly aggravating their suffering. ... [S]tates do not have unlimited freedom of choice of means in the weapons they use."[21]

The first restriction, an affirmation of the applicability of the principle of distinction, runs again counter to the general nature and structure of the Internet. The principle of distinction requires that belligerents always be capable of distinguishing between civilians and combatants, civilian objects and military objects.[22] In conjunction with the principle of proportionality, belligerents are obliged to minimise collateral damage to civilians and civilian objects when attacking military objects. This also obliges the belligerents to abstain from attack if the damage of the attack would be disproportionate to the military advantage gained.

The crux of the matter seems to be that if cyber attacks could be considered as weapons, then they can be employed during the conduct of hostilities and they must be aimed at specific military targets so as not to be indiscriminate. As with conventional weaponry, cyber attacks could be employed in an indiscriminate manner.

A belligerent could be tempted to initiate large-scale cyber attacks against the networks of other belligerents. But without the ability to distinguish between targets this attack would be indiscriminate. Another possibility is the so-called "hope and pray" attack where a belligerent launches a cyber attack of low sophistication in the hope that the civilian networks would not be affected. There is no foolproof segregation between public or private, military or civilian networks on the Internet as it is inherently dual-use. Creating a cyber attack that is fully in compliance with the principle of distinction requires high levels of sophistication which still might not guarantee the avoidance of knock-on effects to civilian systems and to civilians. Employing cyber attacks of low sophistication could run the risk of an indiscriminate attack.

On the flipside, modern technology is increasingly utilizing electronic circuitry and control software that can be compromised by cyber attacks or hacking.[23] Even though modern technology is far away from the dystopia

---

[20] *Nuclear Weapons*, para. 78.

[21] *Ibid.*

[22] AP I, Articles 48 and 52(2).

[23] For example, cars, pacemakers, fridges etc contain electronic control units (ECU) which oversee the functions of different electronic components. The BBC News reported recently that a group of researches were successfully able to hack into ECUs of cars enabling them

seen in the Terminator movies,[24] militaries all over the world are starting to employ combat function robots and sentry guns.[25] Some of these are autonomic robots – they can distinguish between friends or foes and are fitted with weapons.[26] Thus some combat robots are already programmed to act in accordance with the principle of distinction. The IT security of combat robots is essential since where there is IT capability, there are also vulnerabilities and the adversary can launch a cyber attack that modifies the robots to conduct "friendly fire" or force them to act indiscriminately. Unforeseen consequences may also rear their ugly head when the robot confuses its target sets owing to human programming error.

Additionally, when cyber attacks are regarded as weapons systems, LOAC prescribes an obligation to evaluate the new weapons to determine whether the employment of the new weapon would, under some or all conditions, be prohibited or restricted under the standards of humanitarian, or some other category of international law.[27] Unfortunately states have no obligation to publicise these findings; thus the majority of these analyses are not available to the general public. As far as the author is aware, there is no public information at present on whether states have conducted such research on specific cyber capabilities.

Notwithstanding the abovementioned caveats, cyber attacks could theoretically be executed in line with the LOAC requirements against military objects such as the belligerents' command and control centres, military

---

to remotely shut off car engines, brakes and make the instruments give false readings. **BBC News.** 2010. Hack Attacks Mounted on Car Control Systems. 17 May. <www.bbc.co.uk/news/10119492>.

[24] **J. Markoff.** 2009. Scientists Worry Machines May Outsmart Man. – New York Times. 25 July. <www.nytimes.com/2009/07/26/science/26robot.html>.

[25] The Phalanx Close-In Weapons System is a fast-reaction, rapid fire 20-millimeter gun system "capable of autonomously performing its own search, detect, evaluation, track, engage and kill assessment functions". **United States Navy.** 2011. Phalanx Close-In Weapons System. – United States Navy Fact File. 21 November. <www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2>.

[26] The iRobot 710 Warrior can carry payloads weighing more than 150 pounds and has some autonomous functionality. **iRobot**. 2010. iRobot 710 Warrior. Product Details. <www.irobot.com/gi/ground/710_Warrior>. The defunct Gladiator Tactical Unmanned Ground Vehicle besides being weaponized was supposed to employ scouting, reconnaisance, surveillance and target acquisition capabilities. **GlobalSecurity.** 2006. Gladiator Tactical Unmanned Ground Vehicle. – GlobalSecurity.org. 16 January. <www.globalsecurity.org/military/systems/ground/gladiator.htm>. For a general overview on different combat robots, their uses in the field and discussion on ethical and legal questions, see **P. W. Singer.** 2009. Wired for War: The Robotics Revolution and Conflict in the 21st Century. New York, Penguin Press.

[27] AP I, Article 36.

communications networks, combatants etc.; but the commanders' responsibility with regard to precautions in attack is probably relatively higher than the standards applied to conventional weapons.

3.2.1. Conventional, Economic, Dual-use Targets and Targets Containing Dangerous Forces

The principle of distinction restricts the totality of permissible targets to combatants or military objects while protecting the civilian population as much as possible. But what can be considered as concrete targets for cyber attacks? It is most probably the same set of targets that are available to conventional kinetic weapons – combatants, military targets, civilians taking direct part in hostilities, dual-use objects etc.

If a "cyber target" meets the criteria set out in AP I Article 52(2), it is a legitimate target for cyber attack. Before launching an attack against the chosen target, an assessment must be made whether the attack is in conformity with the principles of distinction and proportionality.[28] Thus, aiming cyber attacks against combatants is permissible, and when conducting attacks against military targets, the target must considerably contribute to military action and provide a definite military advantage (e.g. command and control networks).[29] Difficulties arise when the cyber attack does not bring forth any physical destruction, because the affected adversary must conclude whether such action is a military action or just an inconvenience. If the purpose is only to cause inconvenience, this does not cross the threshold of a military attack.

But what would be the guidance for military planners and targeting officers? The principle of distinction is under fire because cyber attacks open a door to operations that are not directed at military targets, but which can nevertheless impede or disable such targets. The universality and suitability of cyber attacks can create a counterproductive environment where LOAC is pushed aside in favour of political or military expediency. Military planners could be tempted to target sets which do not conform to LOAC standards but which contribute to the achievement of political or strategic objectives.

One such example is the broad interpretation of "definite military advantage" contained in AP I Article 52(2). The United States of America

---

[28] AP I, Article 52 notes that civilian objects shall not be the object of attack and that attacks shall be limited to military objects. Article 57(2)(a)(i) demands that the attackers must do everything feasible to verify that the objects to be attacked are not civilian objects, but military objects.

[29] AP I, Article 52(3).

considers certain economic targets to be covered by the definition when such targets "indirectly but effectively support and sustain the enemy's warfighting capability."[30] Such an interpretation can blur the lines between participation in the general war effort and direct participation in hostilities, and might erode the protection afforded to a civilian population. If the belligerent reasons that making the adverse party unable to pay wages to its armed forces is military tactics, is it then acceptable and legal to target the adversary's banking system or the stock exchange to force the adversary's economy into submission? Unfortunately, there is no clear answer with regard to this issue, other than to weigh the pros and cons on a case by case basis and to interpret the criteria of Article 52(2) in good faith.

When the principle of proportionality is added to the mix, then there is an obligation to balance the damage caused to the civilian population or civilian objects with the military advantage gained from the attack.[31] The attack is not illegal if the incidental effects of the attack are not excessive to the military advantage anticipated. The problem with cyber attacks is, as referred to above, the fact that the effects of the attack are unpredictable and could endanger the civilian population. These are called knock-on effects which 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".[32] The US Operational Law Handbook contains an example of conducting a cyber attack against an electrical grid, which would have an effect of degrading the command and control systems of the adversary, but at the same it may

> have the effect of shutting down electricity for civilian facilities with follow-on effects such as: unsanitary water and therefore death of civilians and the spread of disease because the water purification facilities and sewer systems don't work; death of civilians because the life support systems at emergency medical facilities fail; or death of civilians because traffic accident increase due to a failure of traffic signals.[33]

A recent study conducted by the North American Electric Reliability Corporation identified cyber attacks as one of the vulnerabilities of the electrical

[30] **JAG School** 2008, p. 149.

[31] AP I, Article 57(2)(a)(iii).

[32] **E. T. Jensen.** 2003. Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations? – American University International Law Review, Vol. 18, p. 1177.

[33] **JAG School** 2008, p. 151.

grid.[34] So far there has been only anecdotal evidence regarding attacks against electrical grids,[35] but the analysis of the mentioned study suggests that the risk is clear. For example the study foresees that a cyber attack or simultaneous cyber attacks could facilitate long-term damage to key components and systems. Such damage could bring forth an outage that would "affect a wide geographic area and cause large population centers to lose power for extended periods".[36] If such acts were conducted by belligerents then adequate means must be employed so as not to endanger the civilian population[37] or cause harm disproportionate to the military advantage.[38]

If a commander wants to utilize cyber attacks, he or she must also take precautions in the attack during the planning of the operation – assess the damage which might be caused by the attack, foresee positive and negative causal sequences, and seek mitigating actions against such harmful effects. But a cyber attack can also be an enabler during military operations as it may help to decrease the incidental damage by turning off certain infrastructure, or contain the incidental effects of cyber attacks (Schmitt gives an example

---

[34] **North American Electric Reliability Corporation.** 2010. High-Impact, Low-Frequency Event Risk to the North American Bulk Power System: A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop. – NERC. June. <www.nerc.com/files/HILF.pdf> (hereinafter **NERC** 2010).

[35] The Wall Street Journal has reported that hackers from China and Russia have penetrated the computer systems of the U.S. electrical grid and have also left behind a computer code that could be used for disrupting the system. Although no damage was afflicted there existed speculations that these backdoors were to be utilised during conflict. **S. Gorman.** 2009. Electricity Grid in U.S. Penetrated By Spies. – The Wall Street Journal. 8 April. <online.wsj.com/article/SB123914805204099085.html>. Worries over the security of the electrical grid against cyber attacks were already prevalent in 2008 when the U.S. Congress considered legislation that would have given more authority to the federal government over the electric companies. See **S. Condon.** 2008. 'Cybersecurity' Worries Spur Congress to Rethink Electrical Grid. – CNET News, Politics & Law. 12 September. <news.cnet.com/8301-13578_3-10040101-38.html>. The Center for Strategic and International Studies has published a paper that concentrates on the issue why electrical grids are priority targets and contains evidence of successful laboratory tests conducted against computer systems of electrical grids. See **J. A. Lewis.** 2010. The Electrical Grid as a Target for Cyber Attack. – Center for Strategic and International Studies. March. <csis.org/files/publication/100322_ElectricalGridAsATargetforCyberAttack.pdf>.

[36] **NERC** 2010, p. 26.

[37] For example by way of disabling objects indispensable to survival of civilian population. AP I, Article 54.

[38] AP I, Article 57(2)(a)(iii).

that instead of bombing an airport it is possible to disturb the operation of the flight control systems).[39]

Dual-use targets are targets that serve both military and civilian purposes, and they are closely intertwined with collateral damage. Such targets are, for example, airports, railways, electrical grids, communications systems etc.[40] Dual-use targets are also such objects that normally are used by the civilian population, but by necessity are also used by the military. If such an object is used for military purposes, the object becomes a military objective that can be targeted. When targeting dual-use systems, all LOAC norms and principles regarding the conduct of hostilities are applicable. Such objects can be targeted by conventional weapons but also by cyber attacks, even though targeting such installations is usually contentious and sensitive, and therefore calls for meticulous planning. Cyber attacks might provide more flexibility for the commanders as, for example, they can disable the flight control systems of an airport, but leave the runways and other objects intact. As O'Donnell and Kraska opined in 2003, "information warfare may prove to be an effective means of coercion that is more adept at insulating civilians from the dangerous kinetic effects of war".[41]

Besides dual-use targets, cyber attacks could facilitate the execution of attacks against installations and infrastructure containing dangerous forces.[42] Under LOAC, objects such as dykes, dams, nuclear power plants are granted special protection because an attack on such facilities may unleash dangerous forces and cause serious losses among the civilian population. The aim of the law is to protect against the release of dangerous forces as these would most likely harm the civilian population (radiation, flooding). Nevertheless, the prohibition is not absolute as belligerents may attack such installations if precautions are taken to eliminate the possibility of the release of dangerous forces. Cyber attacks could be problem solvers in this regard. Even though it is advisable to keep these facilities disconnected from the Internet, the reality seems to be the opposite. Many critical infrastructure installations such as water treatment facilities, electrical power grids, oil and gas pipelines would most likely employ Supervisory Control and Data

[39] **Schmitt** 2002, p. 394.

[40] **Schmitt** 2002, p. 384.

[41] **B. T. O'Donnell & J. C. Kraska.** 2003. Humanitarian Law: Developing International Rules for the Digital Battlefield. – Journal of Conflict and Security Law, Vol. 8, No. 1, p. 134.

[42] AP I, Article 56.

Acquisition (SCADA) accessibility.[43] SCADA computer systems monitor and control different industrial processes (transmission of electricity, transportation of oil and gas, etc.) and it is recommended that they be disconnected from the Internet. Nevertheless, connecting SCADA systems to the Internet gives the administrators the possibility to conduct maintenance and other actions remotely and as such it is likely that security will be undermined by the comfort factor. Although cyber attacks can be conducted over the Internet against critical infrastructure, the SCADA systems can be enabled to conduct operations in such a way as to neutralise the chances of launching dangerous forces and give the attacking belligerent a new tool for the successful completion of their mission.

3.2.2. Indiscriminate Attacks

The principle of distinction outlaws the use of indiscriminate attacks. These not only comprise attacks that are not directed at a specific military object; the prohibition also bars the employment of a method or means of combat which cannot be directed at a specific military object or the effects of which cannot be limited.[44] The latter seems to be the main challenge to the legality of cyber attacks.

The difficulty of cyber attacks is that, to be conducted legally, they have to be of high sophistication so as not to violate the requirements of LOAC. But a cyber attack can easily, either intentionally or through a human or technological mistake, transform into an indiscriminate attack. If a belligerent programs a virus the sole purpose of which is to replicate in IT-systems, infect as many computers as possible and destroy all the data on infected machines, then it would be hard to argue that such a cyber attack is in accordance with LOAC. In this example, the cyber attack (virus) would be uncontrollable and spread through military and civilian systems alike, constituting an indiscriminate attack. Therefore, a cyber attack must be of high sophistication and adhere to the principle of distinction and to LOAC in general.

But then again, even with the best programming skills, there is still the possibility of human error and unforeseen consequences. Even if it were possible to construct a cyber attack that *prima facie* is legal under LOAC, the uncertainty of unforeseen consequences or knock-on effects would not be

[43] **Wikipedia**. 2010. SCADA. <en.wikipedia.org/wiki/SCADA>; **Centre for the Protection of National Infrastructure.** 2010. Supervisory Control and Data Acquisition (SCADA). <www.cpni.gov.uk/advice/infosec/business-systems/scada/>.

[44] AP I, Article 51(4).

eliminated. Notwithstanding the architecture of the Internet, which does not distinguish between military and civilian networks, there is also the indeterminacy of different operating systems and connections between both user-sides of the Internet. Thus, the employment of cyber attacks would, most of the time, be in conflict with the prohibition on endangering the civilian population.

For example, there is evidence from NATO's history of cyber attacks that have been planned but not executed. In the first case, there was a plan to launch a cyber attack against certain bank accounts in Switzerland belonging to Slobodan Milošević. The train of thought involved went as follows: if Milošević cannot fund the conflict and the armed forces subordinated to him, the conflict would die out sooner. In the end, NATO did not launch such a cyber attack as there was no guarantee that the attack would have distinguished between the accounts of Milošević and those of non-affected persons.[45] The case also brings up an interesting question which is still unanswered to this date – is it legal to conduct cyber attacks against the assets of the belligerent which are not located on the territory of either party to the conflict? Even more, is it legal under LOAC to attack the assets of belligerents on a neutral state's territory? *Lex lata* is more likely to answer both questions in the negative but cyber attacks could definitely modify our understanding of the law in this regard if such operations were to be conducted.

Kelsey gives an example that

> [d]uring NATO's Kosovo campaign, NATO air war planners devised a cyber attack to insert false messages and targets into the Serbian military's air-defense command network. NATO could have delivered the weapon via the host country's Internet or possibly could have "beamed" the weapon to the target directly from a NATO warplane. This attack would have limited Serbia's ability to accurately target NATO warplanes, but, if improperly planned, such a cyber attack could have put civilian targets at risk, with the air-defense network possibly confusing relief planes or commercial aircraft for military targets. Fuel-depleted missiles launched at false targets could have fallen on civilian structures, such as homes, hospitals, and schools. NATO did not ultimately launch this cyber attack, but in the future NATO

[45] **Jensen** 2003, p. 1146; **W. M. Arkin.** 1999. The Cyber Bomb in Yugoslavia. – Washington Post. 25 October. <www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm>; **E. Morozov.** 2010. Battling the Cyber Warmongers. – The Wall Street Journal. 8 May. <online.wsj.com/article/SB10001424052748704370704575228653351323986.html>.

> commanders might be tempted to risk additional harm to the civilian population to reduce risk to the lives of NATO pilots.[46]

When viewing the current operations of NATO, the last sentence might not reflect reality, but on the whole, it is an exemplary account of the problems for operators and lawyers who are tasked with the operational evaluation of the weapon. Even though the Kosovo campaign is over 10 years old and the technology has advanced in leaps and bounds, the above is a stark and sobering reminder of the weak points of cyber attacks.

A more recent example is the Conficker worm which infects computers using advanced malware techniques.[47] When the worm takes over a computer it registers it onto a network called the "botnet", which is a collection of compromised computers running software under a common command-and-control server. Once a hijacked computer is on the botnet, the owner of the botnet can give commands to the hijacked computers and pull data from them. This simplifies the work of cyber criminals and, at the same time, places an unprecedented amount of computing power into the hands of criminals who can conduct Distributed Denial of Service (DDoS)[48] attacks against different targets. DDoS attacks are conducted when the targeted server is bombarded with queries from different sources in such quantities that the available bandwidth for the server is overloaded. The result is that the server cannot process the requests and slows down or goes offline. This can also compromise the server and the data within the computer system. Estimates differ, but the worm could have infected from nine to 15 million computers. The worm breached the French Navy (forcing aircraft at several airbases to be grounded), the United Kingdom Ministry of Defence (including computers on Royal Navy warships and submarines), Bundeswehr, the Manchester City Council, the Greater Manchester Police, the House of Commons and numerous home computers. It is not certain what the Conficker worm is or what it was supposed to do, but if it had been a military cyber attack with physical damages and consequences, it is obvious that the effects

---

[46] **J. Kelsey.** 2008. Hacking Into International Humanitarian Law. – Michigan Law Review, Vol. 106, pp. 1434–1435.

[47] **Wikipedia.** 2010. Conficker. <en.wikipedia.org/wiki/Conficker>; **Microsoft.** 2010. Protect Yourself From Conficker. <www.microsoft.com/en-gb/security/pc-security/conficker.aspx>; **McAfee.** 2010. W32/Conficker.worm. <vil.mcafeesecurity.com/vil/content/v_153464.htm>.

[48] **Wikipedia.** 2010. Denial-of-service Attack. <en.wikipedia.org/wiki/Denial-of-service_attack>.

are indiscriminate as the worm cannot distinguish between civilian and military targets.

3.3. Combatants and Direct Participation in Hostilities

Combatants are permitted to take part in hostilities, while civilians are afforded protection so long as they do not take direct part in the hostilities.[49] Direct participation can involve causing damage to the belligerent or supplying the enemy's armed forces.[50] The ICRC has released guidelines which establish a three-pronged test for direct participation. Firstly, the act must be likely to adversely affect military operations or the military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack. Secondly, there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part. Finally, the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another.[51]

Due to the characteristics of the field, modern weapons and IT systems are seldom operated exclusively by the members of armed forces. The phenomenon is not constrained to cyber attacks but it is even more pressing in the field of drone warfare where there have been reports of employees of intelligence agencies flying operations.[52] Cyber attacks and direct participation are also specifically elaborated in the HPCR Manual on International Law Applicable to Air and Missile Warfare. The Manual considers an example of direct participation as "[e]ngaging in electronic warfare or computer network attacks targeting military objectives, combatants or civilians directly participating in hostilities, or which is intended to cause death or injury to civilians or damage to or destruction of civilian objects."[53]

It is relevant to note the trend because at the heart of LOAC is the notion of combatant privilege and civilian immunity. Not all civilians who conduct

---

[49] AP I, Articles 48, 50(1), 51 (2) and 52(1).

[50] AP I, Article 51(3).

[51] **N. Melzer.** 2009. Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. Geneva: ICRC, p. 46.

[52] **Human Rights Council**. 2010. Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston. – Study on Targeted Killings. A/HRC/14/24/Add.6, paras 18–20 (hereinafter **HRC** 2010).

[53] **HPCR.** 2009. Manual on International Law Applicable to Air and Missile Warfare. Bern, HPCR, p. 15.

activities with the belligerents are taking direct part in hostilities. More and more civilians and civilian experts are employed by the armed forces to be responsible for the so-called non-military duties and for providing the necessary know-how for operational effectiveness. The other side of the coin is that the IT operators could be geographically situated "thousands of miles away from the battlefield, and undertake operations entirely through computer screens and remote audio-feed".[54] This spatial disconnect with the real combat space could give facilitate the development of a so-called "PlayStation mentality"[55] where the operator is desensitised from the consequences of his or her actions, which then can also bring forth abuses of power and breaches of law.

The trend of civilians or sub-contractors accompanying armed forces seems to be increasing because of the complexity of the technology used by the armed forces. The need is understandable, but also increases the risk that civilians working in the armed forces, especially in the area of operations, will be considered to be direct participants in hostilities.[56] And even more so, when civilians or contractors conduct the operations on the orders of commanders and initiate or control the cyber attacks. As such, civilian IT specialists run the risk of becoming legitimate targets. This uncertainty creates a harmful situation for LOAC as it can erode the humanitarian guarantees set forth for the civilian population and for civilians accompanying the armed forces, because belligerents cannot make a reasonable distinction between combatants and civilians.[57] Ideally, members of the armed forces should conduct the cyber attacks, but this does not seem to be a realistic expectation. Watts argues that

> as an irreducible minimum of lawful participation in CNA, state affiliation preserves the spirit and intent of the traditional criteria of combatant status, including the dual principles of distinction and discipline, while offering

[54] **HRC** 2010, para. 84.

[55] *Ibid.*

[56] **Schmitt** 2002, p. 384; **Dörmann** 2001; **ICRC** 2003; **K. Dörmann.** 2004. Applicability of the Additional Protocols to Computer Network Attacks. – ICRC. Conduct of Hostilities, Information Warfare. 19 November. < http://www.icrc.org/eng/resources/documents/misc/68lg92.htm>, pp. 8–9.

[57] For an in-depth analysis of the issue see **J. R. Heaton.** 2005. Civilians At War: Reexamining the Status of Civilians Accompanying the Armed Forces. – Air Force Law Review, Vol. 57, pp. 155–208.

> states workable options to develop capacity for what is perhaps unfortunately, yet inevitably, a new domain of warfare.[58]

Recent conflicts have brought forward contentious examples of civilian participation in hostilities. For example, a case in point is the Conficker worm mentioned above, which involves participation by ignorance, in which case either home computers or business computers are hijacked and bandwidth is used for the facilitation of cyber attacks. The Project Grey Goose has prodeced two reports on the Georgia–Russia conflict of 2008 which state that botnets were used to conduct DDoS attacks against Georgian websites and the majority of the owners of the hijacked computers were unaware that they were participating in hostilities.[59]

The other side of the coin is the so-called "patriotic hacking" where computer users voluntarily, willingly and knowingly allow their computers to be used or they themselves conduct actions harmful to the belligerent. This was prevalent again during the 2008 Georgia–Russia conflict where certain Russian message boards provided simple instructions on how to attack Georgian websites. Evgeny Morozov has shown that with some vested interest it is fairly simple to take part in a cyber attack:

> Not knowing exactly how to sign up for a cyberwar, I started with an extensive survey of the Russian blogosphere. … As I learned from this blog post … all I needed to do was to save a copy of a certain Web page to my hard drive and then open it in my browser …. In less than an hour, I had become an Internet soldier. I didn't receive any calls from Kremlin operatives; nor did I have to buy a Web server or modify my computer in any significant way. If what I was doing was cyberwarfare, I have some concerns about the number of child soldiers who may just find it too fun and accessible to resist.[60]

The phenomenon is not confined to the Georgia–Russia conflict, as even during the Operation Cast Lead in Gaza there were instructions from both

---

[58] **S. Watts.** 2010. Combatant Status and Computer Network Attack. – Virginia Journal of International Law, Vol. 50, No. 2, p. 396. The article as a whole gives an excellent overview of issues regarding combatant status in cyber attacks.

[59] **Project Grey Goose.** 2007. Phase I Report: Russia/Georgia Cyber War – Findings and Analysis. 17 October. <www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>; **Project Grey Goose.** 2009. Phase II Report: The Evolving State of Cyber Warfare. 20 March. <www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report>.

[60] **E. Morozov.** 2008. An Army of Ones and Zeroes: How I Became a Soldier in the Georgian-Russian Cyberwar. – Slate.com. 14 August. <www.slate.com/id/2197514>.

Pro-Palestinian and Pro-Israeli civilian groups on how to attack the other party's websites and networks.[61]

Both participation by ignorance and "patriotic hacking" show an alarming upward trend in voluntary civilian interest in conducting actions harmful to the enemy.[62] The aim of this paper is not to analyse whether the actions above constitute direct participation or not, or whether there is state involvement in coordinating the civilians. But these examples highlight at least two concerns. Firstly, the alarming ease with which civilians can take part in hostilities either involuntarily or knowingly. Secondly, the author would venture to suggest that civilians who conduct cyber attacks against belligerents are not aware of their obligations under LOAC and do not understand what such participation can bring in worst case scenarios – in some cases, they can either be targeted for the duration of their direct participation or prosecuted for direct participation later on.

3.4. Ruses and Perfidy

Prohibition of perfidy is an important building block of LOAC. Ruses of war are permitted but there is a fine line between a legal ruse and a perfidious act. AP I defines perfidy as the feigning of protected status with the intent to kill, injure or capture an adversary.[63] A permissible cyber ruse could be the communication of incorrect information on the location and manoeuvres of troops, and the forging of the enemy's reconnaissance database.[64] Deceptive use of codes and signals given to medical transport by the International Civil Aviation Organisation would constitute cyber-perfidy,[65] as would, most likely,

---

[61] **N. Shachtman.** 2009. Wage Cyberwar Against Hamas, Surrender Your PC. – Wired. 8 January. <www.wired.com/dangerroom/2009/01/israel-dns-hack/>.

[62] A. K. Cronin foresees that "[m]ost important is the 21st century's levée en masse, a mass networked mobilization that emerges from cyber-space with a direct impact on physical reality. Individually accessible, ordinary networked communications such as personal computers, DVDs, videotapes, and cell phones are altering the nature of human social interaction, thus also affecting the shape and outcome of domestic and international conflict." **A. K. Cronin.** 2006. Cyber-Mobilization: The New Levée en Masse. – Parameters, Summer, p. 77. D. Brown opines that cyber-levée en masse is not possible because most cyber attacks will be conducted against targets not resident in the non-occupied country and as such "operations go beyond the purpose and purview of the levée en masse, which is intended to provide for spontaneous civilian defense of their homeland. There is no legal precedent for a levée en masse bringing the fight to the attacker's homeland." **D. Brown.** 2006. A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. – Harvard International Law Journal, Vol. 47, p. 192.

[63] AP I, Article 37(1).

[64] **Dörmann** 2004, p. 10.

[65] *Ibid.*

the creation of a lifelike 3D live-image of the adversary's military or political leader giving the troops the order to surrender or to commit war crimes or serious violations. With the growth of computing power, more methods and means will be invented that can be used on the battlefield, but the line between cyber ruse and cyber perfidy could prove to be a blurry one indeed.

4. Conclusion

The main characteristic of the Internet is its structural anarchy; advancements in technology show that this will evolve into more uncertainty with cloud computing. There is no working distinction between different military or civilian networks; thus, theoretically, everything is possibly connected to everything. With the use of cloud computing, there are viable scenarios where the data of terrorist groups or belligerents are stored in the same cloud side by side, unbeknownst to the parties. Taking legal restrictions into account, the conduct of cyber attacks is difficult and challenging but possible. On a positive note, cyber attacks can provide working, even non-lethal, alternatives to kinetic weapons and diversify the methods available to military operational planners.

The question still remains – is the current law sufficient to address cyber attacks? A strong argument is made for the existing LOAC to be applied to cyber attacks. Even though the law did not foresee such weapons upon its inception, the fundamental principles and norms of LOAC are flexible enough to facilitate the extension of the LOAC umbrella to cover cyber attacks and prevent the emergence of lacunae. Some challenges remain – when is a cyber attack an "attack" under LOAC and when is it only a hindrance? The lack of legally relevant state practice is a concern in this field, but does not warrant the rush to a new legal instrument. The unity and indivisibility of LOAC's body of law is capable of dealing with this phenomenon on paper. Only practice will show whether it is also capable of doing that in reality.

Disclaimer

This chapter is based on the presentation made at the conference "Historical and Contemporary Perspectives on the Law of Armed Conflict", held by the Martens Society and the Estonian National Defence College, 9 October 2009. All the views expressed and possible mistakes made in this chapter are the author's alone. All web links were checked and current on 13 March 2012.

Treaties

Hague Convention (II) with Respect to the Laws and Customs of War on Land, adopted 29 July 1899, entered into force 4 September 1900.

Hague Convention (IV) respecting the Laws and Customs of War on Land, adopted 18 October 1907, entered into force 1 January 1910.

Hague Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land, adopted 18 October 1907, entered into force 26 January 1910.

Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), adopted 8 June 1977, entered into force 7 December 1978, 1125 UNTS 3.

Cases

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), ICJ Reports (1996) 226.

Bibliography

Arkin, W. M. 1999. The Cyber Bomb in Yugoslavia. – Washington Post. 25 October. <www.washingtonpost.com/wp-srv/national/dotmil/arkin.htm>.

BBC News. 2010. Hack Attacks Mounted on Car Control Systems. 17 May. <www.bbc.co.uk/news/10119492>.

Belson, K. 2006. Senator's Slip of the Tongue Keeps on Truckin' Over the Web. – New York Times. 17 July. <www.nytimes.com/2006/07/17/business/media/17stevens.html>.

Benatar, M. 2009. The Use of Cyber Force: Need for Legal Justification? – Goettingen Journal of International Law, Vol. 1, pp. 375–396.

Brown, D. 2006. A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict. – Harvard International Law Journal, Vol. 47, pp. 179–221.

Centre for the Protection of National Infrastructure. 2010. Supervisory Control and Data Acquisition (SCADA). <www.cpni.gov.uk/advice/infosec/business-systems/scada/>.

Condon, S. 2008. "Cybersecurity" Worries Spur Congress to Rethink Electrical Grid. – CNET News, Politics & Law. 12 September. <news.cnet.com/8301-13578_3-10040101-38.html>.

Cronin, A. K. 2006. Cyber-Mobilization: The New Levée en Masse. – Parameters, Summer, pp. 77–87.

Department of Defense. 2009. Dictionary of Military and Associated Terms. – Joint Publication 1–02. 12 April 2001, as amended through 31 October 2009.

Dörmann, K. 2001. Computer Network Attack and International Law – Extract from The Cambridge Review of International Affairs "Internet and State Security Forum". Trinity College, Cambridge, UK, 19 May. <www.icrc.org/eng/resources/documents/misc/5p2alj.htm>.

Dörmann, K. 2004. Applicability of the Additional Protocols to Computer Network Attacks. – ICRC. Conduct of Hostilities, Information Warfare. 19 November. <www.icrc.org/eng/resources/documents/misc/68lg92.htm>.

GlobalSecurity. 2006. Gladiator Tactical Unmanned Ground Vehicle. 16 January. <www.globalsecurity.org/military/systems/ground/gladiator.htm>.

Gorman, S. 2009. Electricity Grid in U.S. Penetrated By Spies. – The Wall Street Journal. 8 April. <online.wsj.com/article/SB123914805204099085.html>.

Heaton, J. R. 2005. Civilians At War: Reexamining the Status of Civilians Accompanying the Armed Forces. – Air Force Law Review, Vol. 57, pp. 155–208.

Hollis, D. 2007. Why States Need an International Law for Information Operations – Lewis & Clark Law Review, Vol. 11, pp. 1023–1061.

HPCR. 2009. Manual on International Law Applicable to Air and Missile Warfare. Bern: HPCR, p. 15.

Human Rights Council. 2010. Report of the Special Rapporteur on Extrajudicial, Summary or Arbitrary Executions, Philip Alston. – Study on Targeted Killings. A/HRC/14/24/Add.6.

ICRC. 2003. Direct Participation in Hostilities under International Humanitarian Law. Report. September. <www.icrc.org/ara/assets/files/other/direct_participation_in_hostilities_sept_2003_eng.pdf>.

iRobot. 2010. iRobot 710 Warrior. Product Details. – iRobot Corporation. 2010. <www.irobot.com/gi/ground/710_Warrior/>.

Jensen, E. T. 2003. Unexpected Consequences from Knock-On Effects: A Different Standard for Computer Network Operations? – American University International Law Review, Vol. 18, pp. 1145–1188.

Kellenberger, J. 2009. Statement by ICRC president Jakob Kellenberger. 9 November.<www.icrc.org/eng/resources/documents/statement/geneva-convention-statement-091109.htm>.

Kelsey, J. 2008. Hacking Into International Humanitarian Law. – Michigan Law Review, Vol. 106, pp. 1427–1451.

Kodar, E. 2009. Computer Network Attacks in the Grey Areas of Jus ad Bellum and Jus in Bello. – Baltic Yearbook of International Law, Vol. 9, pp. 133–155.

Korns, S. W; Kastenberg, J. E. 2008–2009. Georgia's Cyber Left Hook. – Parameters, Winter, pp. 60–76.

Lewis, J. A. 2010. The Electrical Grid as a Target for Cyber Attack. – Center for Strategic and International Studies. March. <csis.org/files/publication/100322_ElectricalGridAsATargetforCyberAttack.pdf>.

Markoff, J. 2009. Scientists Worry Machines May Outsmart Man. – New York Times. 25 July. <www.nytimes.com/2009/07/26/science/26robot.html>.

McAfee. 2010. W32/Conficker.worm. <vil.mcafeesecurity.com/vil/content/v_153464.htm>.

Melzer, N. 2009. Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law. Geneva: ICRC.

Microsoft. 2010. Protect Yourself from Conficker. <www.microsoft.com/en-gb/security/pc-security/conficker.aspx>.

Morozov, E. 2008. An Army of Ones and Zeroes: How I Became a Soldier in the Georgian-Russian Cyberwar. – Slate.com. 14 August. <www.slate.com/id/2197514>.

Morozov, E. 2010. Battling the Cyber Warmongers. – The Wall Street Journal. 8 May. <online.wsj.com/article/SB10001424052748704370704575228653351323986.html>.

North American Electric Reliability Corporation. 2010. High-Impact, Low-Frequency Event Risk to the North American Bulk Power System: A Jointly-Commissioned Summary Report of the North American Electric Reliability Corporation and the U.S. Department of Energy's November 2009 Workshop. – NERC. June. <www.nerc.com/files/HILF.pdf>.

North Atlantic Treaty Organisation. 2010. NATO 2020: Assured Security; Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO. <www.nato.int/nato_static/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf>.

O'Donnell, B. T; Kraska, J. C. 2003. Humanitarian Law: Developing International Rules for the Digital Battlefield. – Journal of Conflict and Security Law, Vol. 8, pp. 133–160.

Ottis, R. 2009. On Definitions. – Conflicts in Cyberspace. 14 July <conflictsincyberspace.blogspot.com/2009/07/on-definitions.html>.

C. Pilloud & J. Pictet. 1987. Article 49. Definition of Attacks and Scope of Application. – Y. Sandoz *et al.* (eds). Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949. Geneva: Martinus Nijhoff, pp. 601–608.

Project Grey Goose. 2007. Phase I Report: Russia/Georgia Cyber War – Findings and Analysis. 17 October. <www.scribd.com/doc/6967393/Project-Grey-Goose-Phase-I-Report>.

Project Grey Goose. 2009. Phase II Report: The Evolving State of Cyber Warfare. 20 March. <www.scribd.com/doc/13442963/Project-Grey-Goose-Phase-II-Report>.

Schmitt, M. 2002. Wired Warfare: Computer Network Attack and Jus In Bello. – International Review of the Red Cross, Vol. 84, No. 846, pp. 365–399.

Schweppe, R. Statement by H. E. Ambassador Reinhard Schweppe. 9 November.

SearchCloudComputing.com. 2010. Definitions – Cloud Computing. 5 April. <searchcloudcomputing.techtarget.com/sDefinition/0,,sid201_gci1287881,00.html>.

Shachtman, N. 2009. Wage Cyberwar Against Hamas, Surrender Your PC. – Wired. 8 January. <www.wired.com/dangerroom/2009/01/israel-dns-hack/>.

Shackelford, S. J. 2009. From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. – Berkley Journal of International Law, Vol. 25, No. 3, pp. 191–250.

Singer, P. W. 2009. Wired for War: The Robotics Revolution and Conflict in the 21st Century. New York, NY: Penguin Press.

The Judge Advocate General's Legal Center & School, International and Operational Law Department. 2008. Operational Law Handbook. Charlottesville, VA: US Army.

United States Navy. 2011. Phalanx Close-In Weapons System. – United States Navy Fact File. 21 November. <www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2>.

Watts, S. 2010. Combatant Status and Computer Network Attack. – Virginia Journal of International Law, Vol. 50, pp. 391–447.

Wikipedia. 2010. Conficker. <en.wikipedia.org/wiki/Conficker>.

Wikipedia. 2010. Denial-of-service Attack. <en.wikipedia.org/wiki/Denial-of-service_attack>.

Wikipedia. 2010. SCADA. <en.wikipedia.org/wiki/SCADA>.