Military objectives in cyber warfare

Roscini, M.

This is an author's accepted manuscript of a chapter published by Springer in Ethics and Policies for Cyber Operations, edited by Glorioso, L. and Taddeo, M.

Full details of the published version are available at:

http://www.springer.com/gb/book/9783319452999

Military Objectives in Cyber Warfare

Marco Roscini[*]

Abstract: This Chapter discusses the possible problems arising from the application of the principle of distinction under the law of armed conflict to cyber attacks. It first identifies when cyber attacks qualify as 'attacks' under the law of armed conflict and then examines the two elements of the definition of 'military objective' contained in Article 52(2) of the 1977 Protocol I additional to the 1949 Geneva Conventions on the Protection of Victims of War. The Chapter concludes that this definition is flexible enough to apply in the cyber context without significant problems and that none of the challenges that characterize cyber attacks hinders the application of the principle of distinction.

1. The Principle of Distinction in the Law of Armed Conflict

Article 48 of the 1977 Protocol I additional to the 1949 Geneva Conventions on the Protection of Victims of War provides for the 'basic' obligation of the belligerents to 'at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly [to] direct their operations only against military objectives'. This obligation of distinction applies both in international and non-international armed conflicts (Henckaerts and Doswald-Beck 2005 (vol. I): 3) and its customary status has been firmly upheld by national and international courts. In particular, according to the 1996 International Court of Justice (ICJ)'s Advisory Opinion on the *Legality of the threat or use of nuclear weapons*, the obligation to protect the civilian population and civilian objects is a 'cardinal' principle of international humanitarian law (*Legality of the Treat or Use of Nuclear Weapons*, Advisory Opinion, 1996, para 78). The International Criminal Tribunal for the former Yugoslavia (ICTY) confirmed that 'it is now a universally recognised principle . . . that deliberate attacks on

[*] Professor of International Law, Westminster Law School. This Chapter is largely based, with some amendments and updates, on the author's book, Roscini 2014a: 176-192. Mail: M.Roscini@westminster.ac.uk.

civilians or civilian objects are absolutely prohibited by international humanitarian law' (*Prosecutor v Kupreškić*, 2000, para 521).

While both Article 48 and Article 51(1) of Additional Protocol I refer to the notion of 'military operations', which includes 'all movements and acts related to hostilities that are undertaken by armed forces' (Sandoz, Swinarski and Zimmermann 1987: para 1875),[1] the Protocol's Commentary makes clear that the application of the principle of distinction is limited 'to military operations during which violence is used', i.e. 'attacks' (Sandoz, Swinarski and Zimmermann 1987: para 1875). This is confirmed by the language of Articles 51(2) and 52(1) of Additional Protocol I, according to which civilians, the civilian population and civilian objects 'shall not be the object of *attack*' (emphasis added). With regard to other military operations, only a more general obligation of 'constant care ... to spare the civilian population, civilians and civilian objects' applies (Additional Protocol I, 1977, Article 57(1)). Rules 1 and 7 of the International Committee of the Red Cross (ICRC)'s Study on Customary International Humanitarian Law, which incorporate the principle of distinction, also refer to 'attacks', and not to 'military operations' (Henckaerts and Doswald-Beck 2005 (vol. I): 3 and 25).

Whenever cyber operations conducted during an armed conflict and having a nexus with it amount to 'attacks', then, they are subject to the principle of distinction and may only be directed against military objectives. Before discussing what a military objective is in the cyber context, however, we need to examine when cyber operations qualify as 'attacks' under the law of armed conflict.

2. Cyber Operations Qualifying as 'Attacks' under the Law of Armed Conflict

'Attacks' are defined in Article 49(1) of Additional Protocol I as 'acts of violence against the adversary, whether in offence or in defence'. In other words, attacks under the law of armed conflict are only those acts of hostilities characterized by 'violence': unlike other acts of hostilities, like military espionage, non-violent military harm is not sufficient. It is not the author, the target or the intention that define an 'act of violence'. Rather, a cyber operation amounts to an 'attack' in the sense of Article 49(1) of Additional Protocol I when it employs cyber means or methods of warfare that result or are reasonably likely

[1] *The Commentary* subsequently rephrases the definition as 'any movements, manœvres and other activities whatsoever carried out by the armed forces with a view to combat' (Sandoz, Swinarski and Zimmermann, 1987: para 2191). Inconsistently, the Commentary of Art 13 of Additional Protocol II defines 'military operations' more narrowly as 'movements of attack or defence by the armed forces in action' (ibid., para 4769).

to result in violent effects (Roscini 2014a: 179). If a cyber operation causes or is likely to cause loss of life or injury to persons or more than minimal material damage to property, then, it is an 'attack' and the law of targeting fully applies, including the principle of distinction.[2] Had it been conducted in the context of an armed conflict between Iran and those states allegedly responsible for the cyber operation, for instance, Stuxnet would have been an example of such an 'attack' because of the damage it caused to the centrifuges of Iran's Natanz uranium enrichment facility. Similarly, the cyber attack that allegedly damaged a steel mill in Germany (Zetter, 2015) would have qualified as an 'attack' under Article 49(1) if it had had a belligerent nexus with an armed conflict. The relevant violent effects of a cyber attack include 'any reasonably foreseeable consequential damage, destruction, injury, or death', whether or not the computer system is damaged or data corrupted (*Tallinn Manual* 2013: 107). If the attack is intercepted and the reasonably expected violent effects do not occur, or occur to a lesser degree, the operation would still qualify as an 'attack' for the purposes of Article 49(1) (*Tallinn Manual* 2013: 109-110).

There is disagreement, however, on whether cyber operations that merely disrupt the functionality of infrastructures without causing material damage also amount to 'attacks' in the sense of Article 49(1) of Additional Protocol I. Rule 30 of the *Tallinn Manual on the International Law Applicable to Cyber Warfare* appears to rule this out. The majority of the experts that drafted the Manual maintained that disruptive cyber operations may be 'attacks' only 'if restoration of functionality requires replacement of physical components' (*Tallinn Manual* 2013: 108). The problem with this view, which still relies on the occurrence of some physical damage, is that the attacker may not be able to know in advance whether the restoration of functionality will require replacement of physical components or mere reinstallation of the operating system: the attacker could claim, therefore, that it was not aware that it was conducting an 'attack' and thus avoid the application of the law of targeting.

The limits of the doctrine of kinetic equivalence, which requires the occurrence of physical consequences for a cyber operation to be an 'attack', become evident if one considers that, under the Tallinn Manual's approach, a cyber attack that shuts down the national grid or erases the data of the entire banking system of a state would not be an 'attack', while the physical destruction of one server would. Some commentators have therefore tried to extend the notion of 'attack' to include at least some disruptive cyber

[2] Rule 30 of the *Tallinn Manual* for instance, defines a cyber attack as 'a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects' (*Tallinn Manual,* 2013: 106). *The Manual* includes 'serious illness and severe mental suffering' in the notion of 'injury' (*Tallinn Manual,* 2013: 108).

operations. Dörmann, for instance, recalls that the definition of 'military objective' in Article 52(2) of Additional Protocol I mentions not only destruction but also 'neutralization' of the object and concludes that, when the object (person or property) is civilian, '[i]t is irrelevant whether [it] is disabled through destruction or in any other way.' (Dörmann 2004). Therefore, the incapacitation of an object, like a civilian power station, without destroying it would still qualify as an 'attack'. Melzer adopts a different approach to reach the same conclusion and argues that the principles of distinction, proportionality and precautions apply not to 'attacks', but rather to the broader notion of 'hostilities': therefore, 'the applicability of the restraints imposed by IHL [international humanitarian law] on the conduct of hostilities to cyber operations depends not on whether the operations in question qualify as "attacks" (that is, the predominant form of conducting hostilities), but on whether they constitute part of the "hostilities" within the meaning of IHL' (Melzer 2011: 11). According to this view, cyber operations disrupting the enemy radar system would not amount to 'attack' because of the lack of violent consequences, but, as an act of hostilities, they would still be subject to the restrictions on the choice and use of methods and means of warfare (Melzer 2011). This position, however, is inconsistent with the above mentioned prevailing view according to which the rules contained in Part IV, Section I of Additional Protocol I essentially apply to 'attacks' and not to 'hostilities' or 'military operations'.

It is submitted that a better way of including at least certain disruptive cyber operations in the definition of 'attack' under Article 49(1) of Additional Protocol I is to interpret the provision in an evolutionary way taking into account the recent technological developments and to expand the concept of 'violence' to include not only material damage to objects, but also severe incapacitation of physical infrastructures without destruction.[3] This is suggested by Panama in its views on cyber security submitted to the UN Secretary-General, where it qualifies cyber operations as a 'new form of violence' (UN Doc A/57/166/add.1, 2002: 5). Indeed, the dependency of modern societies on computers, computer systems and networks has made it possible to cause significant harm through non-destructive means: cyber technologies can produce results comparable to those of kinetic weapons without the need for physical damage. After all, if the use of graphite bombs, which spread a cloud of extremely fine carbon filaments over electrical components, thus causing a short-circuit and a disruption of the electrical supply, would undoubtedly be considered an 'attack' even though it does not cause more than nominal physical damage to the infrastructure, one cannot see why the same conclusion should not apply to the use of viruses and other malware that achieve the same effect. It is,

[3] On evolutionary interpretation in the cyber context, see Roscini 2014a: 20-24, 280-281.

however, only those cyber operations that go beyond transient effects and mere inconvenience and cause significant functional harm to infrastructures that can qualify as 'attacks' in the sense of Article 49(1) of Additional Protocol I During the crisis between Ukraine and Russia over Crimea, a limited disruption of Ukrainian mobile communications through Distributed Denial of Service (DDoS) attacks and the defacement of certain state-run news websites and social media (the content of which was replaced with pro-Russian propaganda) were reported: because of their limited disruptive effects, such operations would not be 'attacks' under Article 49(1).[4] Only the less stringent obligation of 'constant care ... to spare the civilian population, civilians and civilian objects' (Additional Protocol I, 1977, Article 57(1)) would apply to such cyber operations short of attack, but not the prohibition to conduct them against civilians and civilian objects.

3. The Definition of 'Military Objective'

The principle of distinction requires that cyber operations conducted during an armed conflict by the belligerents against each other and amounting to 'attacks' be directed only against military objectives.[5] The first definition of 'military objective' to appear in a legal text can be found in the 1923 Hague Rules on Air Warfare: 'an object of which the destruction or injury would constitute a distinct military advantage to the belligerent' (Article 24(1)).[6] To clarify the definition, the Rules provided an illustrative list of military objectives (Article 24(2)).[7] The Rules, however, have never been adopted in treaty form. No definition appears in the 1949 Geneva Conventions, although the term is employed.[8]

[4] Roscini 2014b. Denial of service (DoS) attacks, of which 'flood attacks' are an example, aim to inundate the targeted system with excessive calls, messages, enquiries or requests in order to overload it and force its shut down. Permanent DoS attacks are particularly serious attacks that damage the system and cause its replacement or reinstallation of hardware. When the DoS attack is carried out by a large number of computers organized in botnets, it is referred to as a 'distributed denial of service' (DDoS) attack.

[5] For a discussion of the application of the principle of distinction to the targeting of individuals (as opposed to objects), see Roscini 2014a: 192-215.

[6] Without referring to the notion of military objective, Art 2 of the 1907 Hague Convention IX Concerning Bombardment by Naval Forces in Time of War contains a list of objects that can be destroyed.

[7] The list includes military forces; military works; military establishments or depots; factories constituting important and well-known centres engaged in the manufacture of arms, ammunition or distinctively military supplies; lines of communication or transportation used for military purposes. It is doubtful whether the list is exhaustive (Rogers 2004: 60).

[8] See Arts 4, 19(2) of Geneva Convention I and Arts 4, 18(5) of Geneva Convention IV. The 1956 New Delhi Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War, drafted by the ICRC, proposed a list of military objectives, to be reviewed at intervals of no more than ten years by a group of experts; however, even if an object had belonged to one of the listed categories, it would not have been a military objective if its total or partial destruction, in the circumstances ruling at the time, had offered no military advantage (Art 7). Another attempt to define the concept of 'military objective' was

On the other hand, 'military objectives' are expressly defined in Article 52(2) of the 1977 Additional Protocol I as

those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total and partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.

This definition has been incorporated into several military manuals and, in spite of the unclear position of certain states like the United States (which will be discussed below), it is largely thought to reflect customary international law (Henckaerts and Doswald-Beck 2005 (vol. I): 30). The definition is also applicable in non-international armed conflicts (Henckaerts and Doswald-Beck 2005 (vol. I): 29).

If one applies the above definition of 'military objective' to targeting in the cyber context, however, some interpretative problems arise. First of all, what 'objects' are relevant? Cyber operations can be directed at cyber targets, i.e. data, software, or networks, and/or hard targets, i.e. information hardware (e.g. computers, servers, routers, fibre-optic cables, and satellites), physical infrastructures, or persons.[9] When the cyber operation aims to cause material damage to physical property or persons or incapacitation of infrastructures, or such effects are foreseeable, the attacked 'object' is not only, and not mainly, the information itself, but rather the persons, property or infrastructure attacked *through* cyberspace (*Tallinn Manual* 2013: 108). In the case of Stuxnet, for instance, the relevant 'object' was not the Siemens software that operated the centrifuges at the Natanz uranium enrichment facility in Iran, but the centrifuges themselves. Similarly, in the previously mentioned cyber attack against a steel mill in Germany, the object of the attack was the mill, not its operating system. Commentators have debated whether data are per se an 'object' for the purpose of Article 52(2) of Additional Protocol I (Schmitt 2011 and Lubell 2013). The Experts that drafted the Tallinn Manual did not manage to achieve consensus on this point so no solution was incorporated in the black-letter rules (*Tallinn Manual* 2013: 127). The problem should not be overestimated. As already said, if the cyber operation deletes, corrupts or alters data in order to cause damage to or disrupt the functioning of an infrastructure, it is such infrastructure that is the intended 'object' of the attack. Similarly, if the cyber operation deletes or alters medical records, so that patients receive the wrong treatment, it is those individuals that are (also)

made by the Institute of International Law in 1969 (Annuaire de l'Institut de droit international (1969–II).359).

[9] Hard targets can be attacked both by kinetic or cyber means, while software and data can be attacked only by cyber means (Rauscher and Korotkov 2011: 19).

targeted. If, on the other hand, the cyber operation only results in the corruption, deletion, or alteration of data without destructive or disruptive consequences on physical infrastructures, it will not be an 'attack' in the sense discussed above, and the law of targeting and the notion of 'military objective' will therefore not apply, whether or not the data are an 'object'. Cyber attacks not qualifying as 'attacks' under the law of armed conflict will only be subject to the general duty of 'constant care' when conducting military operations provided in Article 57(1) of Additional Protocol I and to the rules providing for special protection if applicable, such as those on cultural property for certain digital art and on the protection of diplomatic archives and correspondence.

3.1 'Effective Contribution to Military Action'

According to Article 52(2) of Additional Protocol I, two cumulative elements must be present for an 'object' to be a military objective and therefore targetable: it must effectively contribute to military action *and* its total or partial destruction, capture or neutralization, in the circumstances ruling at the time, must offer a definite military advantage. Article 52(2) indicates the criteria to evaluate whether the object effectively contributes to military action, i.e. nature, location, purpose, or use.[10] Effective contribution to military action by nature characterizes those objects which are inherently military and cannot be employed but for military purposes, for instance computers designed specifically to be used as components of weapon systems or to facilitate logistic operations (Dinstein 2013).[11] Other examples include military command, communication, and control networks used for the transmission of orders or tactical data and military air defence networks.[12] The premises from where the military cyber operations are conducted (such as USCYBERCOM headquarters at Fort Mead or the 12-storey building in the Pudong New Area of Shanghai which is allegedly the home of the People's Liberation Army's Unit 61398) (Mandiant 2013) are also military objectives by nature (Turns 2012). An example of effective contribution by use would be a server

[10] Confusingly, the Commentary to Rule 38 of the *Tallinn Manual* makes the example of a cyber operation against a website that inspires 'patriotic sentiments' among the population as a case of non-effective contribution to military action (*Tallinn Manual* 2013:13); however, such an operation would not be an 'attack' in the sense of either Art 49(1) of Additional Protocol I or Rule 30 of the *Manual* itself.

[11] It is however normally the software rather than the hardware that turns a computer into a military objective (Dinstein 2012: 263).

[12] The three US Department of Defense's internal networks, for instance, would be examples of networks that are military objectives by nature. In particular, the Secret Internet Protocol Router Network (SIPRNet), which is not connected to the internet, is used for classified information and to transmit military orders, while the Joint Worldwide Intelligence Communications System (JWICS) is used to communicate intelligence information to the military. On the three DoD networks, see Clarke and Knake 2010: 171-3.

normally used for civilian purposes which is taken over by the military, even if it is used for non-combat purposes (Dinstein 2013). If the server is about to be used by the military but this has not occurred yet, it may be a military objective by purpose.[13] As to military objectives by location, the Commentary to Rule 38 of the Tallinn Manual makes the example of a cyber attack on a water reservoir's Supervisory Control and Data Acquisition (SCADA) system to cause the release of water and thus prevent the use of a certain area by the enemy (*Tallinn Manual* 2013: 128).

The use of an object by the military is then sufficient to make it a military objective (providing that its destruction or neutralization also offer a definite military advantage in the circumstances ruling at the time). Most cyber infrastructures, however, are dual-use, i.e. at the same time used by civilians and the military. It is well known, for instance, that about 98 per cent of US government communications travel through civilian-owned or civilian-operated networks (Geiß and Lahmann 2012). Servers, fibre-optic cables, satellites, and other physical components of cyberspace are also almost entirely dual-use, as well as most technology and software used in this field: everyday applications such as web browser, e-mail client and even command line (cmd.exe) can be used as an instrument for cyber attacks. The advent of cloud computing, where military and civilian data are stored side by side, is nothing but the latest manifestation of the dual-use character of information technology.[14] The fact that an object is *also* used for civilian purposes does not affect its qualification under the principle of distinction: if the two requirements provided in Article 52(2) of Additional Protocol I are present, the object is a military objective but the neutralization of its civilian component needs to be taken into account when assessing the incidental damage on civilians and civilian property under the principle of proportionality.[15] What is prohibited is to attack the dual-use cyber infrastructure *because* of its civilian function or to attack a dual use facility where the anticipated concrete and direct military advantage of the attack is outweighed by the expected civilian damage and/or injury. It should be recalled that, under Article 52(3) of Additional Protocol I, '[i]n case of doubt whether an object which is normally dedicated to civilian purposes . . . is being used to make an effective contribution to military action,

[13] According to the ICRC *Commentary*, purpose is 'the intended future use of an object, while that of *use* is concerned with its present function' (Sandoz, Swinarski and Zimmermann 1987: para 2022, emphasis in the original).

[14] Jensen has for instance claimed that 'Microsoft Corporation Headquarters in Washington State is a valid dual-use target, based on the support it provides to the U.S. war effort by facilitating U.S. military operations' (Jensen 2002-2003: 1160). However, he eventually denies that it is a lawful military objective because of doubts with regard to the military advantage that can be gained from its destruction or neutralization (1167-6).

[15] See Rule 39, *Tallinn Manual*. As has been observed, an 'object becomes a military objective even if its military use is only marginal compared to its civilian use' (Droege 2012: 563).

it shall be presumed not to be so used'.[16] Unlike its counterpart with regard to persons (Article 50(1) of Additional Protocol I), the customary status of this provision is, however, dubious: it is, for instance, not included in the ICRC Study on Customary International Humanitarian Law. It has also been observed that satellites, cables, routers, and servers are not 'normally dedicated to civilian purposes', as they are also widely used by the military (Geiß and Lahmann 2012: 386).

The effective contribution must be to 'military action'. 'Military action' has a broad meaning that corresponds to the 'general prosecution of the war' (Rogers 2004: 67). The United States' definition of 'military objective' employs language different from that contained in Additional Protocol I and it includes all objects which 'effectively contribute to the enemy's war-fighting or war sustaining capability' (US Navy, U.S Marine Corps, U.S Coast Guard 2007: para 8.2). If 'war fighting' can be considered equivalent to 'military action', 'war sustaining' is much broader and includes activities not directly connected to the hostilities: it would therefore allow attacks aimed to incapacitate political and economic targets in order to 'persuade' the enemy to stop fighting.[17]

The US definition of 'military objective' is also reflected in the cyber context. According to the US Air Force's Cornerstones of Information Warfare, the United States 'may target any of the adversary's information functions that have a bearing on his will or capability to fight' (Department of Air Force 1997: footnote 5).[18] This view would, for instance, legitimize attacks like the 2012 cyber operations against Saudi Aramco, the world's largest oil producer, which destroyed the data of about 30,000 company computers and, according to Saudi Arabia, targeted the country's economy with the purpose of preventing the pumping of oil into domestic and international markets.[19] The US CYBERCOM former Head also declared that power grids, banks, and other financial institutions and networks, transportation-related networks, and national telecommunication networks are 'all potential targets of military attack, both kinetic and cyber, under the right circumstances', although only when 'used solely to support enemy military operations'.[20]

[16] The provision only applies when doubt concerns the use of the object, not its nature, location or purpose (Boothby 2012: 71).
[17] For critical comments of the US position and the documents in which it appears, see Bartolini 2006: 235-6.
[18] It also appears that China sees cyber operations against financial systems, power generation, transmission facilities, and other NCIs as part of a conflict with another state (Owens et al. 2009: 333)
[19] Al Arabiya News: 2012. Oil production, however, remained uninterrupted.
[20] Responses to advance questions, Nomination of Lt Gen Keith Alexander for Commander, US Cyber Command, US Senate Committee on Armed Services, 15 April 2010, 13, http://armed-services.senate.gov/statemnt/2010/04%20April/Alexander%2004-15-10.pdf.

This expanded notion of military objective is at odds with the definition contained in Article 52(2) of Additional Protocol I, which is largely considered to reflect customary international law. It should be noted that the 1976 US Air Force Pamphlet incorporated a definition of military objective analogous to that contained in the Protocol (U.S. Air Force 1976: para 5-3(b)(1)). The subsequent 1998 USAF Intelligence Targeting Guide also incorporates the Protocol's definition to the letter (U.S. Air Force 1998: para 1.7.1) and the 1997 edition of the Report on US practice in international law notes that '[t]he *opinio juris* of the U.S. government recognizes the definition of military objectives in Article 52 of Additional Protocol I as customary law', although it adds that 'United States practice gives a broad reading to this definition, and would include areas of land, objects screening other military objectives, and war-supporting economic facilities as military objectives' (Henckaerts and Doswald-Beck 2005 (vol. II): 188).

3.2 'Definite Military Advantage'

Even objects that, because of their nature, use, purpose, or location, effectively contribute to military action are not, as such, military objectives unless their total or partial destruction, capture or neutralization, in the circumstances ruling at the time, are militarily necessary, i.e. offer a 'definite military advantage' (Boothby 2012: 103).[21] Article 52(2) envisages not only the total or partial destruction of the attacked object, but also its capture or neutralization, which includes 'an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it' (Bothe et al. 1982: 325). These words fit cyber operations that incapacitate but do not destroy infrastructures like a glove. As the ICRC has observed, 'the fact that a cyber operation does not lead to the destruction of an attacked object is . . . irrelevant': the definition of military objective, which refers to neutralization, 'implies that it is immaterial whether an object is disabled through destruction or in any other way' (ICRC 2011: 37).

The advantage must be of a military nature and 'definite', i.e. not speculative or indirect: the Commentary explains that 'it is not legitimate to launch an attack which only offers potential or indeterminate advantages' (Sandoz, Swinarski and Zimmermann 1987: para 2024). Shutting down the computer system operating the adversary's air defences would, for instance, provide an evident 'definite' military advantage. By contrast, a cyber

[21] DeSaussure refers to the examples of the 1972 Christmas bombing of Hanoi or the never implemented bombing of a depot in the heart of Argentina during the Falklands war, which would have not helped the British reoccupy the islands (DeSaussure 1987: 513).

attack aimed at demoralizing the civilian population would be unlawful. The problem with establishing the definite military advantage requirement in the cyber context is that measurement of effects can often be difficult: it is still not confirmed, for instance, whether Stuxnet did destroy any centrifuges at Natanz and, if so, with what consequences on the Iranian nuclear programme. Indeed, while Iran denied that the incident caused significant damage, the IAEA reported that Iran stopped feeding uranium into thousands of centrifuges (Broad, 2010): it is however unclear whether this was due to Stuxnet or to technical malfunctions inherent to the equipment used (Ziolkowski 2012). The fact that a definite military advantage is eventually not gained from the operation, however, does not necessarily deprive the object of its qualification as a military objective, as long as the attacker had a reasonable expectation that the intended results would occur.

The destruction, capture or neutralization of the object must offer a definite military advantage 'in the circumstances ruling at the time'. This excludes any potential future advantage but also implies that an object which could not normally be considered a military objective may become one if it is used in direct support of the hostilities. The time between the identification of the target, the planning of the attack and the execution of the attack must therefore be reasonably short, as the circumstances could rapidly change and an object that qualified as a military objective at a certain time may subsequently turn into a civilian one (Vierucci 2006).

4. Is the internet a military objective?

The internet can be disrupted by attacking its hardware or software components. The former type of attack targets servers, fibre-optic cables and other physical internet infrastructure used to ensure connectivity, while the latter affects systems like the Domain Name System (DNS), which translates domain names into IP addresses: if the DNS is compromised, the web browser would not know where to direct the visit. The China Internet Network Information Centre (CNNIC), for instance, reported that the national domain name resolution registry came under a series of a sustained DDoS attack on 25 August 2013, which interrupted or slowed down visits (Vincent 2013). A cyber operation against either the hardware or software components of the internet would qualify as an 'attack' in the sense of Article 49(1) of Additional Protocol I if material damage or significant loss of functionality of infrastructure ensue.

The internet is a computer network, which is a type of communication network: the question whether or not the internet is a military objective, then, can first be approached

reasoning by analogy with more traditional means of communication (Doswald-Beck 2002; Dörmann 2001). The 1956 ICRC list of military objectives includes 'the lines and means of communication, installations of broadcasting and television stations, telephone and telegraph exchanges of fundamental military importance'.[22] Military manuals also include 'communication installations used for military purposes' as an example of military objective (UK Ministry of Defence 2004: 57). Targeting communication nodes has been a high priority in all recent armed conflicts. Media and broadcasting systems were included in the target list both in Operation Desert Storm and in Operation Allied Force (Fenrick 1996-97). In the former case, the attacks were justified by the United States not only on the ground that the facilities were part of the military communications network, but also because they were used for Iraqi propaganda (Bartolini 2006). On 23 April 1999, NATO aircraft bombed the headquarters of the Radio Television of Serbia (RTS) in Belgrade (Aldrich 1999). According to the Organization, it was a lawful target, since the station was used for military purposes as part of the control mechanism and of the propaganda machinery of the Milošević government (Amnesty International 2000). The ICTY Final Report concluded that the attack was lawful because it was aimed mainly at disabling the Serbian military command and control system and at destroying the apparatus that kept Milošević in power (ICTY *Final Report* 2000). On 12 November 2001, the Kabul office of Al-Jazeera news television was hit by a guided bomb during Operation Enduring Freedom (Herold 2002) and other radio/television stations were attacked because they were used as means of propaganda by the Taliban (Cryer 2002). In Operation Iraqi Freedom, the United States bombed the Ministry of Information, the Baghdad Television Studio and Broadcast Facility and the Abu Ghraib Television Antennae Broadcast Facility (Human Rights Watch, 2003). Unlike in the 1991 operation, however, it seems that in 2003 the emphasis in the legal justification of the attacks was more on the facilities being part of the military communications network than on their use to spread propaganda (Bartolini 2006). The antennas of Libya's state broadcaster were also attacked by NATO aircraft during the 2011 Operation Unified Protector (Bartolini 2013). The attack had the purpose 'of degrading Qadhafi's use of satellite television as a means to intimidate the Libyan people and incite acts of violence against them' and was motivated on the fact that 'TV was being used as an integral component of the regime apparatus designed to systematically oppress and threaten civilians and to incite attacks against them' (NATO Operation *Unified Protector,* Statement by Colonel Lavoie, 2011).

Although, as a means of communication, the internet could potentially qualify as a military objective, it would still have to meet the two requirements of Article 52(2) of

[22] The list is reprinted in ICTY *Final Report*, 2000, para 39.

Additional Protocol I. If internet disruption had the sole purpose of stopping propaganda, undermining civilian morale or psychologically harass the population, its neutralization would not offer a 'definite' military advantage (even if it weakened the political support for the enemy government) (ICTY *Final Report* 2000: para 55). On the other hand, if the internet had become part of the adversary's military communication system, it would effectively contribute to military action, but, if connection can be easily and promptly restored, it can be doubted that its neutralization or destruction would provide a definite military advantage. As has been observed, 'an attacker nowadays must probably destroy a network of telecommunication *in toto* (or at least its central connection points) in order to paralyse the command and control structures of the enemy armed forces, which in themselves clearly constitute a legitimate military objective' (Oeter 2013: 174).[23] This may be particularly difficult to achieve in the case of the internet, which is notoriously characterized by a high level of resilience: if certain channels become unusable as a consequence of a cyber or kinetic attack on servers, the data flow will simply find another path to reach its destination and it might well be that the destruction or neutralization of certain internet infrastructure has no practical effect at all (Geiß and Lahmann 2012). Connection would probably slow down, but it would still continue through mirror servers, mobile phones, or satellites.[24]

The ICTY Final Report on the NATO bombing campaign against Yugoslavia suggests that a broadcasting station may also constitute a military objective when it is employed to incite the population to commit war crimes or crimes against humanity as in the case of Radio Mille Collines in Rwanda in 1994 (ICTY *Final Report,* 2000). As has been seen, this argument was also used by NATO to justify the attack on Libya's state television in 2011, but the justification was offered more for the purposes of the Operation's protective mandate than from an international humanitarian law perspective (Bartolini, 2013). Although it is doubtful that these views are consistent with the *lex lata*, as propaganda or incitement to commit crimes do not amount to 'effective contribution to military action', it cannot be excluded that, in parallel with the developments in international criminal law, a customary international law rule is emerging that allows attacks against these heinous uses of means of communication. If this is the case, and

[23] The ICTY *Final Report* on the NATO bombing campaign against Yugoslavia emphasized that, even if the RTS building in Belgrade was considered a military objective, broadcasting was interrupted only for a brief period and in any case Yugoslavia's command and control network, of which the RTS building was allegedly a part, could not be disabled with a single strike (ICTY *Final Report*, 2000, para 78).

[24] Resilience does not, however, mean invulnerability. For instance, 88 per cent of Egyptian internet access was shut down as a consequence of the withdrawal of 3,500 Border Gateway Protocol (BGP) routes by Egyptian ISPs (Williams, 2011).

should the internet be used for such purposes, connectivity could be disrupted through a kinetic or cyber operation against its components.

The internet, however, is not only a means of communication, but also an important economic resource. As the German *Law of Armed Conflict Manual* recalls, only economic objectives that make an effective contribution to military action can be considered lawful targets (Federal Ministry of Defence, *Law of Armed Conflict Manual*, 2013: para. 407) and the same view is contained in the 1998 USAF Intelligence Targeting Guide (*Intelligence Targeting Guide*, para A4.2.2.1). According to the 2002 US Joint Doctrine for Targeting, however, lawful targets also include economic facilities that '*indirectly but effectively* support and sustain the enemy's warfighting capability' (*US Joint Doctrine for Targeting:* A-3; emphasis added). The Eritrea-Ethiopia Claims Commission (EECC) also affirmed that '[t]he infliction of economic losses from attacks against military objectives is a lawful means of achieving a definite military advantage' and that 'there can be few military advantages more evident than effective pressure to end an armed conflict' (EECC, Partial Award, 2005 para 121). While it is accepted that certain economic targets may be military objectives when they meet the two requirements provided in Article 52(2) of Additional Protocol I, the EECC seems to justify attacks against *any* economic target (Vierucci, 2006). This view goes too far and is not consistent with the definition of 'military objective' contained in Additional Protocol I, which reflects customary international law.

It is worth noting that, even if the internet qualified in certain situations as a military objective, the attacker would still have to take into account the disruption caused to its civilian function and to neutrals under the principle of proportionality (Article 51(5)(b) of Additional Protocol I). The possibility of shutting down specific segments, websites, or networks, therefore, should always be explored first (*Tallinn Manual*, 2013: 136).

5. Conclusions

As the United States has observed, the application in the cyber context of the law of armed conflict, which was conceived with kinetic weaponry in mind, presents 'new and unique challenges that will require consultation and cooperation among nations' (UN Doc A/66/152, 2011: 19). This essay has discussed some of these challenges, in particular those related to the application of the principle of distinction and of the definition of 'military objective' to cyber operations conducted during an armed conflict and having a nexus with it. This essay has concluded that none of these challenges significantly affects

the application of the principle of distinction. Indeed, the definition of 'military objective' contained in Article 52(2) of Additional Protocol I is flexible enough to apply in the cyber context, in spite of the peculiar characteristics of this new domain of warfare. The dual-use character of most cyber infrastructures, i.e. the fact that they are at the same time used both by civilians and the military, is also an overestimated problem which is not unique to cyberspace and which does not render the existing rules obsolete.

Bibliography

Books and Articles

Aldrich, George, H. 1999. Yugoslavia's Television Studios as Military Objectives. *International Law Forum du droit international* 1: 149-50.

Bartolini, Giulio. 2013. Air Targeting in Operation *Unified Protector* in Libya. *Jus ad bellum* and IHL Issues: an External Perspective. In *Legal Interoperability and Ensuring Observance of the Law Applicable in Multinational Deployments*, eds. Stanislas Horvat and Marco Benatar, 242-279. Brussels: International Society for Military Law and the Law of War.

Bartolini, Giulio. 2006. Air Operations Against Iraq (1991 and 2003). In *The Law ofAir Warfare-Contemporary Issues,* eds. Natalino Ronzitti and Gabriella Venturini, 227-272. Utrecht: Eleven Publishing.

Bothe, Michael, Partsch, Karl, J. and Solf, Waldemar, A. 1982. *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949.* The Hague: Nijhoff.

Boothby, William, H. 2012. *The Law of Targeting.* Oxford: Oxford University Press.

Clarke, Richard, A. and Knake, Robert, K. 2010. *Cyber War. The Next Threat to National Security and What to Do About it?* Harper Collins: New York.

Cryer, Robert. 2002. The Fine Art of Friendship: *Jus in Bello* in Afghanistan. *Journal of Conflict and Security Law* 7(1): 37-83.

DeSaussure, Hamilton. 1987. Remarks at the Six Annual American Red Cross-Washington College of Law Conference on International Humanitarian Law: A Workshop on Customary International Law and the 1977 Protocols Additional to the 1949 Geneva Conventions. *American University Journal of International Law and Policy* 2: 415-538.

Dinstein, Yoram. 2013. Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Conference. *International Law Studies* 89: 276-287.

Dinstein, Yoram. 2012. The Principle of Distinction in Cyber War in International Armed Conflicts. *Journal of Conflict and Security Law* 17: 261-278.

Doswald-Beck, Louise. 2002. Some Thoughts on Computer Network Attack and the International Law of Armed Conflict. *International Law Studies* 76: 163-186.

Droege, Cordula. 2012. Get off My Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians. *International Review of the Red Cross* 94: 533-578.

Fenrick, William, J. 1996-97. Attacking the Enemy Civilian as a Punishable Offence. *Duke Journal of Comparative and International Law* 7: 539-570.

Fleck, Dieter. 2013. The Law of Non-international Armed Conflicts. In *The Handbook of International Humanitarian Law,* ed. Dieter Fleck, 581-609. Oxford: Oxford University Press.

Geiß, Robin, and Lahmannn, Henning. 2012. Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space. *Israel Law Review* 45: 381-400.

Henckaerts, Jean Marie and Doswald-Beck, Louise (eds.). 2005. *Customary International Humanitarian Law*. Cambridge: Cambridge University Press (two volumes).

Jensen, Eric, Talbot. 2002-2003. Unexpected Consequences from Knock-on Effects: a Different Standard for Computer Network Operations? *American University International Law Review* 18: 1145-1188.

Lubell, Noam. 2013. Lawful Targets in Cyber Operations: Does the Principle of Distinction Apply? *International Law Studies* 89: 252-275.

Oeter, Stefan. 2013. Methods and Means of Combat. In *The Handbook of International Humanitarian Law,* ed. Dieter Fleck, 115-230. Oxford: Oxford University Press.

Owens, William, A., Dam, Kenneth, W. and Lin, Herbert, S. 2009. *Technology, Policy,*

Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. Washington: The National Academies Press.

Rauscher, Karl, F., and Korotkov, Andrey. 2011. Working Towards Rules for Governing Cyber Conflict. Rendering the Geneva and Hague Conventions in Cyberspace. *East West Institute*.

Rogers, A.P.V. 2004. *Law on the Battlefield.* Manchester: Manchester University Press.

Roscini, Marco. 2014a. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press.

Sandoz, Yves, Swinarski, Christophe, and Zimmermann Bruno, eds. 1987. *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949.* Dordrecht: Nijhoff.

Schmitt, Michael, N., ed. 2013. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Schmitt, Michael, N., 2011. Cyber Operations and the *Jus in Bello*: Key Issues. *International Law Studies* 87: 89-112.

Turns, Davis. 2012. Cyber Warfare and the Notion of Direct Participation in Hostilities. *Journal of Conflict and Security Law* 17: 297-300.

Vierucci, Luisa. 2006. Sulla nozione di obiettivo militare nella guerra aerea: recenti sviluppi della giurisprudenza internazionale. *Rivista di diritto internazionale* 89: 693-735.

National Military Manuals and Operational Handbooks

Department of Air Force. 1997. *Cornerstones of Information Warfare*. http://www.google.co.uk/url?url=http://www.dtic.mil/cgi-bin/GetTRDoc?Ad.

Federal Ministry of Defence. 2013. *Law of Armed Conflict Manual*, Joint Service Regulation 15/2, http://www.bmvg.de/resource/resource/MzEzNTM4MmUzMzMyMmUzMTM1MzMyZTM2MzIzMDMwMzAzMDMwMzAzMDY5MzIzNDZmN2E3NjZmNjgyMDIwMjAyMDIw/Law%20of%20Armed%20Conflict_Manual_2013.pdf

UK Ministry of Defence. 2004. *The Manual of the Law of Armed Conflict.* Oxford: Oxford University Press.

US Air Force. 1 February 1998. *Intelligence Targeting Guide.* Air Force Pamphlet 14-210 Intelligence. http://www.fas.org/irp/dodir/usaf/afpam14-210/part17.htm.

U.S Air Force Pamphlet 110-31. 1976. *International Law –The Conduct of Armed Conflict and Air Operations* https://www.cna.org/sites/default/files/research/5500045700.pdf.

US Navy, U.S Marine Corps, U.S Coast Guard. 2007. *The Commander's Handbook on the Law of Naval Operations* http://www.fichl.org/uploads/media/US_Navy_Commander_s_Handbook_1995.pdf.

Reports

Amnesty International. June 2000. 'Collateral Damage' or 'Unlawful Killings?' Violations of the Laws of War by NATO During Operation *Allied Force.* AI-Index EUR70/18/00 https://www.amnesty.org/en/documents/document/?indexNumber=EUR70%2F018%2F2000&language=en.

Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia. 8 June 2000- http://www.icty.org/x/file/Press/nato061300.pdf.

Human Rights Watch. 2003. *Off Target. The Conduct of the War and Civilian Casualties in Iraq.* http://www.hrw.org/reports/2003/usa1203/usa1203.pdf.

ICRC. October 2011. International Humanitarian Law and the Challenges of Contemporary Armed Conflicts. 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.

Mandiant. 2013. APT1. *Exposing One of China's Cyber Espionage Units.* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

Melzer, Nils. 2011. Cyberwarfare and International Law. UNIDIR. http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lang=en&id=134218, 27.

Ziolkowski, Katharina. 2012. Stuxnet - Legal Considerations. *NATO CCD COE Publications,* 5. https://ccdcoe.org/search.html

Cases

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 8 July 1996, ICJ Reports 1996.

Prosecutor v Kupreškić, Case No IT-96-16-T, Trial Chamber Judgment, 14 January 2000.

Partial Award, *Western Front, Aerial Bombardment and Related Claims, Eritrea's Claims 1, 3, 5, 9-13, 14, 21, 25 and 26*, 19 December 2005, Reports of International Arbitral Awards. Vol. XXVI, Part VIII.

On-Line Publications and Other Documents

Al Arabiya News, 9 December 2012. Saudi Aramco Says Cyber Attack Targeted Kingdom's Economy. http://www.alarabiya.net/articles/2012/12/09/254162.html.

Broad, William, J. 23 November 2010. Report Suggests Problems with Iran's Nuclear Efforts. *The New York Times*. http://www.nytimes.com/2012/11/24/world/middleeast/24nuke.html.

Dörmann, Knut. 9 November 2004. Applicability of the Additional Protocols to Computer Network Attacks. https://www.icrc.org/eng/assets/files/other/applicabilityofihltocna.pdf.

Dörmann, Knut. 19 May 2001. Computer Network Attack and International Humanitarian Law. http://www.icrc.org/eng/resources/documents/misc/5p2alj.htm.

Herold, Marc, W. March 2002. A Dossier on Civilian Victims of United States' Aerial Bombing of Afghanistan: A Comprehensive Accounting. http://www.cursor.org/stories/civilian_deaths.htm.

Roscini, Marco. 31 March 2014b. Is there a 'Cyber War' Between Ukraine and Russia. OUPBlog. http://blog.oup.com/2014/03/is-there-a-cyber-war-between-ukraine-and-russia-pil/.

Statement by the Spokesperson for NATO Operation Unified Protector, Colonel Roland Lavoie, Regarding Air Strike in Tripoli. 30 July 2011. NATO Strikes Libyan State TV Satellite Facility. http://www.nato.int/cps/en/natolive/news_76776.htm.

Vincent, James. 27 August 2013. Chinese Domains Downed by 'Largest Ever' Cyber Attack. *The Independent.* http://www.independent.co.uk/life-style/gadgets-and-tech/news/chinese-domains-downed-by-largest-ever-cyberattack-8786091.html.

Williams, Christopher. 28 January 2011. How Egypt Shut Down the Internet. *The Telegraph.* http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html

Zetter, Kim. 1 August 2015. A Cyber Attack Has Caused Confirmed Physical Damage for the Second Time Ever. *Wired*. https://www.wired.com/2015/01/german-steel-mill-hack-destruction/