UiO : Det juridiske fakultet

Cyber-attacks in the context of international humanitarian law

Candidate number: 642

Deadline for submission: 25.11.13

Number of words: 17 237

Table of contents

1 Introduction

There can be no doubt, computers and especially the Internet have revolutionized the way we live our lives. Information is stored in vast databases, and through the Internet, is literally at our fingertips. Many essential services and infrastructures are dependent on computers, and they also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars and stock markets.[1]

The revolution of computers and Internet has also brought with it a potential for misuse, and cyber criminals can be a serious threat. They can do anything from breaking into protected networks, stealing anything from confidential files to money, or vandalise the networks by deleting or altering information, to hijacking it and controlling the computers actions.

Recognising the potential for abuse, numerous states have issued statements on the need of regulating conduct on the Internet. The United Nations General Assembly has issued numerous statements on the possibilities of cyber abuse. For instance, in its fifty-third session the General Assembly recalled that technological developments could have both civilian and military application. They also stated that the use of information technologies could affect the interests of the entire international community, and disrupt international stability and security.[2] In its fifty-fifth session it called on states to criminalize cyber abuse and deny their territory from being used as a safe haven.[3]

---

[1] The White House, The National Strategy to Secure Cyberspace, 2003 page viii.

[2] G.A. Res. 53/70 (Dec. 4, 1998).

[3] G.A. Res. 55/63 (Dec. 4, 2000).

There is also an international convention on Cybercrime[4] which pursues a common criminal policy to protect society against cybercrime, by adopting appropriate legislation and fostering international co-operation.

But as the U.N. General Assembly noted, the technological developments can have both civilian and military applications. In recent years numerous countries have established their own cyber branches/units within the military. To name a few examples, the USA has the US Cyber Command,[5] China's People's Liberation Army has a cyber division called Blue Team,[6] Norway has Cyberforsvaret,[7] and the United Kingdom's Ministry of Defence has started recruiting personnel for a new cyber unit.[8]

The USA has declared that it reserves the right to use all necessary means, including military to defend against hostile acts in cyberspace.[9] Cyber-attacks have the potential to cause a lot of damage. There have already been large scale cyber operations that have had a significant effect on countries, but so far the effects have not been devastating.[10]

1.1.1 Scope of thesis

Considering the potential military use of cyberspace, and the establishment by the military of cyber units, it is worth examining the rules applicable to the use of cyberspace for military purposes more closely. This paper will therefore focus on the *jus in bello* aspects

---

[4] Convention on Cybercrime, 2001.

[5] US Department of Defense - U.S. Cyber Command Fact Sheet (2010).

[6] http://www.forbes.com/sites/williampentland/2011/06/12/china-creates-cyber-warfare-squad/ (Last accessed 06.11.13).

[7] http://forsvaret.no/OM-FORSVARET/ORGANISASJON/CYBERFORSVARET/Sider/cyberforsvaret.aspx (Last accessed 06.11.13).

[8] https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (Last accessed 06.11.13).

[9] Department of Defense Cyberspace Policy Report, 2011.

[10] The cases of Estonia, Georgia and Iran(Stuxnet) will be discussed later on.

of cyber-attacks. First of all, it is necessary to explore what uses of cyberspace, can amount to 'resort to armed force', in triggering an armed conflict and the use of IHL. Whether it can amount to a use of force, or constitute an armed attack under the *jus ad bellum*, which justifies the use of force by States in self-defence, falls outside the scope of this thesis.

This paper will have its main focus on cyber-attacks in international armed conflicts, but aspects of non-international armed conflicts will also be referred to. Cyber weapons were absent when the main IHL was adopted, but this paper will show that the general rules laid down in these widely ratified instruments can still govern cyber-attacks. The research question, broadly construed, is how cyber-attacks fit within IHL's existing framework. I will therefore examine under which circumstances a cyber-operation would constitute as an 'attack' under IHL, and how the rules apply.

In order to analyse the place and use of cyber-attacks within IHL, it is necessary to discuss them in relation to the concept of armed conflict. A cyber-attack does have the potential to trigger an armed conflict because it can have disastrous effects. Further sub questions that will be dealt with in this thesis are how the prohibition on attacking civilians applies in the cyber-context, and what taking necessary precautions mean. Real examples of cyber operations will be analysed in order to show whether or not they qualify as cyber-attacks, and whether they are governed by IHL. Lastly I will examine when acts of non-state actors can be attributed to States, and what the necessary level of State control for such attribution is.

2 Methodology

International law provides a normative framework for the conduct of international relations, and works on the basis that the general consent or acceptance of states can create rules of general application.[11] The United Nations Charter[12] (UN Charter) Article 92 establishes the International Court of Justice (ICJ) as a main organ of the UN and as its principal judicial organ. Article 38 of the Statute of the ICJ, is widely referred to as providing a list of the sources of international law.[13] This Article of the ICJ Statute distinguishes between three primary sources, namely conventions, international custom and the general principles of law recognized by civilized nations, and two secondary sources, namely subsidiary judicial decisions and the teachings of the highly qualified publicists of various nations.

While there is no treaty that specifically deals with cyber-attacks under international law, there are a number of sources which would be applicable to them, including customary international law rules and general principles of law. Article 38 (1b) of the ICJ statute describes international custom as 'a general practice accepted as law'. It is generally agreed that the existence of a rule of customary international law requires the presence of two elements - *State practice*, - and *opinio juris*, a belief that such practice is required, prohibited or allowed as a matter of law.[14] So far there has been no cyber-attack that has been publicly characterized and accepted by the international community as reaching the threshold of 'an armed attack'.[15] However there has been considerable discussion on whether and when cyber-attacks would fulfil the requirements of an armed attack.

[11] Crawford, in Brownlie's Principles of Public International Law (2012) page 20.

[12] Charter of the United Nations, 1945.

[13] Statute for the International Court of Justice, 1945.

[14] ICRC Study on Customary International Humanitarian Law, page xxxviii.

[15] Tallinn Manual, commentary nr. 13 to Rule 13 on page 57.

Article 38 (1)(d) provides that the teachings of the most highly qualified publicists of the various nations can be used as a subsidiary means for the determination of international law. The Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) is a nonbinding manual on the law governing cyber warfare. In 2009, the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) invited an 'International Group of Experts' (henceforward 'the experts') to produce a nonbinding manual on the law governing cyber warfare.[16]

The experts examined how international law applies to cyber warfare, and finally adopted 95 rules, that according to their view, represent customary international law, unless otherwise specified in the accompanying commentary to the rules. The manual is not an official document but represents the views of the experts involved.

The experts were legal practitioners, academics and technical experts. Three organizations were invited as observers, NATO's Allied Command Transformation, the US Cyber Command and the International Committee of the Red Cross. The observers could participate in all discussions, but the unanimity that was required for adoption of a Rule was limited to the experts.[17] Even though this manual is not an official document, it is a persuasive document, arrived at after years of in-depth discussions of relevant matters, by highly qualified experts, and I will be referring to it throughout this thesis.

[16] Tallinn Manual - page 1.

[17] Tallinn Manual pages 6-10.

3 Cyber attacks

'Cyber-attack' is a broad term that covers many aspects. It can be used to refer to a computer network attack (CNA),[18] or computer network exploitation (CNE).[19] The nature of cyber operations will mean that not every cyber operation or cyber-attack will be the same. How they are conducted, and their consequences will often hinge on the imagination and the skill of the attacker. The attacker can generate wrong information, for example by sending malware[20] that affects the computer system, or shuts down a system with a Denial of Service attack (DoS).[21] This could floods the computer network with communication requests, making it unavailable to its intended users. The attacker can also take control over the system, and make it do its own bidding. The consequences of manipulating or deleting data vary depending on what the target is, for instance there is a huge difference between defacing a government website, to shutting down the coolant systems of a nuclear reactor. In colloquial terms, both would probably be referred to as 'cyber-attacks', but 'attack' is a term with special meaning in IHL, and differs from other branches of law.[22]

---

[18] See the NATO GLOSSARY OF TERMS AND DEFINITIONS (2013): CNA is defined as 'Action taken to disrupt, deny, degrade or destroy information resident in a computer and/or computer network, or the computer and/or computer network itself'.

[19] Ibid. CNE is defined as 'Action taken to make use of a computer or computer network, as well as the information hosted therein, in order to gain advantage'.

[20] The Tallinn Manual's glossary defines malware as Instructions and data that may be stored in software, firmware, or hardware that is designed or intended adversely to affect the performance of a computer system. Page 260.

[21] E Tikk, K Kaska and L Vihul, International Cyber Incidents: Legal Considerations Glossary page 112 defines a DoS attack as 'a concerted malevolent effort to deny access to any electronic device, computer, server, network or Internet resource by its intended users. This can be accomplished in numerous ways, e.g. by ping-flood, UDP flood, malformed queries, and other means'.

[22] Knut Dörmann in Applicability of the Additional Protocols to Computer Network Attacks page 3.

Under Additional Protocol 1 (AP 1),[23] Article 49, attacks mean 'acts of violence against the adversary, whether in offence or in defence'. The Tallinn Manual draws upon this definition, and 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'.[24] A cyber operation is defined as 'the employment of cyber capabilities with the primary purpose of achieving objectives in or by the use of cyberspace'.[25] All cyber-attacks will consist of a cyber operation, but not all cyber operations will be considered as cyber-attacks.

By building upon AP 1 Article 49, the Tallinn manual separates the operations that results in inconveniences, and the ones that actually harm the target. It is the use of violence against a target that distinguishes cyber-attacks from cyber operations. Non-violent operations do not qualify as attacks.[26] The violence distinction is a useful one, though not entirely without problems. This paper will use the Tallinn Manual's terminology when it discusses cyber-attacks.

[23] Additional Protocol 1 OF 1977 - Protocol Additional to the Geneva Conventions of 12 August 1949.

[24] Rule 30 of the Tallinn Manual, page 106.

[25] Tallinn Manual page 258.

[26] See the commentary to Rule 30 note 2.

3.1 Distinguishing the *jus ad bellum* and the *jus in bello aspects of cyber-attacks*

When dealing with IHL, it is important to distinguish between the *jus ad bellum*, the rules for when states can go to war, and the *jus in bello*, the rules of conduct in a war. For the jus ad bellum, international law governs the use of force through the UN Charter Article 2(4) and Article 51.

Article 2(4) of the UN Charter provides that
"All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations".

While Article 51 provides that
"Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs … until the Security Council has taken measures necessary to maintain international peace and security".

Therefore a State may not resort to the use of force, besides in self-defence, or as a part of the collective security system, when the use of force has been authorized by the Security Council under Chapter VII of the UN Charter. For triggering the application of IHL in an international armed conflict situation, the question is whether an 'act of violence' has occurred.[27] In IHL there is no consideration on whether the armed conflict is based on a just cause or not. What matters under IHL is to limit the sufferings for those involved, and the destructive effects of armed conflict, independent of who started it or why.

The ICJ found in the 1986 *Nicaragua* Judgement[28] that it is necessary 'to distinguish the most grave forms of the use of force (those constituting an armed attack) from other less

[27] AP1 Article 49.

[28] ICJ, Military and Paramilitary Activities in and against Nicaragua,1986 (Merits).

grave forms',[29] and that an operation's 'scale and effects[30] can determine whether a use of force can be classified as an armed attack.

Despite this while a cyber-attack that causes damage will trigger IHL, it is not automatically given that the damage will be grave enough for the 'scale and effects' to effectively trigger an armed attack under *the jus ad bellum.* When it comes to the threshold for the start of application of IHL to an international armed conflict, there seems to be somewhat of a disconnection between treaty law and State practice. However, for the purpose of this thesis, not any cyber-attack will give rise to the application of IHL. The subsection below will discuss the issue of armed conflict and cyber-attacks within such a context.

3.2 Armed conflict

For IHL to apply there has to be an armed conflict. Armed conflict is a legal term that refers to international and non-international armed conflicts. Different treaty provisions and customary international law rules and principles will apply, depending on whether the conflict is international or non-international. According to the Common Article 2 of the Geneva Conventions (GC),[31] there is an international armed conflict in 'all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognised by one of them.
AP 1 Article 1(4) includes other forms of international armed conflicts where "peoples are fighting against colonial domination and alien occupation and against racist regimes in the exercise of their right of self-determination".[32]

---

[29] Ibid. Para 191.

[30] Ibid. Para 195.

[31] Geneva Conventions of 1949.

[32] AP 1 Article 1(4) is controversial, and might not reflect customary international law, see Jann K. Kleffner, 'Scope of Application of international humanitarian law' page 46 in Fleck,(ed) The Handbook of International Humanitarian Law (2013).

For non-international conflicts, Common Article 3 to the four 1949 GCs simply refers to 'the case of armed conflict not of an international character occurring in the territory of one of the High Contracting Parties', and provides certain minimum rules of humane treatment 'each Party' to the conflict needs to follow. This means that not only States, but every party to the conflict is bound by the provision. Article 3 is supplemented by Additional Protocol 2 (AP 2)[33] Article 1(1) which include additional criteria to the Party to the conflict, such as being an *'organized armed group', ' under responsible command' and ' exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement* [the] *Protocol'*.

Article 1(2) also sets a rather high threshold and excludes its applicability 'to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature…'. Thus two criteria apply for non-international armed conflicts: participation by an organized armed group, and a particular level of intensity.

Neither the Geneva Conventions of 1949 nor their Additional Protocols explicitly define 'armed conflict'. In the ICRC commentary to Common Article 2 of the GCs, an (international) armed conflict is described as "Any difference arising between two States and leading to the intervention of armed forces… It makes no difference how long the conflict lasts, or how much slaughter takes place".[34] This view depicts the so-called first-shot theory,[35] according to which the law of international armed conflict applies from the first moment that force is used by one state against another state. It is irrelevant what form the force takes, or what its intensity or duration is. Common Article 3 does not specify the threshold for when a non-international armed conflict occurs, but AP 2 does. Even though AP 2 is only binding on those States that have ratified it, its requirement that IHL does not apply to internal disturbances and tensions, such as riots, isolated and sporadic acts of

[33] Additional Protocol 2 OF 1977 - Protocol Additional to the Geneva Conventions of 12 August 1949.

[34] ICRC Commentary p.32.

[35] Jann K. Kleffner, 'Scope of application of international humanitarian law' page 44 in Fleck,(ed) The Handbook of International Humanitarian Law (2013).

violence or other acts of a similar nature is generally applied to all non-international armed conflicts.[36]

The concept of 'armed conflict' has however been defined by the International Criminal Tribunal for the former Yugoslavia (ICTY). In *Tadic* (1995),[37] the ICTY Appeals Chamber held that:

'an armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State'.

'Protracted' means that something has to last for a certain duration, but the exact threshold still remains unclear. The question that remains is what 'resort to armed force' means. As mentioned, the ICRC commentary to Article 2 for international armed conflicts rules out any intensity criteria, if the State armed forces intervene or engage against those of another State, that gives rise to an armed conflict. This view is however controversial. Another view on the threshold required for armed violence to amount to an armed conflict is provided by the ILA Study Group on the Use of Force.[38] After reviewing hundreds of violent situations since 1945, they found that the violence must be intense and be organized, in order for it to amount to an armed conflict triggering the application of IHL. They could not pinpoint the exact threshold, but in their view many isolated incidents such as border clashes and naval incidents show that contrary to what the ICRC commentary suggests, 'any difference leading to the intervention of armed forces' is not enough. According to this ILA Study Group, the minimum criteria for giving rise to an armed

[36] Dieter Fleck, 'The law of non-international armed conflict' page 593 in Fleck,(ed) The Handbook of International Humanitarian Law (2013).

[37] ICTY, Prosecutor v Tadic (1995) para 70.

[38] ILA Committee on the Use of Force, Conference Report The Hague (2010).

conflict, as reflected through custom, are the existence of organized armed groups, and that they are engaged in fighting of some intensity.[39]

The ILA Study Group seems to mix the *jus ad bellum* and the *jus in bello* when they proscribe that violence must be intense and be organized for international armed conflicts. In my view, it is not surprising that states have been reluctant to classify border clashes as armed conflicts, as doing so might escalate the situation. Unless tensions are very high, most States will not want to attack another State. By characterising an incident as an armed conflict, it makes it easier to retaliate, which in the end might escalate existing tensions into an actual armed conflict. It must be noted, however, that IHL will apply no matter if the parties acknowledge that there exists an armed conflict or not.[40]

Tom Ruys discusses several incidents ranging from small-scale uses of force to incidents of more substantial gravity where the use of force against another State was not considered an armed attack and no defensive action was undertaken due to a lack of 'hostile intent'. This hostile intent, the deliberate use of armed force against another State is particularly important for qualifying small-scale uses of force. He explains that when dealing with larger scaled uses of armed force, the subjective element will generally be implicit in the act itself. Conversely, when an unarmed missile launched from the territory of State A lands on to the territory of a befriended neighbour, there is no armed attack.[41] When dealing with more complex cases, it is according to Ruys important not only to differentiate on the basis of scale and effects, but to take into account of the broader context as well. Are relations between the States concerned friendly overall, or is there a hostile environment? Has the State offered an apology and/or reparation for its actions? Has it punished those

[39] ILA Committee on the Use of Force, Conference Report The Hague (2010) page 32.

[40] Article 2 of the Geneva Convention explicitly state that the Convention applies 'even if the state of war is not recognized by one of them'.

[41] Tom Ruys 'Armed Attack' and Article 51 of the UN Charter (2010) page 165-167.

responsible for the incident? Does the use of force constitute an isolated event, or does it form a part of a broader series of similar uses of armed force?[42]

Even though Tom Ruys discusses these issues from *a jus ad bellum* perspective, I think that his analysis can be useful for our *jus in bello* discussion of cyber-attacks. In my opinion, the reasoning as to why not every border clash gets labelled as an armed conflict, and why deliberate attacks with hostile intent are easier to trigger the application of IHL, can be applicable to cyber-attacks as well.

3.2.1 Cyber-attacks and armed conflicts

It follows from the discussion above that a cyber-attack would have to be deliberate, and amount to 'armed force'. But what does 'armed force' involve? Schmitt, Harrison and Wingfield argue that it must refer to the application of force, which in turn implies the causation of physical damage or human injury, regardless if the military is behind it or not.[43]

The experts of the Tallinn Manual agreed that a cyber-attack has the potential to amount to 'armed force'. The applicability of the law of armed conflict to cyber-attacks is expressed in Rule 20 of the Manual which provides that "Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict".[44] The experts further distinguish between international armed conflict cyber-attacks and non-international armed conflict cyber-attacks in Rules 22 and 23. For non-international armed conflicts, AP 2 Article 1(2) states that it does not apply "to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature". Together with the requirement of being protracted from the *Tadic* case, Schmitt writes that

---

[42] Ibid. page 167-168.

[43] Schmitt, Harrison and Wingfield, Computers and War: The Legal Battlespace 2004 page 4.

[44] Tallinn Manual Rule 20 page 75.

"This is a high threshold that would preclude many cyber operations from sufficing for the purpose of finding a non-international armed conflict. Even highly destructive cyber attacks would fail to qualify unless they occurred on a regular basis over time".[45] The Tallinn Manual in its commentary to Rule 23 also state that given the requisite threshold of violence and the degree of organization required, "cyber operations in and of themselves will only in exceptional cases amount to a non-international armed conflict".[46]

For international armed conflicts, the experts make note of the controversy regarding the threshold of the requisite violence, noting the ICRC commentary view on "Any difference arising" and the contrary view based on State practice and border clashes. The experts could thus not reach a consensus, but did agree that it would be prudent to treat the threshold of international armed conflict as relatively low, and that in all likelihood, such incidents would need to be evaluated on a case-by-case basis in light of the attendant circumstances.[47]

In my view, any cyber-attack that causes harm has the potential to trigger an armed conflict. While recalling that States will normally be reluctant to argue that an armed conflict exists, let us imagine a scenario where a hostile State conducts a cyber-attack on another States border patrol, hacking one of its vehicles, and causing an accident that results in the death of those border patrol soldiers. It is my view that this would be enough to trigger an armed conflict, due to the hostile deliberate cyber-attack of the attacking State.

Of course, the affected State could choose to classify the situation in another way. In the end, how the affected State responds would ultimately influence how the situation is classified. Note that the ICRC commentary talks about differences 'leading to the

---

[45] Schmitt, Classification of Cyber Conflict page 258.

[46] Tallinn Manual Commentary to Rule 23 note 2 page 85.

[47] Tallinn Manual – Commentary to Rule 22, note 12.

intervention of armed forces'.[48] If the State finds it in its own best interest not to pursue the matter, then it will not be an armed conflict.

If a cyber-operation constitutes an 'attack' under Article 49 of Additional Protocol 1, it would trigger the application of IHL. Article 49 states that "acts of violence against the adversary, whether in offence or in defence', constitute an attack".

Cyber operations are new developments of technology, and the drafters of the four Geneva Conventions and their Additional Protocols did therefore not have them in mind when they drafted the respective treaties. This fact however, cannot exclude IHL from being applicable to cyber operations. The 'Martens clause', which reflects customary international law, functions to ensure that no activities in an armed conflict remain unregulated by IHL.[49]

The 'Martens clause' is included in the GCs[50] and in Article 1(2) of the AP 1 which reads as follows:

"In 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."

The ICRC commentary of the Additional Protocols explains that the reason it was implemented was "First, despite the considerable increase in the number of subjects covered by the law of armed conflicts, and despite the detail of its codification, it is not possible for any codification to be complete at any given moment; thus the Martens clause prevents the assumption that anything which is not explicitly prohibited by the relevant treaties is therefore permitted. Secondly, it should be seen as a dynamic factor proclaiming

[48] ICRC Commentary (1952) page 32.

[49] Tallinn Manual note 10 to Rule 20 on page 77.

[50] The Martens clause can be found in the four Geneva Conventions: GCI Article 63, GCII Article 62, GCIII Article 142 GCIV Article 158.

the applicability of the principles mentioned regardless of subsequent developments of types of situation or technology".[51]

Further more, Article 36 of AP 1 requires states to determine the legality of new means and methods of war which indicates the applicability of the laws to newer technology. And finally, in its advisory opinion *on Legality of the Threat or Use of Nuclear Weapons* the ICJ dismissed the idea that nuclear weapons were not covered by IHL because the Geneva Conventions predated these weapons.[52] However, Article 49 requires an act of violence for it to constitute an armed attack. A question that must be answered is therefore whether a cyber-attack can be seen as an act of violence.

3.2.2 Cyber-attacks as an act of violence

A textual understanding of Article 49 of AP 1 requires a violent act for its qualification as an attack, and the commentary to this Article seems to link acts of violence with physical force.[53] Michael Schmitt points out that according to the 1969 Vienna Convention on the Law of Treaties (VCLT),[54] a treaty must be interpreted in context and in light of its object and purpose. At the time Additional Protocol 1 was adopted, cyber operations did not exist, and the purpose of Additional Protocol 1 is to protect the population. Schmitt points out that "Violence" merely constituted of a useful prescriptive shorthand for use in rules designed to shield the population from harmful effect. It is not the violence of the act that constitutes the condition precedent to limiting the occurrence of an attack, but the violence of the ensuing result.[55] He also points out that chemical and biological attacks are

---

[51] ICRC commentary page 38 and 39.

[52] Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226 para 85.

[53] Schmitt, Cyber Operations and the Jus in Bello: Key Issues page 5 refers to both the ICRC commentary to Additional Protocol 1, and to Bothe, Partsch and Solf's commentary in MICHAEL BOTHE ET AL., NEW RULES FOR VICTIMS OF ARMED CONFLICTS 289 (1982).

[54] Vienna Convention on the Law of Treaties art. 31(1), May 23, 1969.

[55] [55] Schmitt, Cyber Operations and the Jus in Bello: Key Issues page 5 and 6.

considered to be an attack, even though it is not violence through kinetic force, but rather its harmful consequences.[56]

A cyber operation where someone writes a code in itself is not necessarily violent, but its consequences could be. That is why the Tallinn Manual also includes the violent results in its definition in Rule 30; 'that is reasonably expected to cause injury or death to persons or damage or destruction to objects'.[57] Most commentators share the view that if a cyber operation has the same effects as kinetic resort to force, it would trigger an international armed conflict.[58] It is hard to see any justification for why a cyber attack that causes the same harm as for instance a bomb, should be treated any different under IHL.

But what about cyber-attacks that do not have the same effects as kinetic resorts to force? Article 48 of AP 1 states:
'In order to ensure respect for and protection of the civilian population and civilian objects, the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives'. This article sets forth the principle of distinction, which is considered to reflect customary international law,[59] and is referred to by the ICJ in its advisory opinion on *Legality of the Threat or Use of Nuclear Weapons* as one of the cardinal principles of international humanitarian law.[60]

---

[56] Ibid. Page 6.

[57] Tallinn Manual Rule 30.

[58] Cordula Droege Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians, page 546. See also Schmitt, 'Attack" as a Term of Art in International Law: The Cyber Operations Context' (2012) who says There is universal agreement on this point at page 292.

[59] ICRC Study on Customary International Humanitarian Law, Rule 1.

[60] Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion) [1996] ICJ Rep 226 para 78.

Schmitt writes that 'Although the principle of distinction is framed in terms of "military operations," it is clear that not all military operations are contemplated by the norm'.[61] He points to how State practice shows that non-destructive psychological operations that are directed at the civilian population, such as dropping leaflets, broadcasting to the enemy population, or even jamming enemy public broadcasts are lawful as long as no physical consequences attend them, and that the principle of distinction is primarily meant to address 'attacks'.[62]

To prove this, he refers to Article 48's placement in the treaty, and how it appears in the Chapter on "Basic Rule and Field of Application" of the treaty's conduct of hostilities section. According to him, 'Since the only other article in the Chapter is Article 49, which defines attacks, this placement implies that the military operations referred to in Article 48 are primarily attacks'.[63] He also points out how the subsequent articles are also framed in terms of prohibitions and restrictions on attacks, which he illustrates with Article 51. 'It begins by noting that the "civilian population and individual civilians shall enjoy general protection against dangers arising from military operations," but operationalizes the provision by noting that "to give effect to this protection" it is prohibited to attack…'.[64] In his view, it is legal to conduct military operations that do not qualify as attacks on civilians. The same goes for cyber operations. Only those cyber operations that cause injury or death to persons, or damage or destroys objects, count as cyber-attacks. In his view, the *lege lata* is that cyber operations can be directed at civilian systems, as long as the requisite type of harm is not triggered and no other specific international humanitarian law prohibition applies.[65]

---

[61] Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context Page 289.

[62] Ibid.

[63] Ibid.

[64] Ibid.

[65] Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context Page 293.

Cordula Droege thinks that the argument that some operations, such as psychological operations, can be directed at civilians, implying that some military operations could be directed at civilians, rests on a misunderstanding of the concept of military operations.[66] She further explains that operations are meant to describe military operations, and that this term refers to all movements and acts related to hostilities that are undertaken by armed forces. The reason that operations such as propaganda, espionage, or psychological operations does not fall under the concepts of hostilities is because they do not fall within the meaning intended by the Protocols drafters.[67]

According to Knut Dörmann, the fact that a cyber-operation does not lead to the destruction of the object attacked is irrelevant. In accordance with Article 52(2) of AP 1, only those objects, which make an effective contribution to military action, and whose total or partial destruction, capture or neutralization offers a definitive military advantage, may be attacked. According to Dörmann, by referring not only to destruction or capture of the object, but also to its neutralization, the definition of military objects implies that it is irrelevant whether an object is disabled through destruction or in any other way.[68]

According to Schmitt, Dörmann's proposed remedy dispenses with the requirement for damage, destruction, death or injury for an action to qualify as an attack. Schmitt thinks that this approach goes too far, since it would also encompass all denial of service attacks, including those which result in mere inconvenience. It also relies on law that is not to the point when it refers to the definition of military objectives. In Schmitt's view, the question of whether something is an attack must be answered before one goes to the issue of whether something is a military objective. If it is indeed an attack, then the definition of military objects come into play, but otherwise it does not.

---

[66] Cordula Droege, Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians page 556.

[67] Ibid.

[68] Knut Dörmann Applicability of the Additional Protocols to Computer Network Attacks page 6.

"The issue with regard to the definition of military objectives is what may be attacked, not how or with what consequences'.[69] Regarding 'neutralization', Schmitt writes that the drafters envisioned it in the context of an attack, and quotes Bothe et al that the term was included to encompass cases involving "an attack for the purpose of denying the use of an object to the enemy without necessarily destroying it".[70]

Cordula Droege argues that Schmitt fails to acknowledge that 'neutralization' was meant to encompass 'an attack for the purpose of denying use of an object to the enemy without necessarily destroying it', and that the drafters had in mind not only attacks that are aimed at destroying or damaging objects, but also attacks for the purpose of denying the use of an object to the enemy without necessarily destroying it. As an example she uses an enemy's air defence system, which could be neutralized through a cyber operation for a certain duration by interfering with its computer system, but without necessarily destroying or damaging its physical infrastructure.[71]

Nils Melzer takes another look at attacks, and dismisses both Schmitt's and Dörmann's view, pointing out that both arguments have their strong points, but neither seems to provide a satisfactory interpretation of the notion of attack in relation to cyber operations. On the one hand he says, "it would hardly be convincing to exclude the non-destructive incapacitation of a state's air defence system or other critical military infrastructure from the notion of attack simply because it does not directly cause death, injury or destruction. On the other hand, it may well be exaggerated to extend the notion of attack to any denial of service attack against, for example, online shopping services, travel agents or telephone directories".[72] In his view, the rule of distinction is not only found in terms of 'attacks, but

---

[69] Schmitt, Cyber Operations and the Jus in Bello: Key Issues page 7 and 8.

[70] Ibid page 8 and quotes Michael Bothe ET AL., New Rules For Victims of Armed Conflicts page 325 (1982).

[71] Cordula Droege, Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians page 558.

[72] Nils Melzer, Cyberwarfare and International Law page 26.

also in terms of 'operations'. Instead of focusing on 'attacks', one should focus on 'hostilities', and the question should not be whether the operation in question qualifies as 'attack', but on whether it constitutes part of hostilities within the meaning of IHL.[73] This would mean that cyber operations designed to harm the adversary, either by directly causing death, injury or destruction, or by directly adversely affecting military operations or military capacity, must be regarded as 'hostilities' and therefore subject to all restrictions imposed by IHL. Cyber operations that disrupt or incapacitate the military, but lacks physical damage would also qualify as part of the hostilities, and be subject to restrictions.[74] Cyber operations causing neither death, injury or destruction, nor military harm, on the other hand, such as general intelligence gathering, or operations conducted for purely criminal purposes or otherwise unrelated to the hostilities would fall short of the concept of "hostilities" and therefore not be governed by IHL on the conduct of hostilities.[75]

Melzer's hostilities-based approach does not solve the question of how a cyber operation aimed at a civilian object, but with non-destructive incapacitation would be classified, if the operation lacked military harm, death, injury or destruction. As an example Melzer uses the non-destructive incapacitation of a power station used exclusively for civilian purposes, so without military harm.[76] He admits that the question remains unresolved, and the issue boils down to the dilemma between adopting either a too restrictive or a too permissive interpretation of the law, and how one can classify 'destruction'.[77]

The Experts of the Tallinn Manual did not reach a consensus on what classifies as 'damage' to objects. As mentioned, the Manual defines a cyber-attack as a 'cyber

[73] Ibid. page 27.

[74] Ibid. page 28

[75] Ibid.

[76] Ibid.

[77] Ibid.

operation… that is reasonably expected to cause injury or death to persons or damage or destruction to objects',[78] but they fail to classify what damage to an object means. The majority of the experts were of the view that interference with functionality qualifies as damage if restoration or functionality requires replacement of physical components, but were split over whether the 'damage' requirement is met when functionality can be restored by reinstalling the operating system.[79] A few experts suggested that it does not matter how an object is disabled, and that it is the object's loss of usability that qualifies as 'damage'.[80]

It is the violent consequences of a cyber-attack that determine whether it will trigger the application of IHL. Imagine a cyber operation that is directed towards the traffic lights of a city, turning all the lights red in order to cause traffic jams. This would cause inconveniences, but not any harm, and would therefore not be characterised as a cyber-attack that triggers the application of IHL. However, if the same cyber operation rather turns all the traffic lights green, then any accidents caused by the operation would make it into a cyber-attack, which would trigger the application of IHL. The focus on the operations violent consequences is necessary to prevent IHL to be watered down. IHL offers protection against harm for those not taking part in the conflict, but it does not protect against inconveniences. However, I think it is prudent to distinguish cyber-attacks that trigger the application of IHL, and cyber operations conducted once an armed conflict already exists.

While I agree with Schmitt that a cyber-attack should have violent consequences in order to trigger an armed conflict, I disagree with the view that once an armed conflict is in place, civilians can be targeted by any cyber operation that does not reach the threshold of cyber-attacks. It is impossible to place all cyber operations under one umbrella, because the term is so broad. Rather, the legality of the operation should depend on what the cyber operation

---

[78] Tallinn Manual Rule 30 page 106.

[79] Ibid. commentary to Rule 30, note 10, page 108-109.

[80] Ibid. commentary to Rule 30, note 11, page 109.

is designed to do and its intended consequences. This assessment would have to be made on a case-by-case basis.

Schmitt's examples of certain operations such as propaganda operations or jamming operations being allowed, does not change this. Sending emails to the civilian population such as urging them to capitulate might be legal,[81] but that does not necessarily make any other cyber operation legal too. Jamming operations are not operations that target civilians per se, it just affects them negatively. The key in those operations is 'denying the enemy's ability to pass key information at critical times',[82] it is the enemy that is targeted for jamming, civilians are affected but they are not the target. However, I disagree that these examples illustrate that there should be a blanket acceptance of targeting civilians with cyber operation not having destructive consequences in order to achieve a military goal. In my view it would go against the spirit and intention of the principle of distinction.[83] Also, such a broad understanding would be treading a thin line as in their entirety such operations could be intended to collectively punish or to spread terror among the civilian population.

My point is that one cannot have a blanket acceptance of targeting cyber operations towards civilians. What if in an armed conflict, State A hacks the power grid that exclusively provides power to civilians and not military, but configures it so that hospitals still get power. They then drop leaflets saying that the civilians will be out of power until their leaders come to their senses and capitulate. In this example, the cyber operation did not cause any harm, it simply turned off the power. Since hospitals were not affected, lives were not lost. Still, the civilians were targeted, and the civilian power grid was not a military objective because the military was not connected to it. Another example is State A

[81] Example taken from the Tallinn Manual commentary to Rule 31, note 5 page 112.

[82] US Army Field Manual 34-40-7 - Communications Jamming Handbook page 1-1.

[83] The experts of the Tallinn Manual disagrees with this view. In their view, 'Only when a cyber operation against civilians or civilian objects (or other protected persons and objects) rises to the level of an attack is it prohibited by the principle of distinction and those rules of the law of armed conflict that derive from the principle'. The Tallinn Manual commentary to Rule 31 note 5, page 112.

broadcasting that until the leaders of State B come to their senses, everyone's emails will be deleted, and then they proceed to delete the civilians emails. This does not cause any harmful consequences, but the civilians are still targeted even though they are not military objectives. This does not comply with the principle of distinction, even though the operation does not rise up to the level of attacks.

Let us take another example to illustrate the difference between whether there is an armed conflict or not. If tensions are just high between two States, and State A starts deleting emails, it will not cross the threshold of violence, so IHL will not apply. This does not mean that what State A does is legal, but it would fall under another branch of international law, for instance the prohibition on intervention. On the other hand, if the armed conflict is already in place, then IHL would prevent the civilians from being targeted by some cyber operations. Not all cyber operations would be prevented. As mentioned propaganda might be allowed, but harassing the civilians in order to coerce their leaders into submission would not be allowed. It would have to be determined on a case-by-case basis whether a particular cyber operation is allowed or not and generally cyber operations against civilians would be prohibited.

It is worth noting that most academics point out that the meaning of the legal term may shift over time, and that new treaties, new customary law norms might develop and give new understanding to the meaning of cyber-attacks.[84] There has still to occur a cyber-attack which triggers the application of IHL, or cyber operations that target civilians during an armed conflict in such ways as discussed above. The more incidents that happen, the more State practice we will get, and the rules will be clarified.

[84] See for instance Schmitt, "Attack" as a Term of Art in International Law: The Cyber Operations Context page 293, Melzer, Cyberwarfare and International Law page 36.

3.3 Conclusion

A cyber-attack can trigger the application of an armed conflict and IHL, but it needs to have the potential to cause injury or death to persons or damage or destruction to objects. Cyber operation against civilians would generally be prohibited, but would not be sufficient in itself to trigger IHL.

4 Prohibition on attacking civilians and civilian objects

As previously mentioned, IHL tries to limit destruction and the suffering of those affected by an armed conflict. This chapter will focus on one aspect of that, namely the prohibition on attacking civilians and civilian objects, and give examples on how cyber-attacks can fit into the already existing rules.

4.1.1 Basic rules and definitions

Distinguishing between civilians and combatants

It is considered customary international law that the parties to the conflict must distinguish between civilians and combatants.[85] AP 1 has codified this principle in Articles 48 and 51(2), which state respectively that: "the Parties to the conflict shall at all times distinguish between the civilian population and combatants and between civilian objects and military objectives and accordingly shall direct their operations only against military objectives".[86] And "The civilian population as such, as well as individual civilians, shall not be the object of attack. Acts or threats of violence the primary purpose of which is to spread terror among the civilian population are prohibited".[87] Civilian objects shall also not be the object of attack.[88]

As mentioned above, in my view this means that civilians cannot be targeted by either cyber-attacks or certain cyber operations that goes into the territory of harassment. Advancements in technology have made it possible to conduct cyber operations that target civilians and harass them by means that were not conceived of or thought of by the drafters of the Geneva Conventions and their commentators. Back then, kinetic attacks constituted the real danger. Now the situation is that a cyber-operation has the potential to affect

[85] ICRC Study on Customary International Humanitarian Law, Rule 1.

[86] Ibid. Article 48.

[87] Ibid. Article 51(2).

[88] Ibid. Article 52(1).

civilians in a way that was only possible before through kinetic means, but still without causing death, injury or damage. To argue that these operations should be allowed because AP 1 only bans attacks goes against the spirit and intention of the principle of distinction, and blur the line on who can be legally attacked. In my opinion, by not having clear lines, a potential for abuse arises. It is bad enough that, as the ICRC Commentary points out, "acts of violence related to a state of war almost always give rise to some degree of terror among the population"[89], but if the threshold for targeting civilians is dropped, then their suffering increases. Another point highlighted by Heather Dinniss is that when the ICRC commentary refers to military operations during which violence is used, it does so in order to distinguish operations of a military nature rather than 'ideological, political or religious campaigns, and in its referral to the dictionary, military operations refers to all movements and acts related to hostilities that are undertaken by armed forces.[90]

According to the ICRC Commentary to AP 1, the ban on spreading terror in Article 51(2) of AP 1 is intended for acts of violence that spread terror among the civilian population without offering substantial military advantage.[91] Such acts could easily also be conducted with cyber-attacks, so the Tallinn Manual has also included the ban in Rule 36. However, that ban only applies to cyber-attacks, not cyber operations. In the commentary to Rule 36, an example that would not fall under the ban would be using Twitter to cause panic by spreading rumours that a highly contagious and deadly disease is spreading rapidly throughout the population.[92] A minority of the experts, however, took the position that Article 33 of GC 4, Article 51(2) of AP 1, and State practice has resulted in a customary norm prohibiting any operations, including cyber operations, intended to terrorize the civilian population.[93] I agree with the minority of experts.

---

[89] ICRC Commentary to AP 1 para 1940

[90] ICRC Commentary to AP 1 para 1875 and Heather Harrison Dinniss. Cyber Warfare and the Laws of War page 199.

[91] ICRC Commentary to AP 1 para 1940.

[92] Commentary to Tallinn Manual Rule 36 note 3, page 123.

[93] Ibid. Note 7, page 124.

Regarding cyber-attacks, any cyber-attack that can cause harm may not be directed towards civilians. IHL is clear on this point, requiring that attacks can only be directed against military objectives, and civilians shall not be the object of attack.[94] This requirement applies to any means and methods of warfare. No excuses can be made for intentionally directing cyber-attacks against civilians. IHL does not guarantee that civilians will be unaffected by military operations, but one can never intentionally direct an attack against a civilian. It does not matter if the attack would shorten the course of the conflict, for example by conducting cyber-attacks against a civilian leader's private property and damaging it to pressure him into capitulation.[95] Although protected from being made the object of attack, civilians will lose this protection if they directly participate in hostilities, This issue is dealt with in more detail below.

Definition of civilian, civilian population and military objects

A civilian is a person who is not a member of the armed forces. In cases of doubt whether someone is a civilian, that person is to be considered as a civilian.[96] 'The civilian population comprises all persons who are civilians' and 'the presence within the civilian population of individuals who do not come within the definition of civilians does not deprive the population of its civilian character'.[97]

Civilian objects are those objects that are not military objectives.[98] Objects will be military objectives if they 'by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage'.[99]

---

[94] Additional Protocol 1 Article 48 and 52(2).

[95] Example from the Tallinn Manual, commentary to Rule 31, note 6.

[96] Ibid. Article 50.

[97] Ibid. Article 50 (2) and (3).

[98] Ibid. Article 52.

[99] Ibid. Article 52 (2).

In cases of doubt, objects that are normally used for civilian purposes are to be presumed as not being used for military purposes.[100]

Civilians shall not take direct part in hostilities

Civilians are protected against attacks by virtue of being a civilian. They are per definition not a member of the armed forces,[101] and are non-combatants. IHL strives to offer them protection, and they are protected from direct attack and against the dangers arising from military operations.[102] IHL does not ban civilians from participating in the armed conflict, but does set out consequences for doing so. If a civilian takes a direct part in the hostilities, he or she will lose their protection for such time as he partakes in the hostilities.[103] Such time as he partakes in the hostilities does not only refer to the time someone is actually conducting hostilities. Those attempting to be 'farmers by day and fighters by night' lose protection from attack even in the intermediate time-frames punctuating military operations, if they assume a continuous combat function.[104]

The same rationale applies if an individual joins an organized armed group that partakes in hostilities, he would lose civilian protection for as long as that membership lasts, and may be targeted, even when not personally linked to any specific hostile act—simply due to his membership in such a group—as long as that membership endures.[105] So if a civilian joins a hacker group that conducts cyber-attacks in an armed conflict that produce harmful effects, their membership in that group might get them targeted. Note that this only applies if the group commits attacks which have similar effects to those of normal kinetic attacks. A membership in a criminal hacker group unrelated to the armed conflict would not make someone a legal target under IHL.

---

[100] Ibid. Article 52 (3).

[101] Ibid. Article 50(1).

[102] Ibid. Article 51 (1) and (2).

[103] Ibid. Article 51(3).

[104] Dinstein, The Principle of Distinction and Cyber War in International Armed Conflicts page 276.

[105] Ibid.

Geneva Convention 3, Article 4A(6) provides for an exception for situations where a civilian can participate in an armed conflict, and qualify as combatant. That situation is referred to as '*levee en masse*' and is considered a 'long-standing rule of customary international law'.[106] *A levee en masse* exists when "Inhabitants of a non-occupied territory who, on the approach of the enemy, spontaneously take up arms to resist the invading forces, without having had time to form themselves into regular armed units, provided they carry arms openly and respect the laws and customs of war".[107]

The Tallinn Manual has included *'levee en masse'*, and provides that inhabitants of unoccupied territory who engage in cyber operations as part of *levee en masse*, enjoy combatant immunity and prisoner of war status.[108] The commentary to Rule 27 note that if the inhabitants of an unoccupied enemy, spontaneously begin to conduct cyber-attacks to resist the invading troops, it could arguably be seen as a *levee en masse* if the operations involve a large segment of the population and they target the invading force. However, the means and expertise necessary to engage effectively in cyber operations may be relatively limited in the population, and it is unclear whether a *levee en masse* can consist of a significant portion of the cyber-capable members of the population.[109] The commentary also note that it is questionable whether a *levee en masse* can target cyber operations against enemy military objectives other than the invading forces.[110]

There are good reasons for why it should only apply for cyber operations against the invading force. First of all, a textual reading of GC3 Article 4A(6), shows that it is meant for civilians repelling an invading force. With this purpose in mind, it does not make sense

---

[106] It is also considered customary international law, see ICRC Study on Customary International Humanitarian Law 387.

[107] Geneva Convention 3, Article 4A(6).

[108] Tallinn Manual, Rule 27, page 102.

[109] Tallinn Manual, Commentary to rule 27, note 3

[110] Ibid. Note 4.

that a civilian can also attack other enemy targets that would not delay the invading force, and still deserve to be protected as a non-combatant.

The commentary to the Tallinn Manual Rule 27 state that it is also questionable whether a *levee en masse* can also be associated with civilians countering a massive cyber-attack with effects that are comparable to those of a physical invasion by enemy forces. The experts were divided, but the majority viewed *levee en masse* to be understood in a narrow sense, requiring the physical invasion of national territory.[111]

The majority's view is a reasonable one. The concept acknowledges that civilians can help repel an enemy invasion, even though they have not had time to organise themselves yet. Time is of the essence in this situation. By allowing civilians to counter-attack cyber-attacks, they are no longer repelling an invasion, they are instead conducting operations themselves, something which should be limited to combatants. By allowing them to conduct cyber-attacks themselves, the definition of civilian loses some of its meaning.

Doubt regarding the status of a person

In cases of doubt whether someone is a civilian, that person is to be considered as a civilian.[112] This important presumption is adopted by the Tallinn Manual.[113] Exactly how much doubt is sufficient remains unsettled, but it needs to be more than the mere existence of some doubt.[114] The UK manual holds that it is only in cases of substantial doubt that the person is to be considered a civilian.[115] The Norwegian manual provides that a target can only be attacked if it is highly probable that the target is a valid military target.[116] That

[111] Ibid. Note 5.

[112] Ibid. Article 50.

[113] Tallinn Manual Rule 33, page 114.

[114] Ibid. Commentary to Rule 33, note 3.

[115] UK Manual for the Law of Armed Conflict point 5.3.4.

[116] Manual i Krigens Folkerett (my translation) point 2.5.

decision needs to be made by a military commander on the basis of reliable information and intelligence at his or her disposal at the given time.[117]

4.1.2 Cyber-attacks and targeting

The nature of cyber-attacks allows for it to be precise in its targeting, and can reduce the risk of collateral damage. It is safer for civilians if a State turns off an enemy power generator by hacking it compared to bombing it. There are however certain rules that a State has to abide by, namely the principle of distinction, limiting their attacks to military objectives, and that an attack must conform to the principles of distinction, proportionality and necessity.

The principle of distinction:

The principle of distinction is already mentioned. The parties must distinguish at all times between civilians and combatants, and can only direct their operations against military objectives.[118] Military objective is defined in AP 1 Article 52(2), and is limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.[119] Thus, attacks can only be carried out on military targets that make an effective contribution to military action, and the attack must offer a military advantage.

The object must make an effective military contribution, hypothetical or merely 'possible' military uses will not be seen as military objectives.[120] The military advantage must be definite and concrete, not hypothetical.[121] To illustrate, a power station might provide

[117] UK Manual for the Law of Armed Conflict point 5.3.4.

[118] AP 1 Article 48.

[119] Ibid.

[120] Kolb and Hyde, An introduction to the International Law of Armed Conflicts (2008) page 131.

[121] Ibid.

power to both a military base and civilians, and would through its use make an effective contribution, and thus be a military objective. The next question is then if the cyber-attack on the power station would offer a definite military advantage. Would the cyber-attack offer any military advantage? If the mission planners know that the base has backup generators, then the attack might not offer any advantage. Also, States consider that the 'military advantage' refers to the advantage anticipated from the military attack considered as a whole and not only from isolated or particular parts of that attack.[122] So if a cyber-attack is conducted alongside regular kinetic attacks, the whole attack would be considered under one attack when considering the military advantage.

Once a target is determined to make an effective contribution to military action, and is therefore a military object, and the attack is determined to offer a definite military advantage, it must undergo a proportionality assessment. This will be discussed below. As illustrated by the power station example, an object can have both military and civilian purposes, and is referred to as 'dual use object', but if a civilian object is used to make an effective contribution to military action it will be considered a military object.

The principle of distinction also means that it is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature.[123] Such means could be viruses and worms that do not distinguish between targets. To follow this rule, those who launch the cyber-attack in form of a virus or worm, can insert them into a closed system, or the designer of the cyber-attack can program it to check for certain conditions existing on the network or system prior to infection.[124] Other possible measures can be designing the virus or worm to only last for a specific amount of time.

---

[122] ICRC Study on Customary International Humanitarian Law page 49.

[123] Tallinn Manual Rule 43.

[124] Heather Harrison Dinniss. Cyber Warfare and the Laws of War (2012) page 203.

That an attack is limited to military objectives does not mean that attacks that also affect civilians will be unlawful. Several States have stressed that Article 52(2) only prohibits direct attacks against civilian objects and does not deal with the question of incidental damage resulting from attacks directed against military objectives.[125] For example,[126] if a cyber operation is designed to take down an enemy military aircraft by attacking a military air traffic control system, it is an attack on a military object, even though civilians might get harmed when it crashes. IHL does not prohibit collateral damage; it merely tries to limit it. Whether the attack is tolerable is a question of its necessity and proportionality. Note that both the *jus ad bellum* and *jus in bello* contain principles of necessity and proportionality, but it is important to be aware that the two concepts have different meanings.[127] For our purposes, it is the meaning within the *jus in bello* that will matter.

The principle of necessity:

The principle of necessity requires that the belligerent only adopts such measures as are necessary to overpower the enemy and to bring about its surrender.[128] The rule is expressed in AP 1 Article 57(3); "When a choice is possible between several military objectives for obtaining a similar military advantage, the objective to be selected shall be that the attack on which may be expected to cause the least danger to civilian lives and to civilian objects".

The Tallinn manual has adopted this principle in Rule 56, but because a minority of experts disagreed that it had reached customary status, they added to the rule that it only applies to States party to Additional Protocol 1.[129] To illustrate this with an example, if the military objective was to take down an enemy aircraft, and the State had a choice between conducting a cyber-attack on the air traffic control system or take down the aircraft with

[125]ICRC Study on Customary International Humanitarian Law page 29.

[126] Example taken from the Tallinn Manual Commentary to Rule 32, note 6 page 114.

[127] Tallinn Manual, Commentary to Rule 14 note 1, page 62.

[128] Kolb and Hyde, An introduction to the International Law of Armed Conflicts (2008) page 47.

[129] Tallinn Manual commentary to Rule 56 note 1, page 171.

traditional kinetic means, the State would have to assess what causes the least danger to the civilians. In this example the risks to civilians would however most likely be the same. Another clearer example is that of either bombing a power grid or disabling it with a cyber-attack. Bombing would put more civilians at risk, so the principle of proportionality and precautions in attack would give an obligation to use a cyber-attack.

The principle of proportionality:

This principle means that the military advantage obtained by a particular operation must outweigh the damage caused to civilians and civilian objects by that action.[130] It is expressed in AP 1 Article 51(5)b which states that an attack is indiscriminate if it "may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".

The principle is generally accepted as customary international law applicable in both international and non-international armed conflicts.[131] The Tallinn Manual has also adopted it in Rule 51. The ICTY addressed how to determine whether an attack is proportional in the Galić judgement, and found that "[i]n determining whether an attack was proportionate, it is necessary to examine whether a reasonably well-informed person in the circumstances of the actual perpetrator, making reasonable use of the information available to him or her, could have expected excessive civilian casualties to result from the attack".[132]

But military advantage and civilian casualties have no common denominator. Dinstein says they are rather like metaphorical apples and oranges, and to compare between them is an art and not a science.[133] It is possible to count civilian losses and the value of damaged

---

[130] Kolb and Hyde, An introduction to the International Law of Armed Conflicts (2008) page 48.

[131] Tallinn Manual Commentary to Rule 51, note 1 page 159.

[132] Tallinn Manual Commentary to Rule 51, note 13 page 163 referring to ICTY Galić Trial Chamber Judgement, para. 58.

[133] Dinstein, The Principle of Distinction and Cyber War in International Armed Conflicts page 271.

property, but military advantage cannot always be assessed on any measurable objective scale.[134]

The principle of precautions in attack

In addition to undertaking a proportionality assessment, those who plan or decide on an attack must also take all feasible precautions to avoid or minimize incidental loss of civilian life, injury to civilians and damage to civilian objects. It is considered as customary international law,[135] and reflected in AP 1 article 57. The Tallinn Manual has also included it in Rule 55, which holds that 'Those who plan or decide upon attacks shall refrain from deciding to launch any cyber attack that may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated'.[136] This is basically a restatement of AP 1 Article 57 (2)(a)(iii.

The obligation to take all "feasible" precautions has been interpreted by many States as being limited to those precautions which are practicable or practically possible, taking into account all circumstances ruling at the time, including humanitarian and military considerations.[137]

Article 57 of AP 1 provides that certain precautions must be taken. Constant care must be taken to spare the civilian population, civilians and civilian objects.[138] This implies that everyone involved in a military operation must be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and to seek to avoid any unnecessary effects thereon.[139]

---

[134] Ibid.

[135] ICRC Study on Customary International Humanitarian Law Rule 15 page 51.

[136] Tallinn Manual Rule 55, page 170.

[137] ICRC Study on Customary International Humanitarian Law page 54.

[138] AP 1 Article 57(1), and is also adopted by the Tallinn Manual in Rule 52.

[139] Tallinn Manual Commentary to Rule 52 note 4 page 166.

Those who plan or decide the attack must do everything feasible to verify that the objectives to be attacked are neither civilian nor civilian objects and are not subject to special protection.[140] The ones actually conducting a cyber-attack also have an obligation to abort their attack if it becomes apparent that the target is no longer a military objective or is subject to special protection.[141]

4.2 Conclusion

Only military objectives may be the target of cyber-attacks. Once a military objective is selected, the question arises whether attacking it would offer a definite military advantage, and whether the cyber-attack would be proportionate to the probable civilian casualties. Those who plan or decide on a cyber-attack must also take all feasible precautions to avoid or minimize civilian casualties.

Cyber-operations should be assessed on a case-by-case basis, but cyber operations against civilians would generally be prohibited. The rules of distinction, proportionality and taking precautions are there to ensure that civilian losses and sufferings during an attack are limited as much as possible.

[140] AP 1 Article 57 (2)(a)(i) and Tallinn Manual Rule 53.

[141] AP 1 Article 57 (2)(b).

5 The cases of Estonia, Georgia and Iran (Stuxnet) in a cyber-attack perspective

We will now take a look of real world examples of cyber operations in the light of the principles discussed in the last chapter, and see whether the following cases can be classified as cyber-attacks or not, and if they are, whether they were in compliance with the rules of IHL.

The case of Estonia

At the end of April 2007, riots broke out in Estonia by youth groups of mostly Russian origin, after the government had decided to remove a soviet-era Second World War memorial. Not long after the riots, on April 27 web pages of Estonian government institutions and news portals came under a wave of cyber operations that lasted for more than three weeks.[142]

The means of attack used in the April-May 2007 events included denial of service (DoS) and distributed denial of service (DDoS) attacks, defacement of governmental websites, and large amounts of comments and email spam. Public propaganda, distributed on different Internet forums, and dissemination of attack instructions were employed to encourage, coordinate and aid in carrying out the attacks.[143]

As was discussed in the previous chapter on cyber-attacks and armed conflict, there needs to be a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State in order for an armed conflict to arise.

[142] E Tikk, K Kaska and L Vihul, International Cyber Incidents: Legal Considerations page 15 and 16.

[143] Ibid. Page 20.

In the Estonian situation, there is no proof that the Russian Federation was behind the attacks, or that they controlled the hacktivists, so on that basis there cannot be an international armed conflict. But for arguments sake, let us assume that these attacks were conducted by the Russian Federation. Would they then reach the threshold of an armed conflict?

The operations were launched with hostile intent, but defacing of governmental websites, sending of spam emails and distributing propaganda does not fit with the definition of cyber-attacks which requires a certain level of damage. Since such attacks did not reach the threshold for an international armed conflict, they would not satisfy the intensity criteria for non-international armed conflicts either. Even if that were the case, the hackers were not sufficiently organized in groups that had the power to implement IHL. The cyber operations were illegal, but they would nevertheless not trigger the application of IHL.

The case of Georgia

In August 2008, armed conflict broke out between the Russian Federation and Georgia over South Ossetia. South Ossetia had declared independence from Georgia in 1991, but remained commonly recognised by the international community as an integral part of Georgia. On August 7, 2008, Georgian forces launched a surprise attack against separatists in South Ossetia. The Russian Federation referred to national obligations to protect Russian citizen abroad, and on August 8, they responded with military operations into Georgian territory. Before the Russian invasion commenced, cyber operations were already being launched against a large number of Georgian governmental websites. Military operations were ended by a ceasefire agreement on August 12, but cyber operations continued throughout the rest of the month.[144] The website of the Georgian President became unavailable, when it later became available it was hacked to make him look like Hitler, Georgian news portals were attacked, the largest commercial bank of Georgia came under

[144] Ibid. 67 and 68.

attack and public websites were defaced, and a list of Georgian politician's email addresses was distributed for spamming.[145]

Again there is no conclusive proof of who was behind the cyber operations,[146] but for the sake of argument let us assume that the Russian Federation was behind them. In this hypothetical situation, there is already an on-going armed conflict with traditional kinetic means, so the rules of targeting will apply even though they do not reach the necessary harmful consequences that are required in order to give rise to an armed conflict. But recall that not all cyber-operations will automatically be prohibited, since that has to be determined on a case-by-case basis.

First of all, there is the situation that the cyber operations were launched before the Russian invasion commenced. These cyber operations in themselves do not reach the required threshold of violent consequences. Had the cyber operations been conducted in order to ease the later invasion, they would have been part of the invasion attack, and therefore fall under the rules of armed conflict. However, since they were not made to ease the invasion, they fall outside IHL.

The cyber operations conducted between August 8 and the ceasefire on the August 12, however, fall within IHL. The cyber operations conducted during this period have to conform to the principles of distinction, necessity, proportionality and precautions in attack. In this time period, the Presidents website was brought offline, he was made to appear as Hitler, the bank was under cyber-attack, government websites were under attack, as well as news portals.

---

[145] Ibid 69 and 73.

[146] E Tikk, K Kaska and L Vihul, International Cyber Incidents: Legal Considerations page 74.

The first question is whether any of these attacks could be considered cyber-attacks, or if they were just cyber operations. Did any of these 'attacks' cause physical damage? Tikk et al answers the question in the negative and writes "It can be assumed, given the low overall dependence of the Georgian population on online services and the nature of the websites attacked (online distribution of information to the public, which is normally not a life-sustaining service nor necessary to economic stability) that the effect of cyber attacks was not serious enough to amount to severe economic damage or significant human suffering".[147]

The question is now whether these cyber operations could legally target civilians. Under Article 48 the parties had to distinguish between civilian and military objectives, and only direct their operations against military objectives.

However, certain operations are allowed. Would the defacement of news websites count as propaganda that is allowed? In my view that has to be answered in the negative. It is one thing to email propaganda to civilians, but it must be distinguished from blocking news portals, and editing in new content. It is hard to imagine that the world community would find it acceptable that an enemy in an armed conflict could legally hack and insert propaganda onto online news outlets like CNN or the BBC because it is not an 'attack'.[148] Also none of these objects served as a military objective. They did not make an effective contribution to military action, neither did the disabling of them result in a military advantage.

---

[147] Ibid. Page 81.

[148] Kolb and Hyde use a similar argument when they discuss whether CNN and the BBC would have been a legitimate military objective if Serbia had the power to do so during the armed conflict between NATO and Serbia in 1999. They find that it would be highly unlikely. Kolb and Hyde, An introduction to the International Law of Armed Conflicts (2008) page 134.

The case of Iran (Stuxnet)

In 2010, a sophisticated computer virus named Stuxnet was discovered. The virus was designed to target the industrial control system of an Iranian nuclear fuel processing plant, and used stolen certificates to fool the system into thinking that the virus was a trusted program. The virus targeted the centrifuges and drastically increased and then decreased the frequency that they operated at, before turning it back to normal, damaging the centrifuges.

Stuxnet exploited vulnerabilities in the industrial control system that were still unknown to the software maker, so called 'zero-day' exploits, which allowed the virus to spread via infected USB sticks. Inside the Stuxnet's code a dossier detailing the specific technical configuration of the facility it sought. Any system that did not match precisely this configuration would go unharmed: Stuxnet would shut itself down and move on to the next system until it found its victim.[149] It still remains unknown who was behind the Stuxnet attacks,[150] although fingers have been pointed to the United States and Israel.[151] For the sake of argument, for the purpose of the following discussion, we will say that a State was indeed behind the Stuxnet attack.

Was the 'attack' a cyber-attack? The virus did cause harm to the nuclear reactor. The sudden increase and decrease of the frequencies damaged between 1000 to 2000 centrifuges. Further more, the amount of resources it would take to put the virus together, and how it was designed to take out the centrifuges show that there was a hostile intent behind the attack. On the other hand, this attack only affected one nuclear plant. In my

---

[149] Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History" ', Wired (07 November 2011) http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=Previous (accessed 27 October 2013).

[150] Tallinn Manual, Commentary to Rule 22, note 14 page 83.

[151] David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", New York Times (01 June2012)http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0 (accessed 27 October 2013).

view it definitely qualifies as a cyber-attack, but a lot would depend on how the government of Iran would classify it.[152]

The next question is if it is a military objective. Did the nuclear plant by its nature, location, purpose or use make an effective contribution to military action?[153] The plant's nature makes it possible for it to enrich uranium, which can be used for nuclear weapons. That makes it a military objective. We must then ask whether the attack would result in a military advantage. If the attack was designed to cripple Iran's ability to produce a nuclear weapon, then yes, the attack would gain a military advantage by sabotaging their centrifuges.

Did it distinguish between civilians and military targets though? Dinniss writes that "Interestingly, when the Stuxnet virus was discovered and reverse-engineered in 2010, researchers discovered that although the virus had been designed to propagate and spread fairly indiscriminately within a network, it had been coded to only execute its payload where specific conditions were fulfilled that would indicate it was on the targeted system"[154]. With this kind of programming in the virus, it does appear that it tried to distinguish between targets.

The nuclear plant is a dual use object, as it also provides electricity for civilians. We must therefore also determine whether the attack is proportionate. What would the civilian losses be? The civilians would lose electricity. How does that compare to the military advantage? The dangers of nuclear weapons far outweigh the inconveniences of losing power. Can a reasonable well-informed person expect excessive civilian casualties? Not in this case.

---

[152] The experts of the Tallinn Manual were divided as to whether the damage sufficed to meet the armed criterion. See Commentary to Rule 22 note 14 page 83.

[153] AP 1 Article 52(2).

[154] Heather Harrison Dinniss. Cyber Warfare and the Laws of War (2012) page 203 and 204.

Cyber-attacks are actually less likely to lead to civilian deaths, than a regular traditional kinetic bombing would be. By choosing cyber-attacks, the principle of proportionality seems to be followed, and the attackers seem to have taken the necessary precautions.

It therefore seems that Stuxnet had the possibility of amounting to an armed conflict which would trigger the IHL. Even if it did not, it seems that the rules were followed anyways. But as we have seen in all three cases, none of them were attributed to a State. In the next chapter, State attribution will be discussed.

6 State Attribution

For IHL to apply, there has to be a declared war, or an armed conflict between two or more states (international) or one state and an organised group (non-international).[155] A non-international conflict may turn into an international one if another State intervenes, or some of the participants in the conflict act on behalf of another State.[156]

Linking an attack to a state is usually not a problem when the attack is carried out by state organs, for example by its armed forces. However, cyber operations can prove more difficult to link to a state. A common cyber technique is 'spoofing'.[157] With this technique, the attacker can mask his own identification, but at the same time make it look like another state is behind the attack. Spoofing can lead to problems in classifying the conflict. If the State or States cannot be identified, then the situation will not be classified as an armed conflict. The attacking State will still in principle be bound to follow IHL, but it could prove problematic to ensure compliance with IHL if parties to an armed conflict can remain anonymous.

When non-state actors, such as individuals or groups act on behalf of another State, a question of attribution arises. The degree of control over these actors will determine whether State responsibility occurs, and whether an armed conflict will turn international. The following three cases from the ICJ and the ICTY illustrate the difficulty and different approaches with regard to attribution of State responsibility based on the 'control test'.

---

[155] This follows from the Geneva Conventions of 1949, common Article 2 and 3.

[156] Tadic Appeals Chambers 1999 para 84.

[157] According to the Tallinn Manual's glossary, spoofing is impersonating a legitimate resource or user to gain unauthorized entry into an information system or to make it appear that some other organization or individual has initiated or undertaken certain cyber activity.

The International Law Commission (ILC) has worked on codifying Articles on State responsibility. On December 12 2001, the Draft on State Responsibility was annexed to the UN General Assembly resolution 56/83[158], and the Assembly recommended it to all governments without prejudice to their future adoption or other appropriate action (para 3). The Draft Articles is not a Convention, but according to Crawford, "The Articles are an active and useful part of the process of international law. They are considered by courts and commentators to be in whole or in large part an accurate codification of the customary international law of State responsibility".[159] However, a few States are opposed to codifying the Articles. Their argument is that the Draft Articles have more impact through State practice, decisions of courts and tribunals and writings than they would have if they were codified. If codified, old issues may be reopened, and even if a text were to be agreed on, it is unlikely that it would enjoy the wide support currently accorded to the draft articles.[160] Because the Articles are an important part of the international law on State Responsibility, they will also be referred to in the following.

ICJ's Control test

In the *Nicaragua* case,[161] the ICJ dealt with the question of whether Nicaraguan rebels could be considered to be acting on behalf of the United States. The Court held that the financing, organising, training, supplying and equipping the rebels was not enough. In order for the US to be responsible, the rebels either had to be so completely dependent on them that they had to be considered state organs,[162] or the US had to have held 'effective control of the military or paramilitary operations in the course of which the alleged violations were committed'.[163]

---

[158] G.A. Res. 56/83 (Dec. 12, 2001).

[159] Crawford in 'State Responsibility The General Part' (2013) page 43.

[160] Ibid. Page 42 and 43.

[161] Military and Paramilitary Activities in and against Nicaragua,1986.

[162] Ibid. Para 109.

[163] Ibid. Para 115.

The rebels were not found to be in a relationship of such complete dependence on the US that they had to be considered their organs,[164] and since the United States had not 'directed or enforced' the rebels, they had not been in effective control of their operations, and were therefore not responsible.[165] Under ICJ's control test, for a State to incur responsibility it would have to exercise control over the non-state actors that launches the cyber-attacks. Such control would be considered to exist under ICJ's control test if the State would have effective control over the non-state actors.

6.1.1 ICTY's Control test

In *Tadic* (1999),[166] the ICTY looked at the legal conditions required for when individuals can be considered to act on behalf of a State. In doing this, the Court looked closer at the Nicaragua case, and compared its proposed test with state practice.

The *Tadic* case differed from the *Nicaragua* case because the *Nicaragua* case revolved around State responsibility, and not the individual criminal responsibility of the Nicaraguan rebels. However, the ICTY failed to see why this should matter. According to the ICTY logic dictates that the criteria for ascertaining responsibility is the same in the cases where the court wants to attribute the act of an individual to generate State responsibility, or whether the individuals are acting as *de facto* State officials, thereby rendering the conflict international and thus setting the necessary precondition for the "*grave breache*s" regime to apply.[167]

In both cases the issue is not the distinction between State responsibility and individual criminal responsibility, but rather whether a State can be held responsible for acts of individuals not having the status of State officials. In the one case, if the acts are

[164] Ibid. Para 110.

[165] Ibid. Para 116.

[166] Tadic Appeals Chambers 1999.

[167] Ibid. Para 104.

attributable to the State, the acts will give rise to international responsibility for that State, and in the other, these acts will require that the armed conflict be classified as an international armed conflict.[168]

Since there are no specific legal criteria in IHL for when individuals can be said to work on behalf of a State and making it an international armed conflict, reliance must be had on the criteria for State responsibility.[169] The Tribunal did not, however, however find the Nicaragua test of 'effective control' to be persuasive.[170] In its view, it did not hold up to the logic of State responsibility,[171] nor with judicial and State practice.[172]

First of all, the Tribunal did not find the test to be consonant with the logic of the law of State responsibility.[173] According to the principles of international law, if it is proved that individuals have acted on behalf of a State, then their acts are attributable to that State.[174] Otherwise States could escape international responsibility by engaging individuals to carry out tasks, and then point to them not being State organs. However, international law requires that the State exercises control over the concerned individuals. The degree of control necessary will vary depending on the circumstances of each case.[175]

---

[168] Ibid. Para 104.

[169] Ibid. Paras 98 and 105.

[170] Ibid. Para 115.

[171] Ibid. Para 116.

[172] Ibid Para 124.

[173] Ibid. Para 116.

[174] Ibid. Para 117. The Court brings up Article 8 of the Draft on State responsibility. The wording of Article 8 that the Court referred to in 1999 has later changed, but the essence has remained the same. Article 8 now reads: Conduct directed or controlled by a State: The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.

[175] Ibid.

The ICTY distinguishes between the control needed for individuals and organised groups. If an individual is engaged by a State to carry out illegal acts, it is necessary to show that the State has issued specific instructions, or publicly given retroactive approval. A generic authority over the individual would not be sufficient.[176]

Organised and hierarchically structured groups are different than individuals, because they have a structure, chain of command, set of rules and outward symbol of authority. The members of the group usually conform to the standards prevailing in the group, and will not act on their own. For the attribution to a State of acts of these groups, it is enough that the group is under the overall control of the State.[177]

If the controlling State is not the territorial State where the acts are performed, then more extensive and compelling evidence is required to show that the State is genuinely in control of the units or groups and not merely financing or equipping them, but also by generally directing or helping to plan their actions.[178] International rules do not require that such control should extend to the issuance of specific orders or instructions relating to single military actions, whether or not such actions were contrary to international humanitarian law.[179]

In the Tribunal's view, the 'dependency test' is part of the 'effective control'.[180] The difference between the 'effective control test' in the *Nicaragua* case and the 'overall control test' in the *Tadic* case is that no specific instructions are required in the latter. It follows from the ICTY's control test that attributing acts of hacktivists would require the

[176] Ibid. Para 118.

[177] Ibid. Para 120.

[178] Ibid. Para 138.

[179] Ibid. Para 145.

[180] Ibid. Para 112.

State to issue specific instructions or publicly give their approval retroactive. Attributing acts of an organized hacktivist group would just have to be under the overall control, and issuing specific instructions would not be necessary.

6.1.2 ICJ's position restored

In the *Genocide case,*[181] the ICJ discussed whether the acts of genocide carried out by Bosnian Serb armed forces in Srebrenica could be attributed to the Federal Republic of Yugoslavia (FRY). The Court applied the 'dependency test' from Nicaragua, but found that it had not been proven that the Bosnian Serb armed forces had such ties with FRY that they could be deemed to have been completely dependent on it.[182] It then applied the 'effective control' test from Nicaragua, but reached yet another negative conclusion because it had not been proven that the acts took place either on the instructions or under the control of organs of the FRY.[183]

According to the ICJ, the 'overall control' test may be applicable and suitable for determining whether or not an armed conflict is international, but did not elaborate on it because it was irrelevant for this case, and therefore left the question open.184 However they rejected the 'overall control' test when used to establish whether a state is responsible for acts performed by armed forces and paramilitary units that are not amongst its official organs. They did this on two grounds. First of all, the ICTY addressed an issue which was not indispensable for the exercise of its jurisdiction.185 It was not necessary to bring up state responsibility to decide criminal responsibility. Secondly, the 'overall control' test is unpersuasive for determining State responsibility. In their view, logic does not dictate that

---

[181] ICJ Case concerning application of the convention on the prevention and punishment of the crime of genocide (Bosnia and Herzegovina v. Serbia and Montenegro) , 26 Feb. 2007.

[182] Ibid. Paras 394 and 395.

[183] Ibid. Paras 413 and 415.

[184] Ibid. Para 404.

[185] Ibid. Para 403.

the same test should be used in both cases, as the degree and nature of a State's involvement in an armed conflict can differ from the degree and nature of involvement required to give rise to State responsibility.186 Also, the test broadens the scope of state responsibility beyond the fundamental principles governing the law of international responsibility.[187]

6.1.3 Towards a single control test for attribution of responsibility

Antonio Cassese was critical of how the ICJ rejected the 'overall control test' in the Genocide case. To prove the ICTY wrong, the Court should not have simply dismissed the test, but should have proved its alleged inconsistency with state practice and judicial precedent. But the ICJ did not engage in this discussion.[188] In Cassese's view, ICTY's test is better, and points to the example of terrorists. It would be nearly impossible to prove the issuance of instructions or directions relating to each terrorist operation due to their hidden nature. If one instead relies upon the 'overall control' test, it suffices to demonstrate that certain terrorist units or groups are not only armed or financed by a specific state or benefit from its strong support, but also that such state, generally speaking, organizes or coordinates or at any rate takes a hand in coordinating or planning its terrorist actions.[189]

Even though the ICJ did not find the overall control test persuasive for establishing State responsibility, they did leave the possibility open that it is suitable for determining whether or not an armed conflict is international.[190] That the ICJ rejected the ICTY's position on State responsibility does not mean that the ICTY's arguments and review on state practice are otherwise faulty. The Court specifically mentions that it "attaches the utmost

---

[186] Ibid. Para 405.

[187] Ibid. Para 406

[188] Cassese, The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia page (2007) 668.

[189] Ibid. Page 666.

[190] ICJ Genocide Case. Para 404.

importance to the factual and legal findings made by the ICTY in ruling on the criminal liability of the accused…[but] the situation is not the same for positions adopted by the ICTY on issues of general international law which do not lie within the specific purview of its jurisdiction and, moreover, the resolution of which is not always necessary for deciding the criminal cases before it".[191]

The 'overall control test' was developed because IHL otherwise lacks any unique criteria for establishing that an armed conflict is international when a group acts on behalf of a state. The 'overall control test' fills the gap that would otherwise be there, and the ICTYs argumentation is sound, and the Tribunal provides state practice and jurisprudence. The test has also been applied by the International Criminal Court (ICC). In its *Lubanga Judgement* of 2012,[192] the Court found that the 'overall control' test was the correct approach regarding the necessary degree of control that another State have to have over an armed group acting on its behalf.[193] The experts of the Tallinn Manual also agreed that the 'overall control' test is applicable when non-state actors are involved in the hostilities.[194] Therefore, it seems that the 'overall control' test will still be valid for determining whether or not an armed conflict is international.

6.1.4 Responsibility for acts of State organs

It follows from ILC Draft Article 4 on State responsibility that 'A State is responsible for the actions of its organs'.[195] Under Article 7, such responsibility applies even if the organ exceeded their authority, or contravened instructions.[196] This is only logical, as a State is made up by its organs.

---

[191] Ibid. Para 403.

[192] ICC: Prosecutor v. Lubanga, Trial Chamber judgment, 2012.

[193] Ibid. Para 541.

[194] Tallinn Manual, commentary to Rule 22 in note 2, page 79.

[195] Draft Articles on State Responsibility Article 4, annexed in UN Res A/56/83.

[196] Ibid. Article 7.

The interesting question is rather when non-state actors can be identified with a state. Sometimes, the act of individuals that lacks the status of State organs may still be attributed to the State under international law. For example, Draft Article 8 states that a person or groups conduct shall be considered an act of a State if they are in fact acting on the instructions of, or under the direction or control of the State carrying out the conduct.[197]

6.1.5 Hacktivists and groups that are not considered state organs

Hacktivists[198] are usually dealt with under criminal law, and generally are not sponsored by a State. But what happens if a State encourages a hacktivist?

Since a hacktivist would be an individual, it follows from the *Tadic* case that the State must issue specific instructions or publicly give retroactive approval.[199] A State that merely encourages individuals to attack would not suffice to identify the individuals with the State, thus bringing forth an international armed conflict.

Draft Article 11 holds that 'Conduct which is not attributable to a State under the preceding articles shall nevertheless be considered an act of that State under international law if and to the extent that the State acknowledges and adopts the conduct in question as its own'. The commentary to Draft Article 11 states that "as a general matter, conduct will not be attributable to a State under article 11 where a State merely acknowledges the factual existence of conduct or expresses its verbal approval of it".[200] Imagine a scenario where one State has bad relations with another, and consequently announces that people all over the world should launch cyber-attacks against the other State. In this case, the State has only encouraged cyber-attacks, and if individual hacktivists follow these, they will not be

---

[197] Draft Articles on State Responsibility Article 8, annexed in UN Res A/56/83.

[198] The Tallinn Manual's glossary defines a hacktivist as a person who gains or attempts to gain unauthorized access to hardware and/or software.

[199] Tadic Appeals Chambers 1999, para 118. It also follows from the Draft Articles on State Responsibility Article 8, which the ICJ deemed reflection of customary international law in the Genocide case, para 398.

[200] Commentaries to the draft articles on Responsibility of States for internationally wrongful acts page 53 in the YEARBOOK OF THE INTERNATIONAL LAW COMMISSION Volume II Part Two (2001).

identified with the State for the purpose of internationalizing an armed conflict, and the hacktivists will be dealt with under criminal law.

However, it follows that should people on the encouraging State's territory launch cyber-attacks, that State might breach their international obligation with knowingly allowing their territory to be used for acts contrary to the rights of other States.[201] This would still not transform the cyber-attacks into an international armed conflict, but the State would breach international obligations.

If the State, however, does more than encourage, it also provides lists of vulnerable targets, provides detailed instructions on how to attack the targets, then the hacktivists could be considered as acting under the specific instructions of the State. This is also the case even though the cyber-attacks in question were independently started by non-state actors, but the State approved of the cyber-attacks after the fact, and took steps to keep it up. Such steps could be providing lists of suitable targets, provide funding to continue the attacks, establish cyber mechanisms to defend the attacks and so on. By engaging in such cyber-attacks, hacktivists would become *de facto* agents of the endorsing State. The ICTY proved this when they referred to the ICJ Tehran Hostages case in *Tadic* 1999[202] to find the degree of control necessary, and how the Iranian students that stormed the embassy had not originally acted on behalf of Iran, but when later on, the Iranian authorities formally approved and endorsed the occupation, the militants became *de facto* agents of the Iranian State and their acts became internationally attributable to that State. Another alternative would be that a State hires hacktivists to attack their targets. If they were hired to conduct attacks, then it is clear that they were 'acting under instructions' under Draft Article 8.

---

[201] In ICJ *the Corfu Channel* Case (Merits), ICJ Reports 1949 on page 22 the Court held that every State has an obligation to not allow knowingly its territory to be used for acts contrary to the rights of other States.

[202] Tadic Appeals Chambers 1999 para 133 -137.

One should remember that cyber-attacks must cause some substantial harm for them to trigger the application of rules of IHL. Otherwise the attacks would most likely be dealt with under criminal law, while the encouraging State would probably be guilty of intervention in the internal affairs of the other State.

When it comes to groups, the requirement is no longer 'specific instructions', but 'overall control'. It follows from the *Tadic* case that only equipping and financing the group would not be enough,[203] so a State could finance and equip the group with hacking tools without being in 'overall control' of them. What is needed is that the State has sufficient control over the group to instruct them to mount cyber-attacks.[204]

There seems to be a significant difference in proving responsibility, depending on whether the attacks have been carried out by individuals, or by a group. In the *Tadic* (1995) case, the Tribunal laid out a test for determining the existence of an armed conflict: 'An armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State'.[205]

The *Tadic* judgment (1999) talked about 'overall control' over organised groups. Organised groups will normally have a structure, a chain of command and a set of rules as well as the outwards symbols of authority.[206] The hacktivists must be organised in order to be a group. The fact that many hackers are attacking a State individually would not make them organised. If they are working under a leadership structure and operating cooperatively,

[203] Ibid. Para 137.

[204] Tallinn Manual, commentary to Rule 22 note 4, page 80/81.

[205] Tadic 1995 para 70.

[206] Tadic Appeals Chambers 1999, para 120.

things might be different.[207] Whether the group is organised will have to be determined on a case by case basis.

The experts of the Tallinn Manual were divided on whether a group that is only organised online, can be said to be an organised group. Under Article 1(1) of AP 2 , applicable to non-international conflicts, there is a requirement that the group must be able 'to implement this protocol'. According to the experts, if this means that the organisation must be of a nature to allow implementation of the law of armed conflict, then a group that is organised purely online might be hard to classify as an organised group, because there would be no means to implement the law when the group has no physical contact.[208]

6.2 Conclusion

The requisite control needed for a State to be attributable to hacktivists will depend on whether they are organized or not. If the hacktivists are organized, 'overall control' will be enough for attributing the conduct to the State. Individual hacktivists, however, require specific instructions to attribute the acts to the State.

[207] Tallinn Manual , Commentary to Rule 23, note 13, page 89.

[208] Tallinn Manual, Commentary to Rule 23 note 14, page 89.

7 Concluding remarks

The threat of cyber-attacks is a real one, and it is important that States are aware of their responsibilities under IHL, and recognize that even though cyber-attacks might represent new means and methods of warfare, that there is an established framework of rules applicable to it. Cyber-attacks have the potential for less civilian casualties, but it also has the potential for mass destruction. It all depends on who designs and launch the attack. As more States implement and add cyber-attacks to their arsenals, State practice will emerge, leading to clearer rules. Hopefully States will respect the ban on targeting civilians even for cyber operations, but even if they do not, then clearer rules will probably emerge with State practice and treaties.

8 Bibliography

Books and book chapters

Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949, (Yves Sandoz, Christophe Swinarski & Bruno Zimmermann, eds., 1987).

Crawford, James . State Responsibility. 1st ed. Cambridge: 2013. Cambridge Books Online. Web. 17 November 2013. http://dx.doi.org/10.1017/CBO9781139033060.

Crawford, James, Brownlie's Principles Of Public International Law. 8th ed. Oxford University Press (2012).

E Tikk, K Kaska and L Vihul, International Cyber Incidents: Legal Considerations , Cooperative Cyber Defence Centre of Excellence, 2010.

Fleck, Dieter(ed), The Handbook of International Humanitarian Law (Oxford University Press, third edition 2013).

Harrison Dinniss, Heather. Cyber Warfare and the Laws of War. 1st ed. Cambridge: 2012. Cambridge Books Online. Web. 15 November 2013.Available at: http://dx.doi.org/10.1017/CBO9780511894527.

J-M Henckaerts and L Doswald-Beck, Customary International Humanitarian Law. Cambridge University Press. (2005) Referred to in thesis as ICRC Study on Customary International Humanitarian Law.
Available at
http://www.cicr.org/eng/assets/files/other/customary-international-humanitarian-law-i-icrc-eng.pdf.

Kolb, Robert and Hyde, Richard. An Introduction to the International Law of Armed Conflicts. Hart Publishing. 2008.

Pictet (ed.), Commentary to the First Geneva Convention for the Amelioration of the Condition of the Wounded and the Sick in Armed Forces in the Field (Translated from the original French) (ICRC 1952).

Ruys, Tom. 'Armed Attack' and Article 51 of the UN Charter, Evolutions in Customary Law and Practice. Cambridge University Press. 2010.

Articles

Cassese, Antonio (2007). The Nicaragua and Tadic Tests Revisited in Light of the ICJ Judgment on Genocide in Bosnia, in The European Journal of International Law Vol. 18 no. 4 EJIL .

Dinstein, Yoram.'The Principle of Distinction and Cyber War in International Armed Conflicts' Journal of Conflict & Security Law (Summer 2012) 17 (2): 261-277 doi:10.1093/jcsl/krs015.

Droege, Cordula (2012). Get off my cloud: cyber warfare, international humanitarian law, and the protection of civilians. International Review of the Red Cross, 94, pp 533-578 doi:10.1017/S1816383113000246.

Dörmann, Knut. Applicability of the Additional Protocols to Computer Network Attacks. International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law, Stockholm, 17-19.11.2004. Available at: http://www.icrc.org/eng/resources/documents/misc/68lg92.htm.

Melzer, Nils. Cyberwarfare and International Law.2011, UNIDIR Resources Paper, 2011, p.38, available at: http://www.unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf.

Schmitt, Michael N., Cyber Operations and the Jus in Bello: Key Issues (March 2, 2011). Naval War College International Law Studies, 2011.
Available at SSRN: http://ssrn.com/abstract=1801176.

Schmitt, Michael N., 'Attack' as a Term of Art in International Law: The Cyber Operations Context (September 7, 2012). PROCEEDINGS OF THE 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT 283-293 (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., 2012) Available at SSRN: http://ssrn.com/abstract=2184833.

M.N.Schmitt, D.H.A. Harrison & Th.C. Wingfield, Computers and War: The Legal Battlespace, International Humanitarian Law Research Institute, Background Paper 2004.

Schmitt, Michael. Classification of Cyber Conflict in the Journal of Conflict & Security Law (2012), Vol.17 No. 2, 245-260.

Reports and manuals

NATO GLOSSARY OF TERMS AND DEFINITIONS, AAP-06 Edition 2013. Available at: http://nsa.nato.int/nsa/zPublic/ap/aap6/aap-6.pdf.

US Department of Defense - U.S. Cyber Command Fact Sheet (2010): Available at: http://www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

US Army Field Manual 34-40-7 - Communications Jamming Handbook: Available at: http://www.enlisted.info/field-manuals/fm-34-40-7-communications-jamming-handbook.shtml.

Department of Defense Cyberspace Policy Report, A Report to Congress Pursuant to the National Defense Authorization Act for Fiscal Year 2011, Section 934, 2011. Available at: http://www.defense.gov/home/features/2011/0411_cyberstrategy/docs/NDAA%20Section%20934%20Report_For%20webpage.pdf.

The White House, The National Strategy to Secure Cyberspace, 2003, Available at https://www.uscert.gov/sites/default/files/publications/cyberspace_strategy.pdf.

Manual I Krigens Folkerett. Merkur-Trykk AS. 2013.

Schmitt, Michael N (Editor). Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge University Press. 2013.

(UK) Joint service manual of the law of armed conflict (2004 edition). Referred to in thesis as the UK Manual for the Law of Armed Conflict. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/27874/JSP3832004Edition.pdf.

ILA Committee on the Use of Force, Conference Report The Hague (2010), Available at http://www.ila-hq.org/en/committees/index.cfm/cid/1022.

YEARBOOK OF THE INTERNATIONAL LAW COMMISSION Volume II Part Two (2001) Available at: http://legal.un.org/ilc/publications/yearbooks/Ybkvolumes%28e%29/ILC_2001_v2_p2_e.pdf.

Internet resources

http://www.forbes.com/sites/williampentland/2011/06/12/china-creates-cyber-warfare-squad/ (Last accessed 06.11.13).

http://forsvaret.no/OMFORSVARET/ORGANISASJON/CYBERFORSVARET/Sider/cyberforsvaret.aspx (Last accessed 06.11.13).

https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit (Last accessed 06.11.13).

Kim Zetter, "How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History" ', Wired (07 November 2011)
http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1?utm_source=Contextly&utm_medium=RelatedLinks&utm_campaign=Previous
(accessed 27 October 2013).

David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran", New York Times
(01 June2012)http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0
(accessed 27 October 2013).

Treaties

Charter of the United Nations, Jun 26, 1945.

Convention on Cybercrime, Nov 23, 2001.

Geneva Convention (I), Aug 12, 1949 - for the Amelioration of the Conditions of the Wounded and Sick in Armed Forces in the Field.

Geneva Convention (II), Aug 12, 1949 – for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea.

Geneva Convention (III), Aug 12, 1949 – relative to the Treatment of Prisoners of War.

Geneva Convention (IV), Aug 12, 1949 – relative to the Protection of Civilian Persons in Time of War.

Protocol 1 on International Conflicts, Jun 8, 1977 - Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 1).

Protocol 2 on International Conflicts, Jun 8, 1977 - Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol 2).

Statute for the International Court of Justice (ICJ), Jun 26, 1945.

Vienna Convention on the Law of Treaties, May 23, 1969.

U.N. General Assembly Resolutions

G.A. Res. 53/70, (Dec. 4, 1998), U.N. Doc. A/RES/53/70 (Jan. 4, 1999).

G.A. Res. 55/63, (Dec. 4, 2000), U.N. Doc. A/RES/55/63 (Jan. 22, 2001).

G.A. Res. 56/83, (Dec. 12, 2001), U.N. Doc. A/Res/56/83, (Jan 28, 2002).

Case law

ICJ case law

Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America). Merits, Judgment. I.C.J. Reports 1986, p. 14.

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, I.C.J. Reports 1996, p. 226.

Application of the Convention on the Prevention and Punishment of the Crime of Genocide (Bosnia and Herzegovina v. Serbia and Montenegro), Judgment, I.C.J. Reports 2007, p. 43.

ICTY case law

International Criminal Tribunal for the Former Yugoslavia (ICTY), Prosecutor v. Tadic, Case No. IT-94-1-T, Appeals Chamber Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995.

International Criminal Tribunal for the Former Yugoslavia (ICTY), Prosecutor v. Tadic, Case No. IT-94-1-A, Appeals Chamber Judgment, 15 July 1999.

International Criminal Tribunal for the Former Yugoslavia (ICTY), Prosecutor v. Stanislav Galić, Case No. IT-98-29-T, Trial Chamber Judgment, 5 December 2003.

ICC case law

International Criminal Court, The Prosecutor v. Thomas Lubanga Dyilo, Case No ICC-01/04-01/06, Trial Chamber judgment, 10 July 2012.