



FACULTY OF LAW
Lund University

Amanda Bills

Cyber Warfare and *Jus in Bello* –
The Regulation of Cyber ‘Attacks’ under
International Humanitarian Law

LAGF03 Essay in Legal Science

Bachelor Thesis, Master of Laws programme
15 higher education credits

Supervisor: Matilda Arvidsson

Term: Spring Term 2017

Contents

Summary	3
Sammanfattning	4
Abbreviations	5
1 Introduction	6
1.1 Background	6
1.2 Purpose	7
1.3 Research Questions	7
1.4 Scope and Delimitations	8
1.5 Method	8
1.6 Perspective	8
1.7 Materials	8
1.8 Previous Research	9
1.9 Structure	9
2 Cyber Warfare	10
2.1 Terminology	10
2.2 The Characteristics of Cyber Warfare	11
3 International Humanitarian Law Applied to Cyber Warfare	13
3.1 Applicability of International Humanitarian Law	13
3.1.1 <i>The Scope of Application</i>	13
3.1.2 <i>Cyber Warfare: A 'Fifth' Domain of Warfare</i>	13
3.2 The Concept of a Cyber 'Attack'	15
3.2.1 <i>Attacks under the Additional Protocol I</i>	15
3.2.2 <i>Cyber Operations as 'Attacks'</i>	15
4 The Conduct of Hostilities in Cyber Warfare	17
4.1 Cyber 'Attacks': Applicable Principles	17
4.2 Cyber 'Operations': Interpretation of the Additional Protocol I	18
4.2.1 <i>The Permissive Approach</i>	18
4.2.2 <i>The Restrictive Approach</i>	20
5 Case Studies	22
5.1 Estonia (2007)	22
5.2 Georgia (2008)	22
5.3 Stuxnet (2010)	23
6 Analysis and Conclusion	24
6.1 Analysis	24
6.2 Conclusion	26
Bibliography	27

Summary

The aim of this paper is to examine how cyber operations that are undertaken in the context of international armed conflicts are regulated in international humanitarian law. It will focus on the qualification of cyber operations as 'attacks' and the applicability of the substantive rules that restrict the conduct of hostilities under the Additional Protocol I to the Geneva Conventions. In particular, this paper aims to examine to what extent cyber operations that do not amount to attacks are regulated by the rules of the Additional Protocol I, as well as the practical implications of their non-qualification as attacks.

The legal dogmatic method is applied to determine how the legal framework of international humanitarian law applies to cyber warfare. In its analysis, the paper will engage in a normative discussion to evaluate the legal framework from a developmental perspective. An international perspective is applied throughout to emphasise how the relevant rules function in the international relations of states.

This essay found that while international humanitarian law applies to cyber warfare, the concept of an attack should be narrowly interpreted to refer only to cyber operations that result in either death or injury to persons, or damage or destruction to objects. The implications of this consequence-based understanding of the notion of an attack is that most of the substantive provisions protecting civilians and their objects under the Additional Protocol I are not applicable to cyber operations.

The permissive approach, one that allows for a wider range of cyber operations to be directed against civilians, was found to be the most consistent with *de lege lata*. Large-scale but non-physical cyber operations may therefore intentionally – and lawfully – be directed against civilians, and may lead to an expansion of war's impact on civilians. These effects are likely to amplify as modern societies become increasingly reliant on cyber technologies for essential infrastructure such as oil and gas, transportation networks, electricity generating systems, water treatment facilities and emergency response services. The negative reality of the permissive approach represents a strong argument for the reinterpretation of the current legal framework in order to adapt to the special characteristics of cyber warfare.

Sammanfattning

Syftet med denna uppsats är att undersöka i vilken utsträckning cyberkrigsföring regleras av den internationella humanitära rätten. Särskild vikt läggs vid hur begreppet "attack" i Tilläggsprotokoll I till Genèvekonventionerna ska tolkas i förhållande till cyberoperationer (en. *cyber operations*) som sker inom ramen för internationella väpnade konflikter, och tillämpligheten av de materiella reglerna som begränsar krigförande parter handlanden. Uppsatsen syftar även till att undersöka de tänkbara konsekvenserna av en icke-kvalificering av cyberoperationer som attacker enligt Tilläggsprotokoll I.

Den rättsdogmatiska metoden tillämpas för att fastställa hur den internationella humanitära rätten bör tolkas och tillämpas ifråga om cyberkrigsföring. I analysen förs en normativ diskussion med ett utvecklingsperspektiv för att utvärdera gällande rätt. Uppsatsens perspektiv är genomgående internationellt och betonar i och med detta det rättsliga regelverkets tillämpning och funktion i staters internationella relationer.

Uppsatsen fann att begreppet "attack" ska tolkas inskränkande så att det endast omfattar cyberoperationer som resulterar i dödsfall eller skada på person, alternativt skada på eller förstörelse av egendom. Det är därmed endast vissa typer av cyberoperationer som omfattas av de materiella reglerna som skyddar civila och deras egendom. Detta synsätt tillåter att ett bredare spektrum av cyberoperationer får riktas mot civila (en. *the permissive approach*). Storskaliga men icke-fysiska cyberoperationer får därmed avsiktligt – och lagligen – riktas mot civila och deras egendom. Civila riskerar därför att i allt högre utsträckning påverkas av väpnade konflikter, en effekt som förstärks i takt med att det moderna informationssamhället expanderar och blir allt mer beroende av cyberteknologier för infrastrukturer som exempelvis olja och gas, energiförsörjning, transportnätverk, energiförsörjning, vattenreningsverk och krishanteringssystem. I slutsatsen diskuteras dessa aspekter som ett argument för en framtida omtolkning av den gällande internationella humanitära rätten.

Abbreviations

ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
IRRC	International Law Review of the Red Cross
NATO	North Atlantic Treaty Organization
UN	United Nations
UNGA	United Nations General Assembly

1 Introduction

‘The war is taking place on three fronts. The first is physical, the second is on the world of social networks, and the third is cyber’ – Carmela Avner, Israel’s chief information officer, 2012¹

1.1 Background

In 1982, the United States Intelligence Agency (CIA) planted a logic bomb in the computer control systems of a Soviet gas pipeline, allegedly causing a major explosion in Siberia.² Although the attack has never been confirmed, it is considered to be one of the earliest examples of an offensive cyber operation or cyber warfare.³ The expression ‘cyber warfare’ has since been proliferated by the media, with Forbes dubbing 2017 as ‘the year of cyber warfare’.⁴ As late as May 2017, massive cyber attacks struck multiple targets across several countries, including health services in Britain.⁵ The use of and reliance on networked information and communication technologies is one of the defining characteristics of the modern age.⁶ Computer systems are used extensively by states for essential infrastructure such as transportation, oil and gas, electricity, water treatment facilities, and emergency response services.⁷ The increasingly close links between computers and the physical world mean that cyber attacks are more likely to have real-world consequences.⁸ According to the United Nations General Assembly (UNGA), cyber technologies ‘can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security’.⁹

¹ Cowell, *The New York Times*, ‘Cyberwar and Social Media in the Gaza Conflict’ (2012), as cited in Roscini (2014), p. 4.

² Harrison-Dinniss (2012), p. 218.

³ Roscini (2014), p. 4.

⁴ Laudicina, *Forbes*, ‘2017 Will Be The Year Of Cyber Warfare’ (2016).

⁵ Wong and Solon, *The Guardian*, ‘Massive ransomware cyber-attack hits nearly 100 countries around the world’ (2017).

⁶ Harrison-Dinniss (2012), p. 11-13.

⁷ Woltag (2014), p. 17-18.

⁸ Harrison-Dinniss (2012), p. 11-13.

⁹ See Preambles of UNGA Res. A/RES/58/32 of 8 December 2003; A/RES/59/61 of 3 December 2004; A/RES/60/45 of 8 December 2005; A/RES/61/54 of 6 December 2006; A/RES/62/17 of 55December 2007; A/RES/63/37 of 2 December 2008; and A/RES/64/25 of 2 December 2009.

The use of cyber operations in armed conflict is becoming strategically as important as airpower in traditional conflicts, and is likely to increasingly supplement traditional warfare.¹⁰ On an international level, cyber activities are dealt with primarily in criminal law, for example in the Council of Europe's 2001 Convention on Cybercrime¹¹ and in the European Union's 2013 Directive on attacks against information systems.¹² In cyber warfare, there is no specific regulation to govern the conduct of cyber operations, and consequently no consistent terminology.¹³ This has created uncertainty as to how international humanitarian law – the laws of war (*jus in bello*) – applies to cyber warfare.

1.2 Purpose

The aim of this paper is to examine how cyber operations that are undertaken in the context of international armed conflicts are regulated in international humanitarian law. It will focus on the qualification of cyber operations as 'attacks' under the Additional Protocol I to the Geneva Conventions and the applicability of the substantive rules that restrict the conduct of hostilities. The analysis will evaluate the current legal framework and discuss the potential implications of the non-qualification of cyber operations as attacks.

1.3 Research Questions

- What is a cyber 'attack' under international humanitarian law?
- What are some examples of cyber attacks, and how can they be analysed under the existing legal framework of international humanitarian law?
- What are the practical implications of the non-qualification of a cyber operation as an 'attack' under international humanitarian law?

¹⁰ See Geiß and Lahmann (2012), *Israel Law Review*, 45(3), pp. 381-399, at p. 384; and Schmitt (2014), *IRRC*, Vol. 96, No. 893, pp. 189-206, at p. 190.

¹¹ Council of Europe, *Council of Europe Convention on Cybercrime*, European Treaty Series (ETS), No. 185, 23 November 2001 (accessed 18 May 2017).

¹² Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] L 218/8.

¹³ Solis (2016), p. 673-674.

1.4 Scope and Delimitations

This paper is limited to the *jus in bello* of cyber warfare, and will not discuss the *jus ad bellum* (right to war) or the activities of individuals (e.g. 'hacker' groups). The technical aspects of cyber warfare will be dealt with as is necessary for the research questions of this paper. This paper focuses on the qualification of cyber operations as attacks in the context of international armed conflicts, and excludes topics such as attribution and conflict classification.

1.5 Method

This paper uses the legal dogmatic method, and as such relies on an analysis of the established sources of international law to respond to the research questions.¹⁴ The uncertainties of the applicability of international humanitarian law to cyber warfare motivate the choice of the legal dogmatic method, in order to determine *de lege lata* (the law as it is) in relation to cyber warfare. This paper will also engage in a normative discussion *de lege feranda* (the law as it ought to be).

1.6 Perspective

The perspective of this paper is international, i.e. focuses on how the rules and principles of international law function in the relations between states. Consistent with the normative discussions of the legal dogmatic method, some issues will be explored from a developmental perspective.

1.7. Materials

The starting-point of this paper is the recognised sources of international law. These include treaties, customary law, general principles of law, judicial decisions and legal doctrine.¹⁵ The treaties that govern warfare include the Geneva Conventions I-IV¹⁶

¹⁴ See Korling and Zamboni (ed.) (2013), p. 21.

¹⁵ Art. 38(1), Statute of the International Court of Justice (ICJ).

¹⁶ Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field (12 August 1949) (I); Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of Armed Forces at Sea (12 August 1949) (II); Geneva Convention Relative to the Treatment of Prisoners of War (12 August 1949) (III); and Geneva Convention Relative to the Protection of Civilian Persons in Time of War (12 August 1949) (IV) [cit. Geneva Conventions].

and the Additional Protocols I-II to the Geneva Conventions.¹⁷ As cyber warfare is not subject to any specific regulation, soft law instruments and secondary sources will be used extensively. It should be noted that there is no case law from the International Court of Justice (ICJ) interpreting the relevant terms and provisions.

1.8 Previous Research

There is little research on how the principles of international humanitarian law apply to cyber operations that do not meet the threshold of an attack. Previous research on the other aspects of the jus in bello of cyber warfare is extensive. A leading author on the subject is Michael Schmitt, whose most notable contributions include the *Tallinn Manual on the International Law Applicable to Cyber Warfare*¹⁸ and the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*.¹⁹

1.9 Structure

Chapter 2 – *Cyber Warfare* defines the main concepts and distinct features of cyber warfare. Chapter 3 – *International Humanitarian Law Applied to Cyber Warfare* studies the applicability of international humanitarian law to cyber warfare and discusses the concept of a cyber attack under international humanitarian law. Chapter 4 – *The Conduct of Hostilities in Cyber Warfare* examines the principles applicable to cyber attacks and evaluates the permissive and restrictive approaches in relation to cyber operations that do not meet the threshold of an attack. Chapter 5 – *Case studies*, examines three well-known instances of cyber attacks. The final Chapter 6 – *Analysis and Conclusion* will discuss, evaluate and analyse the current legal framework of international humanitarian law in relation to cyber warfare.

¹⁷ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) (8 June 1977) [cit. Additional Protocol I]; Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts (Protocol II) (8 June 1977). The Geneva Conventions deal with the general protection of civilian populations against certain consequences of war, and the Additional Protocols specifically address the conduct of hostilities; see ICRC 'The Geneva Conventions of 1949 and their Additional Protocols', (2010).

¹⁸ Schmitt (2013) [cit. *Tallinn Manual*].

¹⁹ Schmitt and Vihul (ed.) (2017) [cit. *Tallinn Manual 2.0*]. The two Tallinn Manuals are academic, non-binding studies on how international law applies to cyber conflicts. The NATO Cooperative Cyber Defence Centre of Excellence facilitated and led the drafting of the Tallinn Manual 2.0.

2 Cyber Warfare

2.1 Terminology

The term cyber warfare is understood to refer to the military use of cyber capabilities in the context of an armed conflict, either in conjunction with conventional hostilities or as stand-alone activities.²⁰ The term includes both the *means* of warfare (cyber weapons or systems) and *methods* of warfare (cyber tactics, techniques or procedures).²¹ Cyber warfare denotes the involvement of state actors, while other activities such as cyber *crime* or *terrorism* refer to the criminal or terrorist activities of individuals through the use of cyberspace.²²

Cyber attacks are a specific category of cyber operations, and may be defined as ‘cyber operation[s], whether offensive or defensive, that [are] reasonably expected to cause injury or death to persons or damage or destruction to objects’.²³ The technical difference between cyber *attacks* and cyber *operations* is that attacks have hostile intent and are destructive in nature, while operations are non-destructive and typically involve activities such as intelligence gathering, surveillance, or other cyber exploitation or intrusion.²⁴ Cyber attacks may therefore include acquiring control over computer systems, transmitting viruses to destroy or alter data, planting logic bombs, inserting worms to overload networks or sniffers to monitor or seize data.²⁵ The common denominator of all cyber attacks is the use of computer code to disrupt, deny, degrade, manipulate or destroy adversary computer systems or data.²⁶

This paper uses the term ‘cyber attack’ to refer to offensive cyber operations that are undertaken in the context of an armed conflict and that qualify as attacks under the Additional Protocol I. The term ‘cyber operations’ is used broadly to describe cyber activities and other cyber acts that do not meet the threshold of an attack.²⁷

²⁰ Melzer (2011), p. 4-5.

²¹ Tallinn Manual 2.0, Rule 103, p. 452.

²² Clough (2015), p. 9-11, 12-15.

²³ Tallinn Manual 2.0, Rule 92, p. 415.

²⁴ Roscini (2014), p. 181-182.

²⁵ Schmitt (2002), IRRC, Vol. 84, No. 846, pp. 365-399, at p. 367.

²⁶ Ibid; Harrison Dinniss (2012), p. 4-5.

²⁷ See Tallinn Manual 2.0, Rule 80, para. 4, p. 376.

2.2 The Characteristics of Cyber Warfare

Cyberspace consists of a global network of decentralized yet interconnected networks of digital information and communications infrastructures, and is not subject to the regulation of a central body or embedded in an international legal regime.²⁸ It has been described as a non-legal domain, and differentiated from physical spaces by its a-territorial, borderless and ubiquitous character.²⁹ The high interconnectivity of cyberspace means that operations can instantaneously create effects that reach far beyond their points of origin, thereby defying traditional geographical boundaries.³⁰ As cyberspace is comprised of both physical and virtual components, with physical infrastructure located within a state, it is not immune to territoriality.³¹ Physical objects, for example computers or routers, connect the virtual domain of cyberspace to the physical world.³² Cyberspace operations can therefore be territorialized based on the locality of people, infrastructure, and, most notably, their effects.³³ The UN has established the applicability of legal concepts to cyberspace with respect to the UN Charter and the principles that flow from state sovereignty.³⁴

A significant feature of cyber warfare is the potential effects that cyber operations may have on the civilian population. The prevalence of civilian infrastructure that is used for both civilian and military purposes has transformed much of it into valid, dual-use military objectives.³⁵ The legitimacy of targeting such objects is controversial, as certain cyber infrastructures may be essential to a nation's well being but are also used for military purposes.³⁶ The interconnected nature cyber infrastructure means that attacks on such infrastructures are likelier to result in

²⁸ Melzer (2011), p. 4-5; see Woltag (2014), p. 79-81.

²⁹ Tsagourias, 'The legal status of cyberspace', in Tsagourias and Buchan (2015), p. 13-14.

³⁰ Mason, 'Geography, Territory and Sovereignty in Cyber Warfare', in Nasu and McLaughlin (2014), p. 76-77; see also Woltag (2014); and 31-33. Melzer (2011), p. 4-5.

³¹ Roscini (2014), p. 24.

³² Tsagourias, 'The legal status of cyberspace', in Tsagourias and Buchan (2015), p. 15.

³³ Mason, 'Geography, Territory and Sovereignty in Cyber Warfare', in Nasu and McLaughlin (2014), p. 77-78.

³⁴ UNGA, 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013), UN Doc. A/68/98, paras. 19-20 [cit. UNGA A/68/98].

³⁵ Solis (2016), p. 688.

³⁶ *Ibid.*, p. 679.

collateral damage and incidental injury to civilians, blurring the lines between the civilian population and the military.³⁷

³⁷ Schmitt (2005), p. 53-55; and Harrison-Dinniss (2012), p. 25-27.

3 International Humanitarian Law Applied to Cyber Warfare

3.1 Applicability of International Humanitarian Law

3.1.1 *The Scope of Application*

International humanitarian law applies when two or more states wage hostilities against each other, irrespective of the intensity or the length of the fighting, and irrespective of the initial resort to force.³⁸ The requirement is the factual existence of an armed conflict.³⁹ International humanitarian law seeks to restrict the means and methods of warfare by balancing military necessity with humanitarian concerns.⁴⁰ The legal framework consists mainly of treaty law, in particular the Geneva Conventions I-IV and the Additional Protocols I-III to the Geneva Conventions.⁴¹ The Geneva Conventions reflect customary law in their entirety.⁴² The status of the Additional Protocols is more controversial, as these do not have the same level of recognition.⁴³

3.1.2 *Cyber Warfare: A 'Fifth' Domain of Warfare*

The special characteristics of cyberspace have led it to be described as a 'fifth' domain of warfare, alongside land, sea, air and outer space.⁴⁴ The general applicability of international humanitarian law has therefore come into question. In the *Nuclear weapons* case the ICJ held that international humanitarian law applies to all forms of warfare, regardless of the weapons employed.⁴⁵ Cyber operations that occur in the context of an armed conflict are therefore subject to humanitarian law.⁴⁶ Where cyber operations accompany conventional conflict, the latter will be analysed

³⁸ Dinstein (2016), p. 1; and Turns, 'The Law of Armed Conflict (International Humanitarian Law)', in Evans (2014), p. 824-835.

³⁹ Common Art. 3, Geneva Conventions.

⁴⁰ Shaw (2014), p. 850-859.

⁴¹ Turns, 'The Law of Armed Conflict (International Humanitarian Law)', in Evans (2014), p. 821.

⁴² Ibid, p. 824-831.

⁴³ Shaw (2014), p. 847.

⁴⁴ Melzer (2011), p. 3.

⁴⁵ *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, ICJ Reports 1996, p. 226, para. 39 [cit. *Legality of the Threat or Use of Nuclear Weapons*].

⁴⁶ Tallinn Manual 2.0, Rule 80, p. 375.

to determine the applicability of humanitarian law.⁴⁷ Cyber operations may also be launched on their own and without the use of physical force. The requirement of an ‘armed conflict’ should be understood as shorthand for activities of a particular nature and intensity.⁴⁸ Stand-alone cyber operations may by themselves constitute an armed conflict if they are more than sporadic or isolated, and are intended to cause injury or death to persons, or damage or destruction to objects, or that such consequences are foreseeable.⁴⁹ However, this scenario has been described as unlikely, as cyber operations do not ensure the long-term effective damage as conventional operations. Cyber operations are therefore more likely to be used in conjunction to conventional warfare.⁵⁰ The applicability of international humanitarian law to cyber warfare has been established by the UN,⁵¹ and asserted by a number of states.⁵²

The absence of cyber-specific provisions in international humanitarian law does not mean that cyber warfare is unregulated. The Martens Clause⁵³ rejects the assumption that anything which is not explicitly prohibited by the relevant treaties is therefore permitted, ensuring the applicability of existing norms to new situations or technologies.⁵⁴ In the Nuclear Weapons case, the ICJ rejected that because IHL ‘principles and rules had evolved prior to the invention of nuclear weapons’ humanitarian law was inapplicable to them, and that ‘there can be no doubt as to the applicability of humanitarian law to nuclear weapons’.⁵⁵ The same reasoning should apply to cyber warfare.⁵⁶ There is also a legal requirement to review new weapons for their compliance with international humanitarian law.⁵⁷

⁴⁷ Woltag (2014), p. 199.

⁴⁸ Schmitt (2002), IRRC, Vol. 84, No. 846, pp. 365-399, at p. 372-374.

⁴⁹ Ibid, at p. 370-375.

⁵⁰ Gill, ‘International humanitarian law applied to cyber warfare: Precautions, proportionality and the notion of “attack” under the humanitarian law of armed conflict’, in Tsagourias and Buchan (2015), p. 367-371.

⁵¹ UNGA A/68/98, paras. 19 and 43; and UNGA ‘Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security (22 July 2015), UN Doc. A/70/174, para. 28.

⁵² ICRC (2015), p. 39.

⁵³ Art. 1(2), Additional Protocol I. The Clause first appeared in the Preambles to the Hague Conventions of 1899 and 1907 respecting the Laws and Customs of War on Land.

⁵⁴ Pilloud *et al.* (1987), para. 55, p. 38-39.

⁵⁵ *Legality of the Threat or Use of Nuclear Weapons*, para. 85.

⁵⁶ Schmitt (2002), IRRC, Vol. 84, No. 846, pp. 365-399, at p. 370.

⁵⁷ Art. 36, Additional Protocol I.

3.2 The Concept of a Cyber ‘Attack’

3.2.1 Attacks under the Additional Protocol I

Attacks are defined in Article 49(1) of the Additional Protocol I as ‘acts of *violence* against the adversary, whether in offense or in defence’.⁵⁸ The Commentary adds that attacks must involve ‘combat action’, as this is the likeliest way in which civilians will be affected by armed conflict.⁵⁹ There is an ‘act of violence’ (i.e. an attack) if the act results in death or injury to persons, or damage or destruction to objects.⁶⁰ This definition includes acts that are non-violent but have violent consequences, such as biological or chemical weapons.⁶¹ Passing inconvenience or interference does not make an act violent.⁶² This definition excludes non-physical, psychological, political or economic warfare.⁶³

The concept of an attack is different to an ‘armed attack’ under Article 2(4) of the UN Charter⁶⁴, which refers to the use of force *jus ad bellum*.⁶⁵

3.2.2 Cyber Operations as ‘Attacks’

A cyber attack is ‘a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects’.⁶⁶ The decisive factor is not the nature of the attack itself, but its physical effects.⁶⁷ Fatalities or large-scale property destruction would, as with conventional weapons, qualify a cyber operation as an attack under humanitarian law.⁶⁸ A cyber operation that targets an electricity facility and deprives power to a hospital, thereby resulting in the deaths of patients, is an attack under this definition.⁶⁹ The effects of damaging or destructive cyber operations are understood in the same way as

⁵⁸ Art. 49(1), Additional Protocol I (emphasis added).

⁵⁹ Pilloud *et al.* (1987), para. 1880, p. 603.

⁶⁰ Dinstein (2016), p. 2-3.

⁶¹ Schmitt (2002), IRR, Vol. 84, No. 846, pp. 365-399, at p. 375-376.

⁶² Dinstein (2016), p. 2-3.

⁶³ Bothe *et al.* (1982), p. 289.

⁶⁴ Art. 2(4), Charter of the United Nations.

⁶⁵ Pilloud *et al.* (1987), para. 1882, p. 603; see Solis (2016), p. 680, 682-683.

⁶⁶ Tallinn Manual 2.0, Rule 92, p. 415.

⁶⁷ Solis (2016), p. 679-681; see HPCR *Manual on International Law Applicable to Air and Missile Warfare* (2013), Rule 21, p. xxx.

⁶⁸ Solis (2016), p. 679-681.

⁶⁹ Boothby, ‘Where Do Cyber Hostilities Fit in the International Law Maze?’, in Nasu and McLaughlin (2014), p. 60-62.

conventional attacks by an equation of the physical effects of an operation.⁷⁰ Under this definition, cyber attacks might include, for example, cyber operations that that manipulate the control systems of a water dam, causing massive downstream destruction and potential death or injury to persons.⁷¹ Operations that merely break through firewalls or plant malware in enemy computers cannot be defined as attacks unless they result in the required damaging effects.⁷² Likewise, cyber operations that target data are excluded from the concept of an attack, as data is not considered an object in the sense of the Additional Protocol I.⁷³

Cyber operations that interfere with the functionality of an object may qualify as attacks, if the restoration of functionality requires the replacement of physical components or reinstallation of the operating systems or of particular data. The Tallinn Manual drafters developed this test of functionality.⁷⁴ The need to replace components serves as an indicator that damage has occurred, a situation that might be compared to the physical bombing of the same target.⁷⁵ The same reasoning applies with respect to data, and that a cyber operation that destroys even a small amount of data crucial to the operation of the computer system will be considered an attack.⁷⁶

⁷⁰ Tallinn Manual 2.0, Rule 92, paras. 1-5, p. 415.

⁷¹ Tallinn Manual 2.0, Rule 92, para. 5, p. 415.

⁷² Dinstein (2016), p. 3.

⁷³ Schmitt (2014), IRRC, Vol. 96, No. 893, pp. 189-206, at p. 200-201; see Art. 52(2), Additional Protocol I for the use of the term 'object', and Art. 31(3), the Vienna Convention on the Law of Treaties for the obligation to interpret treaties in good faith.

⁷⁴ Tallinn Manual 2.0, Rule 92, para. 10-11, p. 415.

⁷⁵ Boothby, 'Where Do Cyber Hostilities Fit in the International Law Maze?', in Nasu and McLaughlin (2014), p. 60-62.

⁷⁶ *Ibid.*

4 The Conduct of Hostilities in Cyber Warfare

4.1 Cyber ‘Attacks’: Applicable Principles

Cyber operations can be designed to result in a wide range of outcomes, and might not necessarily have physical consequences.⁷⁷ The main effects of cyber operations are almost always secondary to the attack itself, which allows room to question whether an attack has occurred and if there is a causal relationship between the attack and its presumed effects.⁷⁸ The ambiguous nature of cyber operations has led to debate surrounding the scope of the concept of an attack, as most of the law regulating the conduct of hostilities is framed in terms of attacks rather than operations.⁷⁹ The qualification of an act as an attack activates the restrictions placed on attacks under the Additional Protocol I.⁸⁰ Cyber operations that are attacks under the Additional Protocol I are governed by the same rules as kinetic attacks.⁸¹ The relevant legal rules include the principle of distinction⁸², the prohibition on attacking civilians⁸³ and civilian objects⁸⁴, the prohibition of indiscriminatory attacks,⁸⁵ the principle of proportionality,⁸⁶ the obligation to take precautions in the conduct of all military operations⁸⁷ and attacks,⁸⁸ and the obligation to take precautions against the effects of attacks.⁸⁹

There is disagreement in legal doctrine between those who favour a broad interpretation of the Additional Protocol I, that civilians should be protected from any activity whatsoever in conjunction with hostilities, and those who regard civilian

⁷⁷ Harrison-Dinniss (2012), p. 196.

⁷⁸ *Ibid.*, p. 117-138; see also Solis (2016), p. 679; and Turns, ‘Cyber War and the Concept of “Attack” in International Humanitarian Law’, in Saxon (2013), p. 212-213.

⁷⁹ Schmitt (2014), IRRC, Vol. 96, No. 893, pp. 189-206, at p. 191; Harrison-Dinniss (2012), p. 197.

⁸⁰ Turns, ‘Cyber War and the Concept of “Attack” in International Humanitarian Law’, in Saxon (2013), p. 215-217. See *supra* note 17.

⁸¹ Dinstein (2012), *Journal of Conflict and Security Law*, 17(2), pp. 216-277, at p. 261-265.

⁸² Art. 48, Additional Protocol I; Tallinn Manual 2.0, Rule 93, p. 420.

⁸³ Art. 51(2), Additional Protocol I; Tallinn Manual 2.0, Rule 94, p. 422.

⁸⁴ Art. 51(1), Additional Protocol I; Tallinn Manual 2.0, Rule 99, p. 434.

⁸⁵ Art. 51(4), Additional Protocol I; Tallinn Manual 2.0, Rule 105, p. 455, and Rule 111, p. 467.

⁸⁶ Art. 51(5)(b), Additional Protocol I; Tallinn Manual 2.0, Rule 113, p. 470.

⁸⁷ Art. 57(1), Additional Protocol I; Tallinn Manual 2.0, Rule 114, p. 476.

⁸⁸ Art. 57(2), Additional Protocol I; Tallinn Manual 2.0, Rules 114-120, p. 476-484.

⁸⁹ Art. 58, Additional Protocol I; Tallinn Manual 2.0, Rule 121, p. 487.

protection as confined to acts of violence (i.e. attacks).⁹⁰ The two positions represent a *restrictive* approach (restricting the use of cyber operations as a matter of law), and a *permissive* approach (allowing a wider range of cyber operations), respectively.⁹¹

4.2 Cyber ‘Operations’: Interpretation of the Additional Protocol I

4.2.1 The Permissive Approach

The principle of distinction in Article 48 of the Additional Protocol I requires parties to a conflict to at all times distinguish between civilians and combatants, and to only direct their operations against military objects.⁹² The principle is built upon the 1868 St Petersburg Declaration, which states that ‘the only legitimate object which States should endeavour to accomplish during war is to weaken the military forces of the enemy’.⁹³ It is recognised as one of the cardinal principles of customary international law, as famously declared by the ICJ in the Nuclear weapons case.⁹⁴ The reference to military operations is understood to refer to ‘all movements and acts related to hostilities that are undertaken by the armed forces’.⁹⁵ The ICRC interprets the concept in the context of the whole section as referring to ‘military operations during which violence is used, and not to ideological, political or religious campaigns’.⁹⁶ Although the article contains a broad reference to military operations, state practice demonstrates that it should be interpreted to refer to *attacks*.⁹⁷ The ICRC adopts this position in its Study on Customary International Humanitarian Law, i.e. that it is only attacks in the sense of the Additional Protocol I that are subject to the principle of distinction.⁹⁸

The principle of distinction is reflected in the rules protecting civilians and their objects.⁹⁹ Under Article 51 of the Additional Protocol I, civilians are granted ‘general

⁹⁰ Dinstein (2016), p. 143.

⁹¹ Schmitt (2014), IRRC, Vol. 96, No. 893, pp. 189-206, at p. 191.

⁹² Shaw (2014), p. 859-860; Pilloud *et al.* (1987), para. 1871, p. 599-600.

⁹³ Preamble to the 1868 Saint Petersburg Declaration.

⁹⁴ *Legality of the Threat or Use of Nuclear Weapons*, para. 78.

⁹⁵ Pilloud *et al.* (1987), para. 1875, p. 600.

⁹⁶ *Ibid.*

⁹⁷ Schmitt (2014), IRRC, Vol. 96, No. 893, pp. 189-206, at p. 193.

⁹⁸ Henckaerts and Doswald-Beck (2005), p. 3.

⁹⁹ See Tallinn Manual 2.0, Rule 93, para. 4, p. 420.

protection against dangers arising from *military operations*,¹⁰⁰ and ‘shall not be the object of *attack*’.¹⁰¹ Its subparagraphs are all aimed at attacks and not operations, for example the prohibition on indiscriminate *attacks*,¹⁰² that *attacks* must comply with proportionality,¹⁰³ and that reprisal *attacks* are unlawful.¹⁰⁴ The Commentary clarifies that an attack refers to the definition of Article 49(1) of the Additional Protocol I.¹⁰⁵ A contextual approach suggests that the essence of these provisions is a prohibition on *attacking* civilians and their objects, and not on targeting them.¹⁰⁶ Civilians therefore enjoy protection from cyber *attacks*, but not *operations*.¹⁰⁷

The requirement of Article 57(1) of the Additional Protocol I to take ‘constant care’ to ‘spare the civilian population, civilians, and civilian objects’ relates to the conduct of military operations.¹⁰⁸ The term military operation refers to any movements, manoeuvres and other activities carried out by the armed forces.¹⁰⁹ The provision requires parties to a conflict to be continuously sensitive to the effects of their activities on the civilian population and civilian objects, and seek to avoid any unnecessary effects thereon, an example of which is to have the assistance of technical experts to determine whether appropriate precautionary measures have been taken.¹¹⁰ The ICRC Commentary views the requirement as a supplement to the principle of distinction to encompass a general duty to respect the civilian population.¹¹¹ The Tallinn Manual interprets the obligation to be applicable to all forms of hostilities, and that it therefore covers both cyber operations and cyber attacks.¹¹² Using the permissive approach the obligation may also be seen as another set of requirements on attacks, as specified in its subparagraphs 57(2)-(5).¹¹³ It should be noted that Article 58 of the Additional Protocol I is understood to

¹⁰⁰ Art. 51(1), Additional Protocol I (emphasis added).

¹⁰¹ Art. 51(2), Additional Protocol I (emphasis added).

¹⁰² Art. 51(4), Additional Protocol I.

¹⁰³ Art. 51(5)(b), Additional Protocol I.

¹⁰⁴ Art. 51(6), Additional Protocol I.

¹⁰⁵ Pilloud *et al.* (1987), para. 1939, p. 618; para. 1923, p. 615.

¹⁰⁶ Schmitt (2014), IRRIC, Vol. 96, No. 893, pp. 189-206, at p. 193.

¹⁰⁷ Roscini (2014), p. 178.

¹⁰⁸ See Shaw (2014), p. 859-860.

¹⁰⁹ Pilloud *et al.* (1987), para. 2191, p. 680.

¹¹⁰ Tallinn Manual 2.0, Rule 114, para. 5-6, p. 476.

¹¹¹ Pilloud *et al.* (1987), para. 2191, p. 680.

¹¹² Tallinn Manual 2.0, Rule 114, paras. 1-2, p. 476; Roscini (2014), p. 178, 223.

¹¹³ Schmitt (2014), IRRIC, Vol. 96, No. 893, pp. 189-206, at p. 192-193.

refer solely to attacks, as indicated by its title and that there is no customary international law to support that Article 58 also covers operations.¹¹⁴

4.2.2 The Restrictive Approach

The permissive approach has been criticized on the basis of the Commentary and from a humanitarian perspective. In its final sentence, the Commentary to Article 48 of the Additional Protocol I defines military operations as ‘all movements and acts related to hostilities that are undertaken by armed forces’.¹¹⁵ The Commentary to Article 51 further defines the term as encompassing all military operations related to hostilities.¹¹⁶ This view is also echoed in the Commentary to Article 57 which defines military operations as ‘any movement, manoeuvres and other activities whatsoever carried out by the armed forces with a view to combat’.¹¹⁷ The restrictive approach implies that the principles also extend to non-violent operations that are undertaken as part of the hostilities.¹¹⁸ This argument may, however, be rejected with reference to the opening sentence of the Commentary to Article 48, which notes that the section applies to operations during which violence is used, in other words, only to attacks.¹¹⁹ The same reasoning is incorporated into the Commentary to Article 51 through a footnote¹²⁰, and the Commentary to Article 57 uses the term ‘combat’.¹²¹

Another argument of the restrictive approach focuses on the definition of military objectives in Article 52(2) of Additional Protocol I. The provision restricts attacks to military objectives, which are defined as ‘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* [...] offers a definite military advantage’.¹²² Neutralizing an object refers to attacking it for the purpose of denying the adversary the use of the object, without necessarily destroying it.¹²³ It has been argued that the reference to neutralization implies that it is irrelevant *how* an object is

¹¹⁴ Tallinn Manual 2.0, Rule 121, para. 5, p. 487; Pilloud *et al.* (1987), paras. 2257-2258, p. 694-695.

¹¹⁵ Pilloud *et al.* (1987), para. 1875, p. 600.

¹¹⁶ *Ibid.*, para. 1936, note 27, p. 618.

¹¹⁷ *Ibid.*, para. 2191, p. 680.

¹¹⁸ Harrison-Dinniss (2012), p. 199-201.

¹¹⁹ Pilloud *et al.* (1987), para. 1863, p. 598; Schmitt (2014), IRRRC, Vol. 96, No. 893, pp. 189-206, at p. 195.

¹²⁰ Pilloud *et al.* (1987), para. 1936, note 8, p. 618.

¹²¹ *Ibid.*, para. 2191, p. 680; see also Schmitt (2014), IRRRC, Vol. 96, No. 893, pp. 189-206, at p. 195

¹²² Art. 52(2), Additional Protocol I (emphasis added).

¹²³ Droege (2012), IRRRC, Vol. 94, No. 886, pp. 533-578, at p. 558.

disabled, and that the provision must apply to both kinetic and non-kinetic means.¹²⁴ This analysis means that physical consequences are not required for the applicability of the restrictions placed on the conduct of hostilities, thereby restricting the use of non-kinetic cyber operations.¹²⁵ This argument may be rejected, as the definition of an attack under Article 49(1) of the Additional Protocol I does not rely on the definition of its target as a military objective under Article 52(2). The provision in question only applies once an operation has qualified as an attack.¹²⁶

¹²⁴ Dörmann (2011), p. 6; ICRC (2015), p. 41.

¹²⁵ Schmitt (2014), IRRIC, Vol. 96, No. 893, pp. 189-206, at p. 195

¹²⁶ *Ibid*, at p. 197.

5 Case Studies

5.1 Estonia (2007)

The most widely discussed instance of a cyber ‘attack’ is the cyber operations that were directed against Estonia in 2007. Although the operations took place in peacetime, they should be viewed against the background of the political tensions in the region at the time.¹²⁷ The operations targeted the computer systems of the Estonian government, Parliament, hospitals, systems managing emergency call numbers, banks and other targets.¹²⁸ Civilian infrastructures such as newspapers and TV stations were also shut down.¹²⁹ The operations resulted in severe disruptive effects and large-scale financial damage.¹³⁰ The effects of the operations were mainly of economic and societal nature, as there were no injuries, loss of life, or material damage.¹³¹ The incidents are often referred to as the first large-scale cyber assault directed against a state.¹³² While it is believed the operations originated from Russia, there is little concrete evidence to substantiate those claims. Russia has categorically denied any involvement.¹³³

5.2 Georgia (2008)

The Russian-Georgian conflict of 2008 is the first known case of conventional warfare to be accompanied by offensive cyber operations.¹³⁴ The cyber operations that took place systematically defaced Georgian government websites, hacked into news websites to replace their content with anti-Georgian propaganda, and slowed down Internet services, crippling Georgia’s ability to disseminate information during a critical period of time.¹³⁵ The operations preceded Russian troops’ invasion of South Ossetia, and continued for several weeks after ceasefire and the cessation of

¹²⁷ Tikk, Kaska, and Vihul (2010), p. 15-18.

¹²⁸ Ibid, p. 21-23; see also Woltag (2014), p. 43.

¹²⁹ Tikk, Kaska, and Vihul (2010), p. 21-23; Roscini (2014), p. 4-5.

¹³⁰ Harrison-Dinniss (2012), p. 289.

¹³¹ Roscini (2014), p. 4-5.

¹³² Woltag (2014), p. 44.

¹³³ Ibid, p. 44; and Harrison-Dinniss (2012), p. 289.

¹³⁴ Turns, ‘Cyber War and the Concept of “Attack” in International Humanitarian Law’, in Saxon (2013), p. 225-226.

¹³⁵ Roscini (2014), p. 7-8.

traditional military operations.¹³⁶ However, the operations did not cause any physical harm and most closely resemble a form of psychological warfare.¹³⁷ Although suspicions were raised against Russia, there is no conclusive evidence that the Russian government was responsible for the operations. However, the operations appeared coordinated and instructed, and it appears that the Russian hacker community was involved.¹³⁸ Russia denied any involvement in the operations, and stated that they were the work of private citizens.¹³⁹

5.3 Stuxnet (2010)

In 2010, a worm¹⁴⁰ named 'Stuxnet' targeted the control systems of an industrial facility in Iran, allegedly to sabotage Iran's nuclear enrichment programme.¹⁴¹ Although there are no official reports of physical damage, it is believed that Stuxnet caused the destruction of around 1,000 gas centrifuges at the nuclear enrichment plant Natanz.¹⁴² The operation is likely to have delayed the Iranian nuclear programme, thereby providing an alternative to conventional military strike.¹⁴³ Stuxnet is the first known use of malicious software designed to cause material damage.¹⁴⁴ Although no state has claimed responsibility for the operation, the sophistication with which it was carried out indicates that its authors were state-backed professionals, i.e. that the operation originated from a state.¹⁴⁵ Stuxnet is one of the first real military-grade cyber weapons, and possibly the first use of a cyber weapon with effects in the physical domain.¹⁴⁶ The operation occurred during a time when there was no on-going armed conflict, meaning that it would most likely have been considered a use of force *jus ad bellum*.

¹³⁶ Harrison-Dinniss (2012), p. 290.

¹³⁷ Woltag (2014), p. 45-46.

¹³⁸ Tikk, Kaska, and Vihul (2010), p. 74-65.

¹³⁹ Turns, 'Cyber War and the Concept of "Attack" in International Humanitarian Law', in Saxon (2013), p. 226-227.

¹⁴⁰ A worm is used to infiltrate a computer system, allowing the perpetrator to target and control a particular software system, Woltag (2014), p. 291-292.

¹⁴¹ Harrison-Dinniss (2012), p. 291-292.

¹⁴² Albright, Brannan, and Walrond (2010), p. 1-2.

¹⁴³ Albright, Brannan, and Walrond (2011), p. 1-2.

¹⁴⁴ Roscini (2014), p. 6.

¹⁴⁵ Harrison-Dinniss (2012), p. 291-292.

¹⁴⁶ Richards (2014), p. 2-6.

6 Analysis and Conclusion

6.1 Analysis

Cyber warfare is subject to international humanitarian law as any other form of warfare. Humanitarian law applies irrespective of the weapons employed, as confirmed by the Nuclear weapons case, and is able to adapt to new technology by virtue of the Martens Clause and the legal requirement to review new weapons. The issue is rather the nature of the cyber attack. An attack under Article 49(1) of the Additional Protocol I is defined in terms of its consequences. Cyber operations must result in death or injury to persons, or damage or destruction to objects in order to qualify as an attack. This may be problematic, as cyber operations can result in a broad range of outcomes and might not necessarily involve kinetic effects. The qualification of a cyber operation as an attack is significant because it makes most of the substantive provisions restricting the conduct of hostilities operative. There is, however, disagreement in legal doctrine among those who favour a restrictive approach that seeks to restrict the use of cyber operations, and those who favour a permissive approach that allows for a wider range of cyber operations. The restrictive approach can be dismissed through a contextual approach to the Additional Protocol I and its Commentary; the repeated use of terms such as 'violence' and 'combat' in key sections of the text denotes that the relevant provisions do not cover non-violent (i.e. non-physical) cyber operations. The reference made to neutralization, an effect that may be achieved through both kinetic and non-kinetic means, is irrelevant, as the provision constitutes a restriction on the conduct of attacks as they are understood in Article 49(1), and therefore cannot be used to justify a broad interpretation of the term attack. In conclusion, and in response to the first research question, cyber operations that do not engender violence cannot be defined as attacks and are as such not subject to the provisions restricting the conduct of hostilities under the Additional Protocol I. Non-violent cyber operations are therefore on the whole permissible, even if their intended audience is civilians.

An analysis of the case studies demonstrates how the consequence-based understanding of the notion of an attack can be applied to cyber warfare. The cyber

operations that were carried out in 2007 against Estonia occurred during peacetime and were therefore not subject to international humanitarian law. Had the operations occurred during an armed conflict, they would have fallen short of the definition of an attack because they did not result in death, injury, damage or destruction. There are also no reports of excessive human suffering to support the conclusion that the operations amounted to attacks. Despite their large-scale economic and societal effects, most of which affected civilians, the operations would have been lawful as a consequence of their non-qualification as attacks. The 2008 operations directed against Georgian governmental websites and news outlets was the first instance of cyber operations to have occurred in the context of an international armed conflict, and thereby the first case where international humanitarian law would have been applicable. The cyber operations consisted of propaganda and the incapacitation of Georgia's ability to disseminate information, and did as such not result in any physical damage. The operations would therefore not have amounted to attacks in the sense of the Additional Protocol I, making the majority of the provisions restricting the conduct of hostilities inoperative. The Stuxnet virus of 2010 was the first case of a cyber operation with consequences in the physical domain (i.e. the presumed destruction of gas centrifuges at an Iranian nuclear enrichment plant). Although international humanitarian law was inapplicable because there was no state of armed conflict, the operation would undoubtedly have qualified as an attack in such a situation, and would in that case have been made subject to the restrictions of the Additional Protocol I.

The practical implications of the consequence-based understanding of the notion of an attack should not be disregarded. The permissive approach represents an expansion of permissible means and methods of warfare, and opens up for a range of legitimate targets that might otherwise have been unreachable. These aspects of cyber warfare do not necessarily undermine the current legal framework; existing norms still suffice to protect civilians and their objects from the particularly detrimental effects of cyber warfare (death, injury, damage or destruction). However, the Estonia operations illustrate how the regulatory gap with regards to cyber operations that fall below the threshold of an attack may lead to an expansion of war's impact on civilians. The increased reliance on cyber technologies heightens the potential severity of non-kinetic cyber attacks, a factor that is not taken into

account by the current state of legal affairs. A potential development is an interpretative shift of emphasis from the *nature* of harm to the *severity* of harm, or a reinterpretation of the concept of 'injury' to include disruption of or interference with essential civilian infrastructure. The need for reinterpretation is especially apparent in the case of data; data is intangible and does not enjoy protection as an object under the Additional Protocol I. However, the loss of data can have as detrimental effects as those of a kinetic attack. The tendency towards a broader interpretation is seen in the functionality test employed by the Tallinn Manual, which partially resolves the issue by qualifying non-kinetic cyber operations as attacks where the results caused necessitates the replacement of physical components.

6.2 Conclusion

This paper has shown that a permissive approach to the notion of a cyber 'attack' is the most consistent with *de lege lata* in cyber warfare. Cyber operations that are non-physical are not subject to the principles that restrict the conduct of hostilities, unless they result in a need to replace physical components or cause excessive human suffering, and are thus permissible. The case studies illustrate the implications of this state of legal affairs; a large-scale but non-physical cyber attack (e.g. Estonia) may lawfully be directed against civilians despite its substantial societal effects, while a smaller-scale physical attack that targets a handful of civilians would undoubtedly be unlawful. This result is arguably at odds with the underlying principles of international humanitarian law. Arguments for the restrictive approach (i.e. that the use of cyber operations generally should be restricted), however reasonable they may be from a humanitarian perspective, do not reflect *de lege lata* and must therefore be dismissed as reasoning *de lege ferenda*. Future state practice and, in particular, soft law will determine how the understanding of the concept of an attack will adapt in relation to cyber warfare.

Bibliography

Literature

Bothe, Michael, *et al.*, *New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949*, The Hague: Martinus Nijhoff Publishers, 1982.

Clough, Jonathan, *Principles of Cybercrime*, Cambridge: Cambridge University Press, 2015.

Dinstein, Yoram, *The Conduct of Hostilities under the Law of International Armed Conflict*, 3rd ed., Cambridge: Cambridge University Press, 2016.

Evans, Malcolm D. (ed.), *International Law*, 4th ed., Oxford: Oxford University Press, 2014.

Harrison-Dinniss, Heather, *Cyber Warfare and the Laws of War*, Cambridge: Cambridge University Press, 2012.

Henckaerts, Jean-Marie, and Doswald-Beck, Louise (ed.), International Committee of the Red Cross (IRC), *Customary International Humanitarian Law, Volume: 1, Rules*, Cambridge: Cambridge University Press, 2006.

Korling, Fredric, and Zamboni, Mauro (ed.), *Juridisk metodlära*, 1st ed., Lund: Studentlitteratur, 2013.

Nasu, Hitoshi, and McLaughlin, Robert (ed.), *New Technologies and the Law of Armed Conflict*, The Hague: T.M.C. Asser Press, 2014.

Richards, Julian, *Cyber-War: The Anatomy of the Global Security Threat*, Basingstoke: Palgrave Macmillan, 2014.

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

Pilloud *et al.*, International Committee of the Red Cross (ICRC), *Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949*, Geneva: Martinus Nijhoff Publishers, 1987.

Saxon, Dan (ed.), *International Humanitarian Law and the Changing Technology of War*, Leiden; Boston: Martinus Nijhoff Publishers, 2013.

Schmitt, Michael N., *War, Technology and International Humanitarian Law*, Harvard University: Program on Humanitarian Policy and Conflict Research (HPCR), 2005.

Shaw, Malcolm Nathan, *International Law*, 7th ed., Cambridge: Cambridge University Press, 2014.

Solis, Gary D., *The Law of Armed Conflict: International Humanitarian Law in War*, 2nd ed. New York: Cambridge University Press, 2016.

Tsagourias, Nicholas, and Buchan, Russell (ed.), *Research Handbook on International Law and Cyberspace*, Cheltenham: Edward Elgar Publishing, 2015.

Woltag, Johann-Christoph, *Cyber Warfare: Military Cross-Border Computer Network Operations under International Law*, Cambridge: Intersentia, 2014.

Soft Law Documents

Program on Humanitarian Policy and Conflict Research (HPCR) at Harvard University, *Manual on International Law Applicable to Air and Missile Warfare*, Cambridge: Cambridge University Press, 2013 [cit. *HPCR Manual on International Law Applicable to Air and Missile Warfare* (2013)].

Schmitt, Michael N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare / Volume 0*, Cambridge: Cambridge University Press, 2013.

Schmitt, Michael N., and Vihul, Liis (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations: Prepared by the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence*, Cambridge: Cambridge University Press, 2017.

Journals

Dinstein, Yoram, 'The Principle of Distinction and Cyber War in International Armed Conflicts', *Journal of Conflict and Security Law* (2012), 17(2), pp. 216-277.

Droege, Cordula, 'Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians', *International Review of the Red Cross (IRRC)* (2012), Vol. 94, No. 886, pp. 533-578.

Geiß, Robin, and Lahmann, Henning, 'Cyber Warfare: Applying the Principle of Distinction in an Interconnected Space', *Israel Law Review* (2012), 45(3), pp. 381-399.

Schmitt, Michael N., 'Rewired warfare: Rethinking the law of cyber attack', *International Law Review of the Red Cross (IRRC)* (2014), Vol. 96, No. 893, pp. 189-206.

Schmitt, Michael N., 'Wired Warfare: Computer network attack and *jus in bello*', *International Law Review of the Red Cross (IRRC)* (2002), Vol. 84, No. 846, pp. 365-399.

Conference Reports and Materials

Dörmann, Knut, 'Applicability of the Additional Protocol to Computer Network Attack', in Byström, Karin (ed.), *Proceedings on the International Expert Conference on Computer Network Attacks and the Applicability of International Humanitarian Law*, Stockholm, 17-19 November 2011, p. 139, Swedish National Defence College, 2005, reprinted at <www.icrc.org/eng/resources/documents/misc/68lg92.htm>.

International Committee of the Red Cross (ICRC), *International Humanitarian Law and the Challenges of Contemporary Armed Conflicts*, Report of the 32nd International Conference of the Red Cross and the Red Crescent, Geneva, 8-10 December 2015.

Other Reports

Albright, David, Brannan, Paul, and Walrond, Christina, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?*, Washington D.C.: Institute for Science and International Security (ISIS), 2010.

Albright, David, Brannan, Paul, and Walrond, Christina, *Stuxnet Malware and Natanz: Update of ISIS December 22, 2010 Report*, Washington D.C.: Institute for Science and International Security (ISIS), 2011.

Melzer, Nils, *Cyberwarfare and International Law*, Geneva: United Nations Institute for Disarmament Research (UNIDIR), 2011.

Tikk, Eneken, Kaska, Kadri, and Vihul, Liis, *International Cyber Incidents: Legal Considerations*, Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2010.

International Treaties and Conventions

Council of Europe, *Council of Europe Convention on Cybercrime*, European Treaty Series (ETS), No. 185, 23 November 2001.

International Committee of the Red Cross (ICRC), *Geneva Convention for the Amelioration of the Condition of the Wounded and the Sick in Armed Forces in the Field* (First Geneva Convention), 12 August 1949, 75 UNTS 31 [cit. Geneva Conventions].

International Committee of the Red Cross (ICRC), *Geneva Convention for the Amelioration of the Condition of Wounded, Sick and Shipwrecked Members of*

Armed Forces at Sea (Second Geneva Convention), 12 August 1949, 75 UNTS 85 [cit. Geneva Conventions].

International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Treatment of Prisoners of War* (Third Geneva Convention), 12 August 1949, 75 UNTS 135 [cit. Geneva Conventions].

International Committee of the Red Cross (ICRC), *Geneva Convention Relative to the Protection of Civilian Persons in Time of War* (Fourth Geneva Convention), 12 August 1949, 75 UNTS 287 [cit. Geneva Conventions].

International Committee of the Red Cross (ICRC), *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts* (First Protocol/Protocol I), 8 June 1977, 1125 UNTS 3 [cit. Additional Protocol I].

International Committee of the Red Cross (ICRC), *Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of Non-International Armed Conflicts* (Second Protocol/Protocol II), 8 June 1977, 1125 UNTS 609.

International Committee of the Red Cross (ICRC), *Declaration Renouncing the Use, in Time of War, of Explosive Projectiles Under 400 Grammes Weight*, 29 November/11 December 1868 [cit. 1868 Saint Petersburg Declaration].

International Conferences (The Hague), *Hague Convention (II) with Respect to the Laws and Customs of War on Land and its Annex: Regulations Concerning the Laws and Customs of War on Land*, 29 July 1899.

International Conferences (The Hague), *Hague Convention (IV) Respecting the Laws and Customs of War on Land and Its Annex: Regulations Concerning the Laws and Customs of War on Land*, 18 October 1907.

United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI [cit. Charter of the United Nations].

United Nations, *Statute of the International Court of Justice*, 18 April 1946 [cit. Statute of the International Court of Justice].

United Nations, *Vienna Convention on the Law of Treaties*, 23 May 1969, United Nations, Treaty Series, Vol. 1155, p. 331 [cit. Vienna Convention on the Law of Treaties].

Official Documents

Directive 2013/40/EU of the European Parliament and the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA [2013] L 218/8.

United Nations General Assembly (UNGA), 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (24 June 2013), UN Doc. A/68//98.

United Nations General Assembly (UNGA), 'Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (22 July 2015), UN Doc. A/70/174.

United Nations General Assembly (UNGA) Resolution A/RES/58/32, 'Developments in the field of information and telecommunications in the context of international security' (8 December 2003) [cit. UNGA Res. A/RES/58/32 of 8 December 2003].

United Nations General Assembly (UNGA) Resolution A/RES/59/61, 'Developments in the field of information and telecommunications in the context of international security' (3 December 2004) [cit. UNGA Res. A/RES/59/61 of 3 December 2004].

United Nations General Assembly (UNGA) Resolution A/RES/60/45, 'Developments in the field of information and telecommunications in the context of international security' (8 December 2005) [cit. UNGA Res. A/RES/59/61 of 8 December 2004].

United Nations General Assembly (UNGA) Resolution A/RES/61/54, 'Developments in the field of information and telecommunications in the context of international security' (6 December 2006) [cit. UNGA Res. A/RES/61/54 of 6 December 2006].

United Nations General Assembly (UNGA) Resolution A/RES/62/17, 'Developments in the field of information and telecommunications in the context of international security' (5 December 2007) [cit. UNGA Res. A/RES/62/17 of 5 December 2007].

United Nations General Assembly (UNGA) Resolution A/RES/63/37, 'Developments in the field of information and telecommunications in the context of international security' (2 December 2008) [cit. UNGA Res. A/RES/63/37 of 2 December 2008].

United Nations General Assembly (UNGA) Resolution A/RES/64/25, 'Developments in the field of information and telecommunications in the context of international security' (2 December 2009) [cit. UNGA Res. A/RES/64/25 of 2 December 2009].

Electronic resources

Newspaper Articles

Cowell, Alan, 'Cyberwar and Social Media in the Gaza Conflict' *The New York Times*, 19 November 2012, <https://rendezvous.blogs.nytimes.com/2012/11/19/cyberwar-and-social-media-in-the-gaza-conflict/?_r=1>, (accessed 17 May 2017).

Laudicina, Paul, '2017 Will Be The Year Of Cyber Warfare', *Forbes*, 16 December 2016, <<https://www.forbes.com/sites/paulaudicina/2016/12/16/2017-will-be-the-year-of-cyber-warfare/#4a612986bad0>>, (accessed 17 May 2017).

Wong, Julia Carrie, and Solon, Olivia, 'Massive ransomware cyber-attack hits nearly 100 countries around the world', *The Guardian*, 12 May 2017, <<https://www.theguardian.com/technology/2017/may/12/global-cyber-attack-ransomware-nsa-uk-nhs>>, (accessed 17 May 2017).

Other Electronic Resources

International Committee of the Red Cross (ICRC), 'The Geneva Conventions of 1949 and their Additional Protocols', *International Committee of the Red Cross*, 29 October 2010, <<https://www.icrc.org/eng/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm>>, (accessed 20 May 2017).

Table of Cases

International Court of Justice (ICJ)

Legality of the Threat or Use of Nuclear Weapons (Advisory Opinion), ICJ Reports 1996, p. 226, International Court of Justice (ICJ), 8 July 1996.