IFHV
Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht
Institute for International Law of Peace and Armed Conflict

Modern Technologies and Targeting under International Humanitarian Law

Charlotte Lülf

IFHV Working Paper, Vol. 3, No. 3

Bibliographic information:

Title:	Modern Technologies and Targeting under International Humanitarian Law
Author(s):	Charlotte Lülf
Source:	IFHV Working Papers, Vol. 3, No. 3
Date:	December 2013
DOI:	https://doi.org/10.17176/20220622-131740-0
ISSN:	2199-1367

Suggested citation:
Lülf, C. (2013). Modern Technologies and Targeting under International Humanitarian Law. IFHV Working Paper, 3(3).

ISSN: 2199-1367

RUB

RUHR-UNIVERSITÄT BOCHUM

IFHV Working Paper Vol. 3, No. 3, Dezember 2013

Modern Technologies and Targeting under International Humanitarian Law

Charlotte Lülf

IFHV Working Paper Vol. 3, No. 3, December 2013

URL: http://www.ruhr-uni-bochum.de/ifhv/documents/workingpapers/wp3_3.pdf

MODERN TECHNOLOGIES AND TARGETING UNDER INTERNATIONAL HUMANITARIAN LAW

Charlotte Lülf*

LL.M. in Public International Law (Leiden University), M.A. in Political Science (Kiel University), ch.luelf@web.de

Abstract

Over the last decades, the worldwide evolution and advancement of technology interfused nearly all aspects of life, including the conduct of States and non-State actors in armed conflict. The *lex specialis* governing armed conflicts, international humanitarian law (IHL), has always been challenged by these transformation of conflicts and continuously advancing weaponry. However, those involved in armed conflict situation, especially those taking part in actual combat, are in need of precise regulation or at least interpretation thereof to determine which conduct is lawful and which is not. Therefore modern technologies and the alteration in targeting made possible by their use have to be continuously reassessed for their compliance with IHL and its overall objectives. This thesis will focus on two distinctive types of modern technology, on the one hand unmanned Aerial Vehicles (UAV) and unmanned combat aerial vehicles (UCAV) and on the other hand cyber attacks and their (il)legality under the laws of armed conflict.

* This paper is a revised version of the author`s master thesis originally submitted at the LL.M. (reg.) in Public International Law Programme at the University of Leiden (Netherlands).

URL: http://www.ruhr-uni-bochum.de/ifhv/documents/workingpapers/wp3_3.pdf

MODERN TECHNOLOGIES AND TARGETING UNDER INTERNATIONAL HUMANITARIAN LAW

Content

List of Acronyms

AP	Additional Protocol
CIA	Central Intelligence Agency
DoS	Denial of Service
DDoS	Distributed Denial of Service
GC	Geneva Convention
HALE	High Altitude and Long Endurance
HPCR	Manual on International Law Applicable to Air and Missile Warfare
ICC	International Criminal Court
ICJ	International Court of Justice
ICRC	International Committee of the Red Cross
ICTY	International Criminal Tribunal for the Former Yugoslavia
IHL	International Humanitarian Law
NATO	North Atlantic Treaty Organization
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle
UGV	Unmanned Ground Vehicle
UNO	United Nations Organisation
USV	Unmanned Surface Vehicle
UUV	Unmanned Underwater Vehicle
UV	Unmanned Vehicle
VCLT	Vienna Convention on the Law of Treaties

1. Introduction

Over the last decades the worldwide evolution and advancement of technology interfused nearly all aspects of life, including the conduct of States and non-State actors in armed conflict.[1] The *lex specialis* governing armed conflicts, international humanitarian law (IHL), has always been challenged by the transformation of conflicts and continuously advancing weaponry. Solely in the last century machine guns, tanks, intercontinental ballistic missiles and nuclear weapons of various types have been invented, most of them have been used. Those developments in warfare influence the affected civilian population to varying extents. IHL, however, explicitly follows two major purposes, namely to restrain the conduct of hostilities and to protect individual civilians and populations as a whole from the waging of war.[2]

IHL is a compromise between military necessity and humanitarian considerations, balancing national military and security interests and the well-being of the civilian population.[3] Especially when it comes to new developments, legal uncertainty is sometimes worrisome and precise interpretations rare. It is a difficult task, since, as Jacob Kellenberger emphasized, "provisions are framed in rather abstract terms"[4] and, to quote Murphy, "the language of the international instruments in questions [IHL] is often obtuse and unintelligible".[5] However, those involved in armed conflict situation, especially those taking part in actual combat, are in need of precise regulation or at least interpretation thereof to determine which conduct is lawful and which is not, and to know their rights and their duties. Judge Weeramantray addressed this dilemma in its dissenting opinion to the ICJ`s *Advisory Opinion on the Legality of Nuclear Weapons*, "by their very nature, problems in humanitarian law are not abstract intellectual enquiries which can be pursued in ivory-tower detachment from the sad realities which are their stuff and substance."[6] One has to keep in mind that they are regulating actual conduct, one that can have considerable impact on people's lives. Therefore modern technologies and the alteration in targeting

---

[1] *See* D. Brown, *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 47 Harvard International Law Journal 1 (2006), at 179.

[2] ICRC, *What Is International Humanitarian Law*, Legal Fact Sheet 7 (2004), http://www.icrc.org/eng/resources/documents/legal-fact-sheet/humanitarian-law-factsheet.htm (8 October 2012), at 1.

[3] N. Hayashi, *Requirements of Military Necessity in International Humanitarian Law and International Criminal Law*, 28 Boston University International Law Journal 1 (2010), at 48.

[4] J. Kellenberger, International Humanitarian Law at the Beginning of the 21 Century, Keynote address at the 26th Round Table in San Remo on Current Problems of International Humanitarian Law (05 September 2002), http://www.icrc.org/eng/resources/documents/misc/5e2c8v.htm (2 August 2012).

[5] R. Murphy, *International Humanitarian Law Training for Multinational Peace Support Operations – Lessons from Experience*, International Review of the Red Cross 840 (2000), http://www.icrc.org/eng/resources/documents/misc/57jqtg.htm (2 August 2012).

[6] Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, ICJ Reports 1996 (Dissenting Opinion Judge Weeramantry), at 222.

made possible by their use have to be continuously reassessed for their compliance with IHL and its overall objectives.

The latest shift of this revolution in military affairs[7] is a proceeding removal of humans from the actual battlefield. Eventually this also includes the proliferation of robotic technology, which is already assessed as the revolutionary breakthrough in future combat, although creating an obstacle to conventional military strategy as well as legal and moral conceptions. Nonetheless, completely autonomous robots, equipped to execute lethal and targeted strike, are not yet deployed in contemporary armed conflicts and their compliance with IHL regulations is still an assessment on the theoretical level. Therefore this master thesis will focus on two distinctive types of modern technology that can be considered as intermediate steps in this process and that are increasingly dominating current warfare: unmanned Aerial Vehicles (UAV), unmanned combat aerial vehicles (UCAV) and cyber attacks.

No specific legal treaties exist for the employment of either UCAV/UAV technology or cyber attacks during armed conflict. For this reason, the thesis will firstly concentrate on the general legal regime of IHL, which was developed, although influenced by respective historical and technological shifts, mostly non-situation- or weapon-specific, intended to regulate current and future armed conflicts of various characteristics. The binding *lex lata* of IHL applicable to new developments in weaponry, general regulations on methods and means of warfare and specifically the regulations concerning targeting will be described – the fundamental principles of IHL and their characteristics will be in focus - to herewith display the legal framework to which standards both technologies have to live up. Due to the scope of this thesis not every aspect might be assessed in detail. Focus will be given to the major principles and regulations, whereas other issues, as for instance the laws on neutrality, will be excluded.

Operating in a highly automated way, and often only controlled by human operators during the final phase of an operation, drones, so called UAVs or UCAVs, will be analysed in the first part of the main section. These new types of aircraft are most prominent in contemporary armed conflicts and military strategies due to their technological advantages. In the public and within the human rights community, however, their deployment is highly criticized. But is their deployment during armed conflict in general or in specific scenarios violating IHL? The chapter will assess their legal status under IHL, before discussing the application of the fundamental principles concerning targeting with regard to UCAV/UAVs and their deployment and associated conduct during armed conflicts of international and non-international character. Factual information to UAV/UCAV technology as well as some insights regarding their deployment in contemporary armed conflicts will be given in the annex.

---

[7] *Cf.* M. Schmitt, *Bellum Americanum: The US View of Twenty-first Century War and Its Possible Implications for the Law of Armed Conflict*, Michigan Journal of International Law 19 (1991), at 1058 *et seq.*

The next chapter will focus on another major development that is changing the character of armed conflicts today. The internet and increasing dependence on computer technology is not only dominating daily life but has also found its way into the military sector, as military technology itself is nowadays mostly based on computer networks.[8] The possibility to use computer technology as a means of warfare itself by targeting the enemies' computer system through cyber space has already proven itself to be effective, as incidents over the last years have shown. Cyber attacks are however, a new and unfamiliar instrument, not in all parts comparable to conventional weaponry. Nevertheless, if employed during armed conflict, IHL is the field of law applicable to their use. But at what point can one consider an operation in cyber space an armed attack comparable to those caused by conventional kinetic weaponry? After assessing the threshold of armed conflict with regard to cyber attacks, the fundamental principles of targeting will be applied to these operations, to review their effectiveness for application to cyber space. Non-legal background information regarding different techniques and current cases of deployment can also be found in the annex.

The main section will analyse both new technologies and their deployment during armed conflict for compliance with IHL, focussing on the principles relevant to targeting operations. Parallel to assessing the lawfulness of UCAV/UAVs and cyber attacks, existing dilemmas in form of concrete violations or lacunae in the applicable law will be exposed. Is IHL in its current form able to meet the challenges of advancing military technologies? The conclusion of this thesis will further take a more forward-looking perspective, asking a specific question: are the old rules still effectively applicable or does the international community need to create new regulations for those two technologies? Possible arguments for and against new treaties will be discussed.

Keeping in mind the rapidness of events during armed conflict, legal certainty on the "do's and don'ts" of any means and weapons deployment must be provided beforehand to the greatest extend possible. This thesis will tackle this issue with regard to two distinctive types of modern technologies. The application of IHL on those technologies must be assessed properly to follow the premise of IHL to restrict the level of violence and to shield and especially protect those not directly participating in combat.

2. Regulations of International Humanitarian Law

IHL places limits on the use of force and the conduct of belligerents during armed conflict. It has, due to the variety of new actors and developments in advancing renunciation of the classical State-against-State-war, become increasingly important to clarify the meaning of the relevant provisions. For

[8] *Cf.* J. Kelsey, *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review 106 (2008), at 1432.

these reasons, the following chapter will shed some light on the rules and principles regulating the conduct during armed conflict and their interpretation. The legal question of this master thesis limits the relevance of this matter to those regulations concerned with methods and means of warfare and technological development as well as those parts of IHL regulating targeting.

2.1 Regulations Concerning (New) Means of Warfare

Article 22 of the Hague Regulations, later restated in Article 35(I) of the Additional Protocol I (AP I), lays down the general premise, that "the right of belligerents to adopt means of injuring the enemy is not unlimited". This general restriction combined with the principle of distinction creates two specific customary law rules affecting the choice of weapons and means and methods of warfare: Generally IHL forbids to employ weapons or means of warfare that may be expected to cause superfluous injury or unnecessary suffering[9] and it is furthermore forbidden to employ methods or means of warfare that are indiscriminate, which means that they cannot be directed against a specific military objective.[10]

IHL as an effective instrument to restrict the conduct of war is continuously challenged by the advancing technological developments. Henry Dunant stated in his famous book, a Memory of Solferino, "If the new and frightful weapons of destruction which are now at the disposal of the nations seem destined to abridge the duration of future wars, it appears likely […] that future battles will only become more and more murderous."[11] But how does IHL react to new developments and advances in weaponry?

The application of IHL to new weapons was for the first time officially discussed in 1868, when the obligation to review new technologies was inserted into the St. Petersburg Declaration:

"The Contracting or Acceding Parties reserve to themselves to come hereafter to an understanding whenever a precise proposition shall be drawn up *in view of future improvements which science may effect in the armament of troops, in order to maintain the principles which they have established*, and to conciliate the necessities of war with the laws of humanity".[12]

In 1977, this need for review was again empathized and strengthened by its restatement within Article 36 AP I:

"In the study, development, acquisition or adoption of a new weapon, means or methods of warfare, a High Contracting Party is under an *obligation to review* whether its employment would, in some or in all circumstances, be prohibited by

[9] Convention (IV) Respecting the Laws and Customs of War on Land, 18 October 1907, and its Annex: Regulations Concerning the Laws and Customs of War on Land (Hague Convention IV), Art. 23(e) and Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts of 8 June 1977 (AP I), Art. 35(2).
[10] Art. 51(4) AP I.
[11] H. Dunant, A Memory of Solferino (1862), in ICRC Publication 1986, at 30.
[12] Emphasis added by the author.

this Protocol or by any other rule of international law applicable to the High Contracting Party"[13],

enshrining the obligation to determine the lawfulness of weapons, means and methods before they are developed and purchased for a State's military arsenal.[14] The obligation of Article 36 is supported by Article 82 AP I, which requires legal advisors to assess new weapons and means for their compliance with IHL.

At the 28th International Conference of the Red Cross and Red Crescent, the ICRC again stresses,

"in light of the rapid developments of weapons technology and in order to protect civilians from the indiscriminate effects of weapons and combatants from unnecessary suffering and prohibited weapons, *all new weapons, means and methods of warfare should be subject to rigorous and multidisciplinary review*".[15]

In 2006, the ICRC published a guide to the legal review of new weapons, methods and means of warfare, to strengthen the review process. That is of major importance, as IHL does not provide for any concrete instructions to establish such a review process, but leaves it in the States' responsibility.[16] Unfortunately today only a few States have established a formal domestic mechanism to do so.[17]

2.2 Regulations Concerning Targeting

The regulations concerning targeting circle around a special set of questions: Who and what is a lawful target? How is an attack lawfully conducted? What are proportionate casualties? The fundamental principles of IHL, which are applicable when planning and conducting any attack, will be assessed in the following subsections to build a theoretical framework, before it will be applied to the specific modern technologies relevant in this thesis in the following.

2.2.1 Balancing Military Necessity and the Principle of Humanity

Military necessity in times of war is a lawful justification for combatants to conduct otherwise criminal actions, i.e. injure, kill or destroy.[18] During

[13] Emphasis added by the author.

[14] *Cf.* R. Hughes, Towards a Global Regime for Cyber Warfare (2010), Cyber Security Project, Chatham House London, at 3.

[15] Final Goal 2.5 of the Agenda for Humanitarian Action adopted by the 28th International Conference of the Red Cross and Red Crescent, Geneva, 2-6 December 2003, www.icrc.org/eng/resources/.../p1103.htm (18 July 2012) (emphasis added).

[16] ICRC, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, http://www.icrc.org/eng/resources/documents/publication/p0902.htm (21 August 2012), at 20.

[17] *Cf.* ICRC, Review of New Weapons (29 October 2010), http://www.icrc.org/eng/war-and-law/weapons/new-weapons/overview-review-of-new-weapons.htm (20 August 2012).

[18] *Cf.* M. Schmitt, *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 4 Virginia Journal of International Law 50 (2010), at 796 and

hostilities military necessity is the driving force of military campaigns. It is the fundamental principle that "permits a belligerent subject to the law of war, to apply any amount and kind of force to compel the complete submission of the enemy with the least possible expenditure of time, life and money."[19] But IHL is also the law *limiting* the conduct of the parties. In this regard, military necessity at the same time limits the conduct of belligerents: All parties to the conflict are legally restrained to only use the force necessary to attain the military aim that is proportionate to the civilian casualties caused. In a similar manner it was enshrined in the preamble to the St. Petersburg Declaration: "the only legitimate object which states should endeavour to accomplish during war is to *weaken the military forces of the enemy* and for this purpose it is sufficient to disable the greatest possible number of men."[20] But although military necessity may justify certain behaviour during combat that is otherwise illegal, it does not permit violations of IHL.[21] IHL regulations can be considered compromises, balancing between opposites: military necessity, safeguarding national security interest on one hand and on the other hand, the principle of humanity, providing for the well-being of the civilian population[22] – a balance already laid down in the 1886 Declaration that, "fixed the technical limits at which the necessity of war ought to yield to the requirements of humanity."[23]

The principle of humanity can be considered the core value shaping the evolution of IHL, the idea that even in times when the right of the adversaries to injure their enemy is affirmed by, or in consistent with the rules of armed conflict, these rights are not unlimited. This principle is reflected in Article 22 Hague IV[24] and further enshrined in Article 35 AP I[25], as well as in preambles of successor treaties, as the Convention on Certain Conventional Weapons. It also forms an integral part of customary international law.[26] The principle of humanity is therefore, as moral imperative, universally binding and directly inspiring the law.[27]

Under IHL, conduct to weaken the enemy is acceptable and therefore it is lawful to target the enemies' military strength. As we have seen, the conduct in combat

---

similar Y. Sandoz/C. Swinarski/B. Zimmermann (Eds.), Commentary on the Additional Protocol of 8 June 1977 to the Geneva Conventions of 12 August 1949 (1987), at 1386.

[19] H. Lauterbach, *Hostages Trial*, in: H. Lauterbach (Ed.), Annual Digest and Reports of Public International Law Cases: a Selection from the Decision of International Courts and Tribunals and Military Courts Given During the Year 1948 (1953), at 646.

[20] Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight of 29 November/11 December 1868 (1868 St. Petersburg Declaration) (Emphasis added).

[21] *Cf.* Y. Dinstein, The Conduct of Hostilities under the Law of International Armed Conflict (2004), at 19 *et seq.*

[22] *See further* Schmitt, *supra* note 18, at 799.

[23] St. Petersburg Declaration.

[24] Art. 22 Hague Convention IV: "The right of belligerents to adopt means of injuring the enemy is not unlimited".

[25] Art. 35 AP I: "In any armed conflict, the right of the Parties to the conflict to choose methods or means of warfare is not unlimited".

[26] *Cf.* Schmitt, *supra* note 18, at 800.

[27] *Cf.* C. von Buttlar/T. Stein, Völkerrecht (2009), at 441.

is nonetheless subject to concrete restrictions, particularly with regard to targeting issues, all governed by the principle of distinction. This should be discussed in the following subsection.

2.2.2 The Principle of Distinction

The principle of distinction, according to Turns, "should lie at the heart of modern armed conflicts"[28], as it is the basis of major regulations concerning the issue of lawful targeting. Despite its codification in Article 48 AP I, this principle is also of customary law character.[29] The key question concerning the principle of distinction with respect to targeting is: What constitutes a military target? Answering this question one has to distinguish between lawful human and non-human targets.

2.2.2.1 Combatants and Civilians

For decades the rule concerning the targeting of humans was comparably uncontroversial, due to the fact that armed conflicts were for a long time dominated by the classical war with identifiable State armed forces, the combatants, fighting each other. Combatants are lawfully targetable at all times[30] and Article 43(1), (2), (3) AP I, paralleled by Article 4 GC III, defines combatants and their right to participate directly in hostilities, while Article 44 AP I further addresses combatants and their prisoner of war status, including their obligation to distinguish themselves from civilians, by virtue of Article 44(3) AP I.

The counterpart to combatants in IHL is the category of civilians – all those people who are *ipso facto* not combatants, since IHL only provides for a negative definition in Article 50(1) AP I: "1. A civilian is any person who does not belong to one of the categories of persons referred to in Article 4A(1), (2), (3), (6) of the Third Convention and Article 43 of this Protocol […]" and therefore not lawfully directly targetable, but on the contrary, are specially protected. The protection premise of IHL expands further, as all person should be considered civilians by virtue of Article 50(1) AP I in cases of doubt concerning their status.

There is an exception to the absolute rule of protection: If civilians take direct participation in hostilities he or she loses this status of a protected person. Article 50(3) AP I clarifies: "Civilians shall enjoy the protection afforded by this

---

[28] D. Turns, *The Law of Armed Conflict*, in M. Evans (Ed.), International Law (2010), at 830.

[29] *Cf.* M. Schmitt, *The Principle of Distinction in 21st Century Warfare*, Yale Human Rights and Development Law Journal 2 (1999), at 148; Turns, *supra* note 28, at 830; G. Swiney, *Saving Lives: the Principle of Distinction and the Realities of Modern War*, 3 The International Lawyer 39 (2006), at 734; K. Asa, *The Principle of Distinction*, 2 Journal of Military Ethics 6 (2007), at 153.

[30] The only exception concerning the lawful attack on combatants is made when they are *hors de combat*, in accordance with Art. 41(2) AP I. Debated on the criteria for being *hors de combat*, *see for instance*, I. Henderson, The Contemporary Law of Targeting, Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I (2009), at 85; M. Bothe/K. Partsch/W. Solf, New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949 (1982), at 220 *et seq.*

section, unless and for such time as they take direct participation in hostilities." As a sincere challenge to the traditionally clear cut separation of combatants and civilians, a new phenomenon of – disputably called 'unlawful combatants' – civilians taking direct participation came up or at least gained considered attention during the last decades, especially in relation to the increase in non-international armed conflicts and the global 'war on terror'.[31]

The non-legal term of an unlawful combatant was made up on the political level to address civilians participating to a varying extent in combat without being legally permitted to do so. The Israel Supreme Court, assembled as High Court of Justice referred to this paradox: "It is difficult to see for us how a third category can be recognized in the framework of the Hague and Geneva Conventions".[32] Similarly addressed the ICTY in its *Tadic*-Judgment this rather vague term, that has nonetheless became quite popular in debating alleged terrorist, insurgents and alike: "It is unnecessary to define exactly the line dividing those taking an active part in hostilities and those who are not so involved. It is sufficient […] to ascertain whether […] that person was actively involved in hostilities at the relevant time."[33] But due to the increase and the variety of involvements of civilians, the interpretation of the regulations has to be precise to not expand legal uncertainty in this already disputed area.

In 2003, 2004 and 2005 the ICRC and the TMC Asser Institute organized expert-conferences on these questions and also the ICRC Guidelines on direct participation in hostilities tried to shed some light on a precise interpretation of Article 51(3) AP I.[34] For six years the ICRC gathered experts in informal consultations to answer three key questions and clarify the interpretation IHL regulations in light of civilian involvement in hostilities: "Who is considered a civilian for the purpose of the principle of distinction?", "What conduct amounts to direct participation in hostilities?" and "What modalities govern the loss of

---

[31] *See* A. McDonald, The Challenges to International Humanitarian Law and the Principle of Distinction and Protection from the Increased Participation of Civilians in Hostilities, Expert Analysis of the T.M.C. Asser Institute (2004), http://www.asser.nl/default.aspx?site_id=9&level1=13337&level2=13379 (18 August 2012); M. Hakimi, *A Functional Approach to Targeting and Detention*, Michigan Law Review 110 (2012), at 1379.

[32] Third Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report, International Committee of the Red Cross (2005), www.icrc.org/.../2005-09-report-dph-2005-icrc (15 August 2012), at 6.

[33] Prosecutor *v.* Tadic, Opinion and Judgment, Case No IT-94-1-T, T.Ch. II, 7 May 1997, at para. 616.

[34] It has to be mentioned at this point that the ICRC's study has been heavily criticized by commentators and States. State practice and *opinio juris*, not ICRC publications, so the opponents, are the primary source for the establishment of binding custom. Nonetheless, due to the lack of other authoritative reaction within the international community, the study has become a guidance in the discussion on direct participation. *See* J. Marsh/S. Glabe, *Times for the United States to Participate*, 1 Virginia Journal of International Law 13 (2011), at 14. *For further discussion*, B. Boothby, *`And for Such Time As´: The Time Dimension to Direct Participation in Hostilities*, New York University International Law and Policy 42 (2010).

protection against direct attacks?".[35] The ten recommendations given and the commentary supplementing the document reflect the ICRC's suggestions for interpretation of the existing regulations. One major result of the process was the crystallization of three cumulative criteria, the so-called constitutive elements of direct participation in hostilities, to classify acts of civilians that amount to an unlawful direct participation:

1. The Threshold of Harm
2. A Direct Causation
3. The Belligerent Nexus[36]

Regarding the time factor, in general one can say that a civilian who takes direct part in hostilities loses his protection for the time involved in fighting and not further. The classical example in this case would be the farmer that shot at enemy combatants during night but executed his farming activities at daytime. In this scenario, the prevailing view is that the farmer regaines his immunity and protection at the moment he lays down his weapon, although during the moment of his involvement he is lawfully targetable. This leads to the so-called revolving door problem[37], if the farmer acts repeatedly in this manner. The temporal limitation to the loss of the protection status is highly debated among legal scholars. Henderson in accordance with the Israel Supreme Court held that only if the civilian's participation is so continuous it amounts to an uninterrupted participation, the civilian loses its protection completely. "A civilian who commits a chain of hostilities, with short periods of rest between them, loses his immunity from attack 'for such time' as he is committing the chain of acts."[38] Still highly disputed, also by participants of the process themselves, e.g. as being too restrictive due to the exclusion of for instance support activities by Schmitt, by Parks expounding the problems of restrictive use of force against a legitimate target, by Boothby contesting the interpretation of the wording "unless and for such time",[39] the criteria nonetheless offer a valuable guideline, so stated by Melzer in his article in detail, countering some

---

[35] N. Melzer, Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (2009), http://www.icrc.org/eng/resources/documents/publication/p0990.htm (7 October 2012), at 9 and 13.

[36] 1. the act must be likely to adversely affect the military operations or military capacity of a party to an armed conflict or, alternatively, to inflict death, injury, or destruction on persons or objects protected against direct attack. 2. there must be a direct causal link between the act and the harm likely to result either from that act, or from a coordinated military operation of which that act constitutes an integral part. 3. the act must be specifically designed to directly cause the required threshold of harm in support of a party to the conflict and to the detriment of another. *Ibid.*, at 46.

[37] *Inter alia* discussed by the ICRC, Summary Report, Second Expert Meeting on the Notion of Direct Participation in Hostilities, The Hague (2004), *www.icrc.org/.../2004-07-report-dph-2004-icrc.pdf (2 August 2012),* at 22.

[38] The Public Committee against Torture in Israel *v.* The Government of Israel, High Court of Justice 769/02, 13 December 2006, at 39.

[39] N. Melzer, *Keeping the Balance between Military Necessity and Humanity: A Response to the four Critiques of the ICRC's Interpretative Guidance on the Notion of Direct Participation in Hostilities*, New York University Journal of International Law and Policy 42 (2010), at 835.

of the critiques mentioned above, "a coherent and consolidated framework of concepts and principles bases on which operational decisions ought to be made".[40]

But there is another development that also furthers the involvement of civilians in armed conflict due to their expertise. Increasingly and because of the progressing advancement of military technology, as will be discussed in detail in the following chapter, the spectrum of involvement of civilians is expanded and therefore the question has to be raised, at which point civilian experts illegally take part in hostilities, become prosecutable and lose their protection under IHL. These can be for instance civilians working at a munitions factory or civilian scientist conducting research. But how 'direct' must the participation in hostilities actually be to breach IHL? In 1954, Stone assessed that a distinction could be made between true civilians and civilians supporting the parties by for instance equipping and maintaining airplanes, tanks or munitions on which military success depends highly.[41] The latter category should be lawfully targetable at work as well as at home.[42] In today's interpretation of the provisions, particularly of the AP, this assessment must be rejected. Factory workers may contribute to some extent to the armed conflict as a whole but the term 'hostilities' is interpreted narrower. Roger states that for instance producing arms and conducting military engineering would, although making a military contribution, not be considered a direct participation in hostilities.[43] Solf is contributing to the debate in a comparable way by stating that although a civilian may not lose his/her protection against individualized attacks while working at a ammunition plant, the risk of *de facto* collateral injury when the person is in the vicinity of the munitions plant is undeniable, although he/she continues to be under full legal protection.[44] The direct causation of harm to the enemy as consequence of the civilian's action in this regard is the essential link. The ICRC's commentary held: "Direct participation in hostilities implies a direct causal relationship between the activity engaged in and the harm done to the enemy at the time and the place where the activity takes place."[45] Schmitt concretized this test, stating that, a "but for" causation would be the fundamental criterion. The consequence would not have occurred, if the act had not taken place.[46] Regular maintenance on equipment in this regard would not, preparing equipment for a planned combat operation on the other hand, would amount to a direct participation. With regard to the subsequently discussed modern technologies it should be stressed that proximity to the actual battlefield

---

[40] *Ibid.*, at 915.

[41] *Cf.* J. Stone, Legal Controls of International Conflict: A Treatise on the Dynamics of Disputes and War Law (1954), at 628.

[42] *Cf. Ibid.*

[43] *Cf.* Anthony Rogers, Law on the Battlefield (2004), at 8 *et seq.*

[44] *Cf.* W. Solf, *Protection of Civilians Against the Effects of Hostilities under Customary International Law and under Protocol I*, 1 American University Journal of International Law and Policy 117 (1986), at 131.

[45] Sandoz/Swinarski/Zimmermann, *supra* note 18, at 1679.

[46] *Cf.* M. Schmitt, 'Direct Participation in Hostilities' and 21st Century Armed Conflict (2004), http://www.michaelschmitt.org/images/Directparticipationpageproofs.pdf (15 July 2012), at 505.

is not a relevant factor. This is supported by the statement of the ICTY in its *Kunarac, Kovac and Vukovic* Case: "There is not necessary correlation between the area where the actual fighting is taking place and the geographical reach of the laws of war."[47]

The debate on direct participation in hostilities is still controversial. This analysis will again be picked up in the case studies and assessed with regard to the specific technology and civilians involved in their deployment.

2.2.2.2 Military Objectives and Civilian Objects

Military objectives are legitimate military targets. But what are military objectives? In recourse to the Hague Regulations on Air Warfare, Article 24, it was discussed to include an exhaustive list to the Additional Protocol, an approach that was rejected when drafting the Protocol, in favour of a general and abstract definition. AP I sets out the test criteria to assess an object as being military. Article 52(2) AP I defines:

"Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which are 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 that time, offers a definite military advantage".

As Fendrick stresses, "it remains a requirement that both elements of the definition must be met before a target can be properly considered an appropriate military target.[48] The ICRC Commentary also states: "Whenever these two elements are simultaneously present, there is a military objective in the sense of the Protocol."[49] The temporal factor of the interpretation however can be interpreted differently. Robertson for instance argues against this approach stating that for example a stock of ammunition would always be lawfully targetable as military objective. Henderson counters this argument: How could a stockpile of air–to–air–missiles meet the requirements of Article 52(2) if the enemies' whole air force is destroyed and he has no way of using the ammunition?[50] He emphasizes: "It cannot be presumed that all military targets have a military value at all times and in all conceivable circumstances."[51] Bothe, Partsch and Solf and similarly Sassoli argue for a less restrictive interpretation and a cumulative fulfilment of the two criteria.[52] Especially with new developments as for instance computer technology in mind, where the

---

[47] Prosecutor *v.* Kunarac, Kovac and Vukovic, Case No IT.96-23&23/1, 12 June 2000, A.Ch., at 57.
[48] W. Fendrick, *Attacking the Enemy Civilian as a Punishable Offense*, 2 Duke Journal of Comparative and International Law 7 (1997), at 543.
[49] Sandoz/Swinarski/Zimmerman, *supra* note 18, at 2018.
[50] Henderson, *supra* note 30, at 50.
[51] *Ibid.*
[52] *Cf.* M. Sassôli, *Legitimate Targets of Attacks under International Humanitarian Law*, International Humanitarian Law Research Initiative, Background Paper 7 (2003), www.hpcrresearch.org/sites/.../files/.../Session1.pdf (2 June 2012), at 2. *See further* Bothe/Partsch/Solf, *supra* note 30, at 325.

destruction of computer networks could benefit more on a long-term perspective, this assessment can be considered more reasonable.

The element of effective contribution is determined by the objects nature, location, purpose and use at the circumstances ruling at that time.[53] Those objects assessed as military objectives by 'purpose' or 'use' are of most interest, since they are *prima facie* civilian and become military secondary. 'Use' is defined by the ICRC as the present function[54], which means if an otherwise civilian object is utilized as military objective it becomes for that moment a military objective, as could be the case with factories currently producing military equipment, or as used by the ICTY's OTP report regarding the NATO bombings in the former Yugoslavia[55] refugee camps, where people are knitting socks for soldiers. Here one could although, maybe contrary to common sense, assess the refugee camp as military objective, although the military advantage of destruction would probably be to low to meet the proportionality test. 'Purpose' of an object is defined by the ICRC Commentary as intended future use, which could overlap with the nature-criterion in cases of military material, as are tanks by their nature and by their purpose lawfully targetable military objectives.[56] A civilian object used by the military becomes a targetable military objective for the time of its usage and regains its protected status after that. Solely that possible future military use of an otherwise civilian object is not enough to reclassify it. The ICRC Commentary refers to an intention of the belligerent to use the object in question, intention here interpreted as reasonable belief of the future use.[57]

The second classification criterion, the military advantage that the destruction generates, should be considered next. The preamble of the St. Petersburg Declaration enshrines: "The only legitimate object which states should endeavour to accomplish during war is to weaken the military forces of the enemy." And the ICRC Commentary later held: "Military advantage can only consist in ground gained and in annihilating or weakening the enemy armed forces."[58] That does however not limit the military advantage to direct effects. Associated with this issue is the debate on what effects should be taken into

---

[53] 'Nature' is associated with the inherent essence of an object, although e.g. a knife could on one side be military but also for civilian use. 'Location' refers to objects with strategic importance, e.g. bridges and as the commentary states, of limited size and in the combat area.

[54] *Cf.* Sandoz/Swinarski/Zimmermann, *supra* note 12, at 2022.

[55] The report deals with the NATO Operation Allied Forces (OAF) against the Former Republic of Yusgoslavia in 1999. Among several judicial and non-judicial initiatives to investigate the campaign, the prosecutor of the ICTY decided to establish a Committee to review accusations of violations of IHL. This report, known as the OTP report was made public in 2000. Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against The Federal Republic of Yugoslavia (OTP Report) (2000), http://www.un.org/icty/pressreal/nato061300.htm (2 August 2012), at 48.

[56] *Cf.* Sandoz/Swinarski/Zimmermann, *supra* note 18, at 2022.

[57] *Cf.* Expert Meeting, Targeting Military Objectives (2005), University Centre for International Humanitarian Law, http.://www.ucihl.org/research/military_objective_symposium_report.pdf. (3 July 2012), at 7.

[58] Sandoz/Swinarski/Zimmermann, *supra* note 12, at 2218.

account when assessing a target operation, just the direct effects caused by an attack or also later occurring consequences. Schmitt states in favour of including the latter: "Cascading effects are 'indirect effects [that] ripple through the adversary target system, often influencing other target systems as well." [59] The interpretation of Human Rights Watch strengthens the understanding, that "[the] requirement that military objectives effectively contribute to military action does not necessarily require a direct connection with combat operations"[60] as well as several other commentators: "military necessity concept includes other elements besides putting an enemy hors de combat, such as the destruction or neutralization of enemy material, restrictions of movement, weakening of resources and enhancement of the security of friendly forces."[61]

This issue often relates to a specific type of objects, the dual-use objects. They do not build a separate category in legal terms, objects are either civilian or military, but the nature of some objects makes this classification highly controversial and of importance, especially for the following chapter on cyber attacks, where military and civilian objects may not be distinguished easily.[62] "Typically [cascading effects] occur when striking targets at a higher level of conflict. For instance, damaging a national level command and control net will influence lower levels of the conflict as the ability to receive intelligence and direction from above, and to coordinate operations with other units, diminishes'." [63] Assessing whether or not to target objects used for civilian and military aims in the described manner is nowadays referred to as an effect-based theory of targeting. In classical theory, targets were attacked for the purpose of directly weakening the enemy forces. Effect-based operations contrariwise assess indirect and systematic consequences that result in, for instance attacks on power generation stations.[64] As Waxman states, "(d)istinguishing between military and civilian infrastructure is sometimes difficult and, especially with respect to support systems that provide basic needs such as electricity, it may be impossible to destroy or disrupt only those portions

---

[59] M. Schmitt, *Targeting and Humanitarian Law: Current Issues*, 34 Israel Yearbook on Human Rights 59 (2004), at 62.

[60] Human Rights Watch, Needless Deaths in the Gulf War: Civilian Casualties During the Air Campaign and Violations of the Laws of War (1991), http://www.hrw.org/reports/1991gulfwar/ (18 July 2012), at 332.

[61] Bothe/Partsch/Solf, *supra* note 30, at 196.

[62] One major example for a dual-use target as well as the subsequent debate on the legality of the attack is the 1999 NATO bombing of the Serbian radio and television station in Belgrade. It was classified as targetable objective due to the fact that parallel to its regular entertainment and news-function it was used by the Serbian armed forces to transmit commands and military intelligence. The NATO troops destroyed the building during night to minimize the number of casualties. The attacks resulted in 16 civilian deaths but the military advantage anticipated was not reached because of a secret backup transmitter located elsewhere. The Final Report to the Prosecutor revealed no *prima facie* violation of IHL since proper calculation on collateral damage and proportionality was made and precautionary measures were taken. *See* Turns, *supra* note 28, at 831.

[63] *See* Schmitt, *supra* note 59, at 62.

[64] M. Waxman, International Law and the Politics of Urban Air Operations (2000), RAND Corporation, http://www.rand.org/publications/MR/MR1175 (12 July 2012), at 20.

servicing the military. The last point is especially true when the military, generally the priority user during crisis, can be expected to utilize any residual capacity".[65] The Eritrea-Ethiopia Claims Commission considered the status of dual use objects in one of its judgments on the aerial bombardment of the Hirgigo power station.[66] The object in question was a large power plant constructed to provide power for an area that included a port and naval facilities. The destruction of the plant was ruled by the Commission to be lawful since it offered a distinct military advantage.[67] Targeting those objects reveals the importance of case-by-case assessment. General classification of objects as being just military or civilian can lead to serious violations of IHL and constant reassessment according to the actual and concrete situation is inevitable.

Targeting a lawful military objective is restricted by the principle of distinction but planning and conducting the attack is further limited by the principle of proportionality, to assess the lawfulness of possible civilian casualties. This fundamental principle will be discussed in the following section.

2.2.3 The Principle of Proportionality

The principle of proportionality affects an operation to the extent of whether the objective should be targeted, not whether it can be considered a lawful target. The principle of proportionality, also a customary law rule[68], is codified *inter alia* in Article 57(2)(A)(iii) AP I:

"Those who plan or decide upon an attack shall: (iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damages to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated".

There is no mathematical equation to calculate in numbers when an attack on an otherwise lawful target violates IHL by being disproportionate. The principle permits the causing of a certain degree of collateral damage, hereby referring to death or injury of civilians or the destruction of civilian objects. Injuring or killing combatants or destructing military objectives, no matter to which extent, is not included. Considering the military advantage that must be weighed against the collateral damage caused by an attack, only the concrete and direct military advantage must be taken into account, [69] which is assessed for the

[65] *Ibid.*

[66] Aerial Bombardment and Related Claims between the State of Eritrea and The Federal Democratic Republic of Ethiopia, Partial Award – Western Front, Eritrea-Ethiopia Claims Commission, 10 December 2005, at 34.

[67] *Ibid.*, at 34 *et seqq.* and 46.

[68] *Cf.* J.-M. Henckaerts, *Study on Customary International Humanitarian Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict*, 87 International Review of the Red Cross 857 (2005), at 187.

[69] Interestingly the interpretations of military advantage vary between the different scenarios the term is used in. A number of States made for example declarations to the interpretation of the term for the articles. Furthermore, the Rom-Statute of the ICC uses a different wording: Art. 8 (2)(b)(iv) states that incidental loss of live or injuries must not be excessive "in relation to the

operation as a whole and not for each single attack.[70] To attack is prohibited in any case in which the collateral damage would be excessive in relation to the concrete and direct military advantage anticipated. No further instruction is given by Article 57, although one can seek guidance in the extensive reference to State practice, delivered for example by Doswald-Beck and Henackerts.[71] Different values are balanced against each other in this test, which is why the, "proportionality test is quite complex to apply in practice: ideally, balancing involved comparison of like values. In the case of proportionality the values are heterogeneous".[72]

Taking these requirements into account the decision to attack is eventually made by the person in charge, as also interpreted by the ICRC Commentary: "it remains the case that the text adopted by the Diplomatic Conference largely relies on the judgment of soldiers who will have to apply these provisions."[73] The commander must decide on the basis of these information reasonably at hand. The ICTY in one of its judgment also referred to this rather subjective calculation by stating: "In determining whether an attack was proportionate it is necessary to examine whether a reasonably well informed person in the context 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."[74]And similar the OTP report on the NATO bombings: "it is suggested that the determining of relative values must be that of the 'reasonable military commander'".[75]

2.2.4 Precautionary Measures

Crystallizing from the overall notion of protecting the civilian population and balancing the different values against the military interest, the law of armed

---

concrete and direct *overall* military advantage anticipated" (emphasis added). Already in 1998 the ICRC however publicly declared that "*the addition of the words 'clearly' and 'overall' in [the] provision relating to proportionality in attacks must be understood as not changing existing law*. The word "overall" could give the impression that an extra unspecified element has been added to a formulation that was carefully negotiated during the 1974–1977 Diplomatic Conference that led to [Additional Protocol I] and this formulation is generally recognized as reflecting customary law. The intention of this additional word appears to be to indicate that a particular target can have an important military advantage that can be felt over a lengthy period of time and affect military action in areas other than the vicinity of the target itself. As this meaning is included in the existing wording of the 1977 Additional Protocol I, *the inclusion of the word 'overall' is redundant*" (emphasis added), ICRC, Statement at the UN Diplomatic Conference of Plenipoteniaries on the Establishment of an International Criminal Court, 8 July 1998, UN Doc. A/Conf.183/INF/10, 13 July 1998, at 1.

[70] *Cf.* A. Laursen, *NATO, the War over Kosovo, and the ICTY Investigation*, American University International Law Review 17 (2002), at 795.

[71] *Cf.* J.-M. Henckaerts/L. Doswald-Beck (Eds.), Customary International Humanitarian Law (2005), at 299 *et seq.*

[72] Kellenberger, *supra* note 2 and OTP Report, *supra* note 55, at 19.

[73] *Ibid.*

[74] Prosecutor *v.* Galic, Decision on the Motion for the Entry of Acquittal of the Accused Stanislav Galic, Case No IT-98-29-T, 5 December 2003, T.Ch. II, at para. 58.

[75] OTP Report, *supra* note 55, at 50.

conflict imposed another obligation on the parties to the conflict: To take all feasible precautions.

As discussed under subsection 2.2.2.2., a target must be a military one to attack, but it must secondly, be attacked in a lawful manner. Therefore, Article 57 stipulates the obligation to take precautions and lists specific precautions that must be adhered to when planning and executing the attack itself. Those measures listed are, to spare civilian casualties, to do everything feasibly to verify the military status of the target, avoid or minimize collateral damage, cancel or suspend attacks if circumstances change, warn the civilian population and chose the targets with less danger to civilians.[76]

2.2.5 Martens' Clause

"Until a more complete code of laws of war has been issued, the High Contracting Parties deem it expedient to declare that, in cases not included in the Regulations adopted by them, the inhabitants and the belligerents remain under the protection and the rule of the principles of the law of nations, *as they result from the usage established among civilized peoples, from the laws of humanity, and the dictated of the public conscience*".[77]

Although being rather abstract and open to various interpretations, the clause has been assessed as a source of obligation based on humanitarian consideration, one that it restricts the conduct of hostilities in a general way.[78] It has been quoted repeatedly in international treaties[79], renowned judgments and advisory opinions, as for instance the *Nicaragua* and *Legality of the Threat or Use of Nuclear Weapons* Cases of the ICJ[80] and several national military manuals.[81]

The wording of the clause allows for the possibility of a legal rule of customary character, not based on State practice and *opinio juris*, but on a moral foundation. Three major lines of argumentation concerning the legal value of the clause can be identified already in early scientific debate – apart from those

---

[76] *Cf.* Henderson, *supra* note 30, at 230.

[77] Hague Convention (IV), preamble (emphasise added). Firstly introduced was the Martens' clause by Russian publicist Fyodor Martens at the 1899 The Hague Peace Conference, leading to its insertion to the preamble of the Hague Convention II and its successor, the Hague Convention IV; *See* T. Meron, *The Martens Clause, Principle of Humanity, and Dictates of the Public Conscience*, The American Journal of International Law 94 (2000), at 78.

[78] *See* A. Cassese, *The Martens Clause: Half a Load of Simply Pie in the Sky?*, European Journal of International Law 11 (2000), at 188.

[79] As for instance, albeit in differing wording, the 1949 Geneva Conventions for the Protection of Victims of War, the 1977 Additional Protocols and the preamble to the Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons.

[80] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua *v.* United States), Merits, ICJ Reports 1986, at para. 218; Nuclear Weapons Advisory Opinion, *supra* note 6, at para. 79.

[81] As for instance the U.S. manuals, *see* Field Manual No 27-10 (1956), Department of the Army, at para. 6; Similarly the military manual for the German armed forces, Federal Ministry of Defence, *Humanitarian Law in Armed Conflict - Manual*, 2 Zentrale Dienstvorschrift 15 (1992), at para. 129.

denying that it has any effect at all.[82] Commentators as Schwarzenberg[83] and Binz[84] argue for a minimal significance of the clause, as means to interpret international principles and rules in cases of doubt. The second major trend emphasizes the importance of the clause with regard to the sources of IHL, arguing for the creation of two new sources for legal obligations, humanity and dictates of the public conscience. This view was represented *inter alia* by Bernard V. A. Röhling.[85] The third group of scholars thought of the clause as incorporating driving values that motivate and inspire the evolution of international humanitarian law, as laid down by Lord Wright in the Foreword to Volume XV of the Law Reports of Trials of War Criminals.[86] Despite its ambiguity the clause has, according to Cassese, responded to "a deeply felt and widespread demand in the international community: that the requirements of humanity and the pressure of public opinion be duly taken into account when regulating armed conflict".[87]

Nonetheless, one can question its actual relevance with regard to the specific issue of targeting. The Geneva as well as the Hague Law, especially keeping the precise regulations of the Additional Protocol I in mind, build a complex legal framework, that covers contemporary targeting issue in detail. And as one reads the clause' restatement in the AP I, Article 1(2), "*in cases not covered by this Protocol or by other international agreement*, civilians and combatants remain under the protection […]" (emphasis added), the clause will become decisive only if the other instruments fail. Regarding the application of IHL to modern technologies, the Martens' Clause therefore contributes as a moral imperative rather than a foundation of concrete and precise regulations.

---

[82] *Cf.* B. Brown, *The Proportionality Principle in the Humanitarian Law of Warfare: Recent Efforts in Codification,* Cornell International Law Journal 10 (1976), at 136.

[83] G. Schwarzenberg, The Legality of Nuclear Weapons (1958), at 10 *et seq.*: "This clause was not meant to settle with binding force for the Parties […] how rules of warfare came into existence. Its only function was to preserve intact any pre-existing rules of warfare […]". *Similar* R. Abi-Saab, *The Specifications of Humanitarian Law*, in C. Swinarski (Ed.) Studies and Essays on International Law and Red Cross Principles in Honour of Jean Pictet (1984), at 274-275.

[84] G. Binz, *Die Martens`sche Klausel*, Wehrwissenschaftliche Rundschau-Zeitschrift für die Europäische Sicherheit (1960), at 160.

[85] B. Röhling, International Law in an Expanded World (1960), at 37 *et seq.* and H. Strebel, *Martens Clause*, in R. Bernhard (Ed.), Encyclopedia of Public International Law (1997), at 327; J. Von Bernstorff, Martens Clause (2009), http://www.mpepil.com/subscriber_article?Script=yes&id=/epil/entries/law-9780199231690-e327&recno=1&searchTyoe=Quick&query=martens+clause (2 August 2012).

[86] Lord Wright, Foreword. Law Reports of Trials of War Criminals, Volume XV, www.loc.gov/rr/frd/Military_Law/pdf/Law-Reports_Vol-15.pdf (2 August 2012), at xiii.

[87] Cassese, *supra* note 78, at 212.

3. Current Trends in Military Technology: Unmanned (Combat) Aerial Vehicles

The use of, what is often referred to by the common sense as drones, unmanned aerial vehicles, has shaped last decades armed conflict and military strategy to a great extent. Highly criticised by the public as well as human rights lawyers and activists, the use of drones to conduct targeted killings surrounding the globally declared 'war on terror' raises questions about their legality under international law.[88] But what about the deployment of UCAV/UAVs during an armed conflict, where the conduct of the parties involved is guided by the principles and rules of IHL? One has to clearly distinguish between the different fields of international law as well as deployment scenarios at this point: Those concerns of the public, politicians and the human rights movement must be understood in context of the deployment as a means to conduct targeted killings, often outside of an armed conflict situation and therefore outside of the application of IHL. Domestic Law and the human rights framework as *lex specialis* in this scenario may then very well be applied to ask under which or any circumstances it is lawful to kill the designed target at all and in use of drones, since the use of lethal force in times of peace is limited to highly restricted situations and governed by a different set of rules.[89]

This master thesis focuses on modern military technology from a different angle, that of a IHL, accordingly a different set of questions will be raised. For this purpose, the following chapter will, after a clarification of terms, examine the major legal principles relevant to their use in armed conflict.[90] The question at stage is the following: Is the deployment of drones *per se* or under specific circumstances violating the law applicable in armed conflict?

---

[88] The use of drones in Pakistan for example is one of these legal grey areas or even considered to be illegal by renowned scholars and has to be assessed by human rights standards. *See on the debate for instance*, G. Blum/P. Heymann, *Law and Policy of Targeted Killing*, 1 Harvard National Security Journal 145 (2010); P. Rudolf/C. Schaller, *Targeted Killing. Zur völkerrechtlichen, ethnischen und strategischen Problematik in der Terrorismus- und Aufstandsbekämpfung*, SWP-Studie 1 (2012); M. Schmitt, *Targeted Killing in International Law*, 4 American Journal of International Law 103 (2009); M. Llezna, *Targeted Killings in Pakistan: A Defense*, 2 Global Security Studies 2 (2011).

[89] At least if one does not consider Pakistan a party to the conflict in Afghanistan and Pakistan territory not conflict territory. There are, however, commentators suggesting an expansion of the conflict due to spill-over-effects and they consider IHL applicable also in the broader context and therefore would also assess the targeted killings of alleged terrorists in Pakistan under IHL and not only human rights law. *See for instance*, M. Schmitt, *Ten Years in Appraising the International Law of the 'Long War' in Afghanistan and Pakistan: Unmanned Combat Aircraft Systems and International Humanitarian Law*, Boston University International Law Journal 30 (2012); L. Blank/B. Farley, *Characterizing United States Operations in Pakistan: Is the U.S. Enganged in An Armed Conflict?,* Fordham International Law Journal 34 (2010); N. Lubell, *Parallel Application of International Humanitarian Law and International Human Rights Law: An Examination of the Debate*, Israel Law Review 40 (2007).

[90] Since this is a thesis written in international law the chapter itself will only discuss the subject from a legal point of view. Additional Informationen on types and deployment scenarios can be found annexed to this text.

3.1 Definition and Clarification of Terms

As in the case of most modern high technologies, unmanned vehicles (UVs) consist of a wide range of divergent systems, differently equipped and designed for different terrains and purposes – an exact classification and definition is therefore rare to find, nonetheless it is essential to clarify their legal status and to address them under IHL and public international law.

UVs in general may be considered as vehicles that operate without physical contact to its controller. Highlighting their different purposes and theatres of operations, modified acronyms are used to distinguish between them.[91] This thesis will concentrate on two distinctive types of unmanned vehicles and constantly use the following terminology: The unmanned aerial vehicle (UAV) and its weaponised counterpart, the unmanned combat aerial vehicle (UCAV), while for example the unmanned ground vehicle (UGV) and its waterlogged siblings, the unmanned (water) surface as well as the unmanned underwater vehicle (USV/UUS) will be left for another analysis.

In this thesis, UAV will be understood as defined by the HPCR-Manual[92], rule 1(dd), as "unmanned aircraft of any size which does not carry a weapon and which cannot control a weapon."[93] UCAV on the other side is defined by the same provision, rule 1(ee), as "an unmanned aerial military aircraft of any size which carries and launches a weapon, or which can use on-board technology to direct such a weapon to a target".[94]

3.2 Types of UCAVs and UAVs

In academia and among military personnel it is common to divide contemporary types of UCAV/UAVs into three main classes in accordance with their technological design: high altitude and long endurance, medium altitude, micro and small.[95] High altitude and long endurance (HALE) UAVs fly at altitudes of at least 9km and are predominantly used for wide area and long term surveillance, reconnaissance and target acquisition,[96] since they operate outside of most air defence systems.[97] Models like the RG-4 Global Hawk, the largest of

---

[91] Others refer to it as for instance Unmanned Aerial Systems, *see* R. Newman, *The Little Predator That Could*, 3 Air Force Magazine 85 (2002).

[92] The Manual itself, *see infra* note 93, is not a binding documents but it is a comprehensive project to restate the existing and binding international law, customary as well as treaty law, applicable to air and missile warfare and is therefore considered to mirror the prevailing view.

[93] Program on Humanitarian Policy and Conflict Research at Harvard University, Manual on International Law Applicable to Air and Missile Warfare (2009), rule 1 (dd), ihlresearch.org/amw/HPCR%20Manual.pdf (10 July 2012), at 16.

[94] *Id.*, rule 1(ee).

[95] *Cf.* B. Gogarty/M. Hagger, *The Laws Of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air*, Journal of Law, Information and Science 19 (2008), at 86.

[96] *Id.*, at 88.

[97] *Ibid.*

its type with 12 meter length and capable of flying for 35 hours at up to 20000 meters fall into this category.[98]

The medium altitude category operates at heights comparable to those of commercial aircrafts and includes UAVs providing combat functions. The weaponised counterpart of the UAVs, the UCAV, may as well be used for higher altitude reconnaissance missions, but its major purpose is to conduct lethal strikes most commonly against individuals.[99] Today a wide spectrum of different models, equipped with infrared- and night-vision systems, laser designation and armed with missiles are in use and constantly enhanced. To provide combat function they are usually equipped with the hellfire-missile, a long-range supersonic missile that is designed for precise attacks and able to strike against heavy armour.[100] The US MG-1 Predator is possibly the most prominent version of a UCAV, around 17 meters and capable of staying in the air for 24 hours at up to 8000 meter. [101] Its current successor is the second generation Predator B, known as Model MG-9 Reaper. Various other models exist, such as the Shadow or the Hunter, with varying degrees of technology and different deployment scenarios.[102]

Comparable in size to a model aircraft are the UAVs of the micro and small category, which are typically of around 1-3 meter length, and to be launched by hand or a catapult. Examples are the RG-11 Raven, one of smallest types, with a wingspan of merely 1,5 meters, which weights around 2 kilogrammes and can stay airborne for merely 90 minutes. The Raven is solely undercut by the even smaller Wasp. Those types of UAVs are often in use by ground units to deliver short range data and employed in scenarios outside of armed conflict in domestic law enforcement missions as for instance delivering surveillance data on demonstrations, in customs or border control.[103]

The aircraft itself, UCAV or UAV, builds one part of an integrated system, supported by a ground station and a satellite communication suite.[104] Within a short period of time, the former can be rapidly deployed while its human operators remain at their location. The aircrafts fly on flight routes that have been programmed prior to deployment or a manually controlled. In comparison

---

[98] *Cf.* NASA Fact Sheet (22 March 2012), http://www.nasa.gov/centers/dryden/news/FactSheets/FS-098-DFRC.html; US Air Force Fact Sheet (21 January 2012), http://www.af.mil/information/factsheets/factsheet.asp?id=13225 and http://www.globalsecurity.org/intell/systems/global_hawk.htm (All seen on 8 July 2012).

[99] *Cf.* M. O'Connell, *Unlawful Killing with Combat Drones. A Case Study of Pakistan, 2004-2009*, Notre Dame Law School Legal Studies Research Paper 7 (2010).

[100] R. Braybrook, *Strike Drones: Persistent, Precise and Plausible*, Armada International 4 (2009), at 21; M. Franklin, Future Weapons Foe Unmanned Combat Air Vehicles, RUSI Defense System (2008), at 94; Fact Sheet, http://www.lockheedmartin.com/us/products/HellfireII.html (8 July 2012).

[101] *Cf.* Gogarty/Hagger, *supra* note 84, at 83. *See* for more information also, General Atomics, http://www.ga-asi.com.

[102] *See* Vogel, *supra* note 107, at 104.

[103] *Ibid.*

[104] *Cf.* P. Singer, Wired For War (2009), at 386.

to the field of automated weaponry and robotics, a man in the loop, a human operator, is – at the current stand - still necessary to operate this technology.[105]

3.3 Deployment of UCAVs and UAVs

Military technology has been advancing rapidly over the last decades with States or private corporations inventing weapons more accurate and precise or with more firepower than previous generations. Over the last years a slightly different aspect accompanied this evolution. Last decade's technological developments in and goals of warfare circled around the idea of withdrawing human soldiers step by step from the battlefield and replace them to varying degrees through technology. Automated weaponry may for some be the envisaged final objective, but at this point the use of UCAV/UAVs in a majority of today's armed conflicts is far more prominent.[106]

The use of UCAV/UAVs caused a major change in contemporary combat, as Boor states, revolutionising it.[107] And as Newman states, the development of drones, especially the predator model, has been an instant hit. He specially refers to the high quality live video transmission they deliver. UCAV/UAVs deliver footage of enemy action to commanders on the ground and aircrews above the battlefield as well as for illuminating targets for attacks.[108] The risk for one party`s own troops is diminished while for example surveillance over the opponents territory or in areas without ground support is rather simple. For these benefits they can be considered so-called force multipliers, delivering a much wider perspective over the battlefield than former technology was able to.[109] One other non-technological major factor to consider is that they are relatively low priced, at least in comparison to manned aircrafts.[110] Therefore it is not surprising that around 40 States are using UCAV/UAVs today, a number that will, without doubt, further increase. According to Peter Singer, during the Iraq War in 2003, which was one of the defining conflicts of 21st century, the UN mandated allied forces did not deploy any UCAV/UAVs at all. Only ten years later, so the expert, over 8000 UCAV/UAVs are used in all different parts of the world.[111]

The deployment of different kinds of methods or means of warfare directly influenced requirements placed on persons involved in their deployment. Since human soldiers are increasingly removed from the conflict theatre, they will

---

[105] *Cf.* M. McNab/ M. Mathews, *Clarifying the Law Relating to Unmanned Drones and the Use of Force: the Relationship between Human Rights, Self-Defence, Armed Conflict and International Humanitarian Law,* Denver Journal of International Law and Policy 39 (2010-2011), at 664.

[106] *See* D. Gormley, *New Developments in Unmanned Air Vehicles and Land-Attack Cruise Missiles*, SIPRI Yearbook (2003), at 409.

[107] *Cf.* F. Boor, *Der Drohnenkrieg in Afghanistan und Pakistan*, 2 Humanitäre Informationsschriften 24 (2011), at 97 *et seq.*

[108] *Cf.* Newman, *supra* note 80, at 48.

[109] *Cf.* US Army Centre of Excellence, Eyes of the Army: US Army Roadmap for UAS 2010-2035 (2010), Report No. ATZQ-CDI-C-72, http://www.fas.org/irp/program/collect/uas-army.pdf (12 July 2012).

[110] *See* O'Connell, *supra* note 88 and Boor*, supra* note 96, at 97.

[111] *Cf.* Singer, *supra* note 93, at 61.

have to fulfill different requirements and bring a different set of skills compared to the traditional soldier: the ability to digest huge amounts of data and information in a very short time, to be able to operate on computer consoles for hours is replacing conventional criteria as physical fitness and combat techniques.[112] Geographical distance and the different manner of physical involvement in hostilities is on the one hand an advantage with regard to the soldiers' wellbeing but on the other hand, it brought up a new kind of risk, associated with this development and especially the deployment of UCAVs. Not only Alston and Shamsi, but an extensive community within the academia, warned of the so called playstation-mentality.[113]

Nonetheless, the broad range of advantageous factors convinces military sectors and governments worldwide to increase their purchase of UCAV/UAVs.[114]

3.4 Legal Framework Governing the Use of UCAV/UAVs

The legal framework of IHL concerning the methods and means of warfare and especially those concerning targeting has been examined in the previous chapter. In times of combat, decisions are often made in a hurry and with limited information at hand. It is often afterwards, that military decisions are being examined regarding their compliance with the binding law. In the following the principles and rules of IHL will be applied to UCAV/UAVs to determine their status and the legality of their use during armed conflict.

3.4.1 Status of UCAV/UAVs under International Humanitarian Law

Why is it essential to clarify the status of UCAV/UAVs under IHL? If one analyses the principles and norms regulating hostilities and targeting then it is

---

[112] *Cf.* Gogarty/Hagger, *supra* note 84, at 99.

[113] For a legal analysis of UCAVs deployment under IHL, this issue of playstation-mentality is merely a sideliner, dominantly discussed in the neighbouring discipline of political- and social science and peace and conflict research, but should at least in short be mentioned due to its prominence. The UCAV operators mostly recruited over the last years and raised as a generation of videogame players, could be at risk to devalue the life of possible targets due to the schematic presentation of the combat scenario on computer screens, so the accusation. One has to ask if the fact, that their distance from actual fighting, sitting in containers thousand kilometres afar, makes them more prone to forget about the consequences to their actions. Do they become too unaffected due to this advanced technology? These concerns where raised over the last years when it became known that strikes against Al-Qaeda members in different countries all over the world were controlled from Nevada or the CIA Headquarters in Langley and even more when picture and videos, comparing videogames and UCAV-controllers screens were made public. These considerations are however predominantly of sociological or psychological character. Ethical explorations maybe necessary in the future with regard to the expansion of remotely controlled weapons and even more automated weaponry but have, at this point, not shifted the military affinity to this discussed technology or legal considerations on their use.

[114] *See for instance* on the decision of the German Bundeswehr to purchase UCAVs, D. Kurbjuweit, Smarter Sensemann, Deutschland will Kampfdrohnen anschaffen. Sind sie eine humane Waffe?, Der Spiegel 32, 06 August 2012 and N.S., Bundeswehrverband drängt auf Beschaffung von Drohnen, Focus, 25 September 2010, http://www.focus.de/politik/deutschland/verteidigung-bundeswehrverband-draengt-auf-beschaffung-von-drohnen_aid_826082.html (25 September 2012).

necessary to determine who and what might be considered a legitimate target and with what means the enemy combatant or military objective might be targeted. The question, which of the principles and rules discussed in chapter 2, are applicable is linked to the status of UCAV/UAVs under IHL. To determine their status one can resort again to the Program on Humanitarian Policy and Conflict Research of Harvard University that publishes a highly renowned Manual on International Law applicable to air and missile warfare in 2009.[115]

The distinctive feature of a UCAV/UAV is the "U". UCAV/UAVs fly self-propelled and unmanned, mostly to destroy or kill targets chosen prior to their launch. Therefore, they could be compared to weapons, as for instance missiles.[116] "Missiles, when cruising, do not derive support from reaction with air, which aircrafts do."[117] But a UCAV's purpose is redeployment. It is not designed to be only used once, as do missiles. And UCAVs are equipped with a specific missile, carrying it to its target location, which already indicates a distinction between the UCAV as a carrier or platform for a certain type of weapon, as Boothby highlights.[118] If the UCAV itself is not the weapon that causes those injuries[119], but merely the vehicle controlling the weapon and therefore only causing the injury indirectly, by virtue of Rule 1 (ff), the UCAV itself has to fall into another category.[120]

Furthermore, UCAVs are being able to a controlled landing as well as multiple deployments and herewith share undeniable similarities to aircrafts.[121] For the application of the relevant provisions of IHL one further has to determine whether UCAVs fit the criteria of military aircraft rather than a civilian airplane. This distinction is important, as different rules apply to military aircrafts, as enshrined in Article 13 of the Draft Hague Air Rules of 1923, as

---

[115] *Cf. Supra* note 93.

[116] "'Missiles' mean self-propelled unmanned weapons — launched from aircraft, warships or land-based launchers — that are either guided or ballistic", HPCR-Manual, rule 1 (z).

[117] B. Boothby, *The Law Relating to Unmanned Aerial Vehicles, Unmanned Combat Air Vehicles and Intelligence Gathering from the Air*, 2 Humanitäre Informationsschriften 24 (2011), at 82.

[118] *Cf. Ibid.*

[119] As required by the definition of HPCR Manual, rule 1 (ff).

[120] An exception one can imagine is cases in which UCAVs for example by crashing into an objective or people are used to cause injuries or damage directly. This then could also include UAVs, as they too could be used in such a manner. But even for this scenario, the HPCR manual rejects UCAVs/UAVs to fall into the weapons category; Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare (2010), http://www.ihlresearch.org/ *(15 July 2012)*, rule 1 (t). For the application of the provision on means and methods of warfare, one can nonetheless subsume UCAVs, although not a weapon but a carrier, in the control of an attacking party, as a means of warfare and therefore subject of the respective provisions.

[121] Following rule 1(d)., aircrafts are defined as "any vehicle whether manned or unmanned – that can derive support in the atmosphere from the reaction of the air (other than the reaction of the air against the earth's surface, including vehicles with either fixed or rotary wings.)." Therefore helicopters and airplanes, vehicles using aerodynamic, as well as balloons or airships, using aerostatic powers, can be considered aircrafts.

only a "military aircraft are alone entitled to exercise belligerent rights".[122] Merely the possibility to deploy weapons, as for instance the hellfire-missile from the UCAV, does not qualify for military aircraft. There are other conditions to be fulfilled, laid down by customary international law and enshrined in rule 1 lit (x) HPCR-manual: "Military aircraft" means any aircraft (i) operated by the armed forces of a State; (ii) bearing the military markings of that State; (iii) commanded by a member of the armed forces; and (iv) controlled, manned or pre-programmed by a crew subject to regular armed forces discipline." If the respective national and military identifications are applied, the human criteria becomes problematic. *Per definitionem* there is no crew subject to regular armed forces disciplines. Therefore the requirements of (iii) commanded by and (iv) controlled or pre-programmed by a member of the armed forces is of even more importance.[123] At this point one realises that one cannot generalise, but has to assess the status of UCAVs in cases of doubt on a case-by-case analysis.

Foreseeing future developments in UCAV/UAV-technology and the increase in automated decision-making processes it is inevitable to reconsider this classification in the future. But for the time being and having considered the relevant counterarguments UCAV/UAVs should be considered military aircrafts in accordance with the HPCR manual and only in exceptional cases as weapons. Whether they actually launch a weapon or are unarmed does not change their status as military aircraft and therefore as legitimate target for the adversary.[124] If the UCAV can be considered a military aircraft, it is bound by different restrictions, as it has for instance no overflight rights over foreign territory in times of peace or at any times with regard to territory of States not party to the conflict. Not being a weapon but a military aircraft they are furthermore State property and for instance after being taken down, they would have to be returned to the ownerstate after the end of the conflict.[125]

The following subsections will concentrate to a greater extent on those rules concerning targeting and applicable to UCAVs. UAVs will be assessed if necessary.

---

[122] Further rights are associated with this status as for example sovereign immunity or overflight rights; *See* R. Frau, *Unbemannte Luftfahrzeuge im internationalen bewaffneten Konflikt*, 2 Humanitäre Informationsschriften 24 (2011), at 64.

[123] The development of advanced technology opened the military sector to varying degrees to civilian personnel. There easily might be scenarios in which the UCAVs` flightroute is programmed by a civilian manufacturer. Could the UCAV nonetheless be considered a military aircraft, entitled to engage in combat or has it lost its legitimacy to do so? Frau suggests the following approach: The UCAV operator has to be military personnel to still consider it a military aircraft that enjoys the associated rights. Other personnel, as for example those responsible for fuelling or maintaining the UCAV, will not change the status of the UCAV but rather be an issue that must be considered under the principle of distinction and a direct participation in hostilities of the civilians involved.

[124] If UCAVs/UAVs without military status, as they are for instance not marked with the respective military and national identifications, are deployed, on might considerer to apply the rules for espionage. Espionage according to Art. 30 Hague Convention IV is not prohibited by IHL.

[125] Frau, *supra* note 102, at 64.

3.4.2 The Principle of Humanity

The principle of humanity, balancing justifications of military necessity, was the shaping element for IHL, restricting the conduct of the parties involved in the armed conflict by limiting the amount and type of use of legitimate force.[126] UCAV/UAVs as tools used by the parties *per se* are not violating this principle, as there has been no evidence that UCAV strikes cause any more injury or suffering for the respective target than traditional forms of attack.[127]

However the growing critique and concerns mirror the fear that lethal UCAV strikes may be used instead of a more humane option, for example capture and detention.[128] That is correlated to the fact that UCAV/UAVs have shown difficulties up to an inability to react to a surrendering target– or if given the order to abort at the latest stages of deployment, in accordance with the requirements of Article 57 AP I. [129] Furthermore, some other practical challenges have been used to cast doubt on their legitimacy: How can a UCAV, flying over hostile territory without any ground support, inform an *hors de combat* enemy to stay put until he or she is picked up by members of the armed forces? Although this criticism is legitimate, one has to keep in mind that it is not unique to UCAVs but may also be directed at traditional manned aircrafts whose targets for instance do not have a chance to surrender once the bombs are dropped. This is in both cases not considered to violate the principle of humanity.

3.4.3 The Principle of Distinction

The following subsection will focus on the principle of distinction and its relevance for targeting operations, hereby considering the targets themselves as well as those involved in the operations.

3.4.3.1 Regulations Concerning Targeting

Reflecting customary law, Article 48 AP I requires all parties to a conflict at all times distinguish between the civilian population and combatants, and between civilian objects and military objectives, as previously discussed in detail under 2.2.2. To adhere to the requirements of the principle of distinction strikes must always be discriminately. Following the definition of Gutman and Kuttab, this

---

[126] *See* chapter 2.2.1.

[127] *Cf.* R. Vogel, *Drone Warfare and the Law of Armed Conflict*, Denver Journal of International Law and Policy 39 (2010-2011), at 128.

[128] *See for instance*, K. DeYoung/J. Warrick, Under Obama, More Targeted Killings than Captures in Counterterrorism Efforts, Washington Post, 14 February 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/13/AR2010021303748.html?nav = emailpage (16 July 2012); R. Murphy/J. Radsan, *Due Process and Targeted Killing of Terrorists*, Cardozo Law Review 31 (2009), at 406 *et seq.*

[129] *Cf.* P. Singer, *Military Robots and the Laws of War*, The New Atlantis 25 (2009), at 37.

means: "An indiscriminate attack can be described as one in which the attacker does not take measures to avoid hitting non-military objects."[130]

In accordance with the regulations on targeting discussed above, IHL offers some more distinct rules specifically addressing airstrikes that should be mentioned here. Article 25 Hague Convention IV prohibits aerial bombardments by whatever means of undefended towns and Article 26 requires commanders to do all in his power to warn authorities before an aerial bombardment. Since the provisions regulate the conduct of aerial bombardment by any means, UCAV strikes will also be covered by these articles. The 1923 Hague Rules Concerning the Control of Wireless Telegraphy in Time of War and Air Warfare, also considered to reflect customary law, similarly established a number of provisions one can apply to targeting by UCAVs.[131] If ever used in any of the scenarios listed in the Article, UCAVs would violate the principle but that has not been the case yet and is probably not to be expected.

The UCAV itself is rarely used as a weapon itself but merely as the carrier for the respective weapon. The Hellfire-missiles launched to conduct the strikes are precision-weapons, following the laser designation of their target. In itself the missile is clearly able to comply with the distinction requirements, since it does not have undiscriminating effects. With a blast radius ranging from 3-5 meter, it can be considered highly discriminating and therefore in compliance with the principle.[132]

During the execution phase, the deployment is unlawfully if directed or indiscriminately launched at civilians or civilian objects or otherwise protected property or sites. However that concerns the use or misuse of the UCAV rather than the technology itself. In cases of misinformation, if following the launch, the person or object is found to be an unlawful target the attack must immediately be aborted. That is why ground informants are often used on side to confirm the identity of the respective target. Furthermore the technological advantages of UAVs and UCAVs must be taken into account: The UCAV itself or additional data of other UCAV/UAVs deliver rather accurate information on targets due to their surveillance technology. Supporters argue their ability to fly over the designed target for hours or even days and to perform strikes of highest precisions and accuracy make them a serious alternative to other types of aerial warfare. P.W. Singer states: "unmanned systems seem to offer several ways of reducing the mistakes and unintended costs of war, including by using far better sensor and processing powers […] allowing decisions to be made in a more deliberate manner and remov(ing) the anger and emotions from the humans behind them."[133] This was confirmed in a similar manner by US experts as for

---

[130] R. Gutman/D. Kuttab, *Indiscriminate Attacks*, in: R. Gutman/D. Rieff/A. Dworkin (Eds.), Crimes of War: What the Public Should Know (2007), at 239 *et seq.*

[131] *Cf.* Boothby, *supra* note 97, at 82.

[132] *Cf.* M. Schmitt, *Precision Attack and International Law*, 87 International Review of the Red Cross 859 (2005), at 445; J. Weiner, *Targeted Killings and Double Standards*, Strategic Perspectives 9 (2012), at 24.

[133] Singer, *supra* note 109, at 40.

example Koh, highlighting that procedures and practices for identifying lawful targets are extremely robust, and advanced technologies have helped to make targeting even more precise.[134] However, that does not mean that civilian casualties in life and property have never been caused by UCAV strikes, especially if conducted in civilian settings. Just recently, in September 2012, the "Living under Drones: Death, Injury and Trauma to Civilians from US Drone Practices in Pakistan" – report assessed this in detail. The International Human Rights and Conflict Resolution Clinic of Stanford Law School in cooperation with the Global Justice Clinic at New York University researched for nine month, interviewing witnesses and victims, reviewing media reports and documentation, on the negative impacts of the drone deployment on Pakistani people, an impact that must be considered much stronger than publicly admitted by governments using the technology.[135]

Whether the principle is adhered to during planning and execution is depending upon commanders and operators. As long as they conduct these strikes with care and precaution UCAVs offer a possible means to conduct the operation while reducing the risk of collateral damage.

3.4.3.2 Status of Persons Involved in UCAV-Strikes

The potentially most controversial or complex issue regarding the principle of distinction is the status of the personnel engaged in a UCAV-strike. The status of the operator is legally not problematic if he/she is military personnel. But most prominently discussed and legally problematic are cases in which UCAVs are operated by civilian personnel to perform combat functions, as it obviously has been the case with CIA personnel.[136] By virtue of Article 4 GC III, this personnel, even with a broad interpretation of the article, does not meet the requirements of being either a lawful combatant, member of a militia or volunteer corps. Therefore, the operator, in control of the UCAVs action, is unprivileged to conduct hostilities and in breach of IHL regulations, similarly assessed by the Israeli High Court of Justice and renowned scholars like Dinstein.[137] For the case of a civilian operator it is uncontroversial to assess his/her conduct as an unlawful direct participation in hostilities, losing his/her protection of Article 51(3) AP I. But less obvious are scenarios in which civilians are not controlling the UCAV, but conduct support works as for example,

---

[134] *Cf.* H. Koh, Keynote Address at the American Society for International Law Annual Meeting: The Obama Administration and International Law (21 March 2010), http://www.state.gov/s/l/releases/remarks/139119.htm (12 July 2012).

[135] International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at NYU School of Law, Living under Drones: Death, Injury, and Trauma to Civilians from the US Drone Practices in Pakistan (2010), http://livingunderdrones.org/download-report/ (3 October 2012), at vi.

[136] *See* Vogel, *supra* note 107, at 139; J. Mayer, The Predator War. What are the Risk of the CIA's Covert Drone Program, New Yorker, 26 October 2009, http://www.newyorker.com/reporting/2009/10/26/09102
6fa_fact_mayer (28 June 2012).

[137] *See* Public Committee against Torture in Israel *v.* Government of Israel *et al.*, High Court of Justice 769/02, Judgment of 13 December 2006, at para. 33; Dinstein, *supra* note 21, at para. 371.

fuelling, programming flight routes, and maintaining. At this point one has to differentiate. The ICRC was always working with an approach based on a single step causation, i.e. the respective conduct leads "in one causal step"[138] to the impairment. The Third Expert Meeting on the Notion of Direct Participation in Hostilities in 2005 challenged this approach, highlighting that modern warfare technology is often too advanced and in need of multiple technicians and personnel conducting different steps in for instance the launch of a UCAV:

"It has to be recognized that the contemporary reality of warfare involves a multitude of personnel and very complex weapons systems controlled by computer systems that have in turn been programmed in advance by computer specialists." […] In addition to the individual guiding the aircraft, there may well be an individual illuminating the target, and guidance may be received from another platform, an AWACS aircraft flying overhead with various individuals performing various functions. Thus, the *question of uninterrupted linkage* could become very complex."[139]

The direct linkage between the conduct and the consequences in cases like these may not be effectively assessed by a single-step-approach. The ICRC already acknowledged the inadequateness of the approach and broadened it, now including all conduct that is "integral" for causing the envisaged harm.[140] Going back to the examples, programming flight routes, fuelling the vehicle or other measures necessary for deployment, including servicing and landing, the ICRC and the HPCR manual as well as commentators like Dinstein agree, would amount to a direct participation in hostilities, as they are preparatory and aim at causing the envisaged harm.[141] In contrast to these, follow up measures will not amount to a direct participation, missing a causation linkage.[142] However, civilians engaging in the latter, risk to become part of a legitimate collateral damage, not violating Article 51(4)(b) AP I.[143]

3.4.3.3 Status of Persons Involved in UAV-Flights

The unarmed UAV is deployed for information gathering and surveillance, activities not always directly linked to causing harm, but nonetheless legitimate conduct of warfare: "the employment of measures necessary for obtaining information about the enemy and the country are considered permissible."[144] On one hand, the civilian involvement in information gathering and surveillance might be considered to indirect to causing harm and therefore not a direct

---

[138] ICRC, Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (2009), at 55.

[139] Third Expert Meeting on Direct Participation in Hostilities, Summary Report (2005), at 35 (emphasis added).

[140] *Cf.* M. Schmitt, *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, Harvard National Security Journal 1 (2010), at 27.

[141] *Cf.* HPCR Manual rule 29 (v)-(xii); Dinstein, *supra* note 21, at para. 371.

[142] *Cf.* ICRC, *supra* note 118, at 66.

[143] *Cf.* C. DeCock, *Counterinsurgency Operations*, in: M. Schmitt/T. McCormack/L. Arimatsu (Eds.), Yearbook of International Law (2010), at 112.

[144] Hague Convention IV, Art. 24.

participation in hostilities. But on the other hand, their conduct often leads to the intended military goal since single strikes as well as whole operations are build on information delivered by UAVs. It can be understood in light of the interpretation on direct participation in hostilities, also in comparison to the civilian involvement discussed in the previous chapter, that a civilian controlling a UAV – gathering data that is used directly to engage in a military operation – is directly participating in hostilities.[145] Less involvement or involvement in the deployment of a UAV is gathering information not directly relevant for a concrete military mission, which has to be assessed on a case by case basis, but will possibly not amount to a direct participation in hostilities.

3.2.4 The Principle of Proportionality

Every single military operation, including the use of UCAVs to conduct strikes, is restricted by the principle of proportionality, the notion that the expected collateral damage must not be excessive in relation to the anticipated military advantage.

The deployment of UCAVs like the use of conventional weapons or weapons systems in general, can meet the requirements of the principle. But that is more a question of the anticipated goals and the assessment made by commanders rather than one on the legitimacy of the instrument used to fulfil the task. Critics of UCAV targeting accuse it of being highly disproportionate to the military goals since the number and frequency of civilian death seems to be rising, as lately stated by the already mentioned Stanford/NYU report.[146] But whether they actually cause excessive collateral damage or not depends on their specific deployment and the decision made by the person in command. The commander or UCAV operator must affirm that the deployment of the UCAV offers the distinct military advantage necessary to accomplish a certain military goal.[147] A relatively high number of civilian casualties may be assessed proportionate if the target is some senior high-ranking enemy combatant. On the contrary, strikes against low level targets in public places, risking enormous collateral damage, may in most situations not be proportionate. This test nonetheless is not unique to the use of UCAVs. Its advanced technology on the contrary gives the opportunity to carefully chose and target specifically and minimize collateral damage. Therefore, it can be assessed that the deployment of UCAVs in general does not violate the principle of proportionality, as long as it is deployed in a lawful manner.

---

[145] *Cf.* ICRC, *supra* note 118, at 66.

[146] *Cf.* M. O'Connell, Rise of Drones II: Unmanned Systems and the Future of Warfare: Hearing before the U.S. House Subcommittee on National Security and Foreign Affairs (28 April 2010), Written testimony of Mary Ellen O'Connell, http://oversight.house.gov/images/stories/subcommittees/NS -Subcommittee/4.28. 10-Drones II/O'Connell Statement.pdf (8 June 2012), at 5 *et seq.*; O. Bowcott, Drone Strikes Threaten 50 Years of International Law, Says UN Rapporteur, The Guardian, 21 June 2012, ahttp://www.guardian.co.uk/world/2012/jun/21/drone-strikes-international-law-un (18 August 2012).

[147] *Cf.* Schmitt, *supra* note 112, at 461.

3.2.5 Special Issues Concerning the Deployment in Non-International Armed Conflicts

Some special attention has to be directed to the deployment of UCAV/UAVs in non-international armed conflicts. There are some factual as well as legal differences to be mentioned in comparison to the use of UCAV/UAVs in international armed conflicts.

There are two major problems arising, the combatant status and civilians taking direct participation in hostilities. The distinction between civilians and combatants in international armed conflicts has to be respected at all times. In the laws applicable to non-international armed conflicts however, there are no rules on the status of person involved in fighting, since most parts of the Geneva Conventions and the AP I are not applicable. Person fighting for a non-State actors are therefore neither combatants nor protected person but have been referred to as "fighters" or "unlawful combatants"[148], which consequently means they are not legally privileged to engage in combat.[149] If a fighter of a non-State actor is involved in the launch of a UCAV, a future scenario which has to be considered due to the increase in black-market activities or the possible loss of control over a State-operated[150], is that this person has no immunity for its involvement, by virtue of Article 6(5) AP II.

Another problem arising in non-international armed conflicts in relation to the use of UCAV/UAVs is the possible expansion of the territorial scope, in non-legal terms one could label it the theatre of war.[151] The location of the operator does not present limitations. For IHL there is no difference to the launch of rockets or missiles from warships offshore, domestic missile installations deploying inter-continental ballistic missiles across the globe to UCAVs launching a Hellfire-missile. The location itself poses no legal challenge. The only thing changing is the possible territorial scope of combat situations. The UCAV/UAVs as well as its ground station and communication link can be considered military targets. One can imagine a counterattack on the ground and control station in Nevada, which would have become a lawful military target itself, despite its distance to the actual armed conflict for instance in the middle east. The territorial scope of a non-international armed conflict has raised some legal debate especially in the last years. Common Article 3 GC[152] broadly describes the conflict territory to the

---

[148] *See among others* K. Dörrmann, *The Legal Situation of 'Unlawful/Unprivileged Combatants'*, 85 International Review of the Red Cross 849 (2003); J. Bialke, *Al-Qaeda & Taliban. Unlawful Combatant Detainees, Unlawful Belligerency, and the International law of Armed Conflict*, 1 Air Force Law Review 55 (2004); J. Callen, *Unlawful Combatants and the Geneva Conventions*, 4 Virginia Journal of International Law 44 (2004).

[149] *Cf.* J. Kleffner, *From „Belligerents" to „Fighters" and Civilians Directly Participating in Hostilities*, Netherlands International Law Review 54 (2007), at 323; J.-M- Henckaerts/L. Doswald-Beck, Customary International Humanitarian Law, Vol. 1: Rules (2005), Rule 3, at 13.

[150] For example if it's computer system is attacked through cyberspace.

[151] *Cf.* P. Stroh, *Der Einsatz von Drohnen im nicht-internationalen bewaffneten Konflikt*, 2 Humanitäre Informationsschriften 24 (2011), at 76.

[152] "[…] armed conflict not of an international character occurring on the territory of one of the High Contracting Parties […]".

territory of the High Contracting Party to the conflict. If the provisions of AP II are also applicable, this territory is further restricted to the part under control of the non-State conflict party, both treaties thereby trying to limit the territorial scope to the actual battlefield, in accordance with Article 1.[153] But the AP II provisions, although more restrictive, define the application to persons involved in the conflict, no matter their exact location. In the renowned *Tadic*-Judgment, the bench also applied a wider less restrictive interpretation of the relevant provisions and by referring to both rules, expanded the territorial scope of the non-international armed conflict to a wider geographical area.[154] If for example the UCAVs ground station is located outside the described area, the conflict areal is expanded accordingly and so is the territorial application of IHL.

3.2.6 Precautionary Measures

Especially the protection of civilians during times of armed conflict has shaped the development of IHL regulations. The obligation to take precautionary measures prior to attacks to reduce the danger to civilians and protected parts is an integral part of that development, which, as one can demand, will be increased as military technology becomes more and more sophisticated. The HPCR Manual and its commentary explicitly refer to the application[155] of these rules to UCAV/UAV-deployments as well as to the advantage UCAV/UAV-technology may offer in this regard. "2. UAVs can be a useful asset in complying with the obligation to take feasible precautions in attack […] hence, if available and when their use is feasible, UAVs ought to be employed in order to enhance reliability of collateral damage estimates".[156] That recommendation, however, clearly has to be reevaluated or at least critically read in light of the new data delivered by the above mentioned "Living under Drones" report.[157]

Obligations, as to cancel an attack or suspend it if it is realised that the target is not a military object or under protection, by virtue of Article 57(2) (b) AP I, are due to the technology at hand more easily to adhere to. The same applies to the requirement of Article 57(3) to select and attack the objectives, "on which max be expected to cause the least danger to civilian lived and to civilian objects." Comparable to conventional manned military aircrafts this is usually possible till the latest stages of an attack.[158] The same applies for the prohibition to

---

[153] "[…] take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organised groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this protocol."

[154] "[…] the temporal scope of the applicable rules clearly reaches beyond the actual hostilities […] suggests a broad geographical scope […], Prosecutor *v.* Tadic, *supra* note 33.

[155] *Cf.* HPCR Manual Commentary, *supra* note 109, rule 39 I, at 135.

[156] *Ibid.*

[157] Due to the scope of this thesis the factual question on whether drones do or do not cause less collateral damage will not be further discusses here.

[158] More on UCAVs taking autonomous decision to a greater extent, Boothby, *supra* note 97, at 84. Boothby raises the question how the important the man in the loop for compliance with the obligation is.

attack persons that are surrendering, as enshrined in Article 41 AP I. Whether or not the UCAV may observe this rule depends to a great extent on its technology and the operator monitoring the data. As the HPCR Manual Commentary states "[…] such assessments by remote operators may be more reliable than those of aircrews on the scene facing enemy defences and other distractions"[159] To conclude, the technological advances of UCAVs may enhance compliance with the regulations and facilitate the implementation of precautionary measures. But if this is put in practice it still depends on the people in command of the mission and the UCAV.

4. Current Trends in Military Technology: Cyber Attacks

While the internet and in general the advance in computer technology have brought countless advantages to the public as well as State activity, it also has it downsides, as the nervous system of our contemporary world is a double-edged sword. It has become clear over the last few years that cyber space is not only an arena for hacker or criminal activity but also for attacks of a different kind. The use of computer technology has already caused an extensive transformation and a major challenge to the regulation of the waging of armed conflicts. Incidents as the 2008 Russian-Georgian armed conflicts where cyber DDoS-attacks were used to hamper the Georgian communication but also the deployment of the Stuxnet worm to sabotage Iranian Nuclear Facilities have proven:[160] Cyber space has emerged as a new battlefield and cyber activities have to be considered as new means of warfare, challenging us to revise our former understanding on the dynamics of armed conflict and the application of traditional IHL.

The following chapter aims at clarifying the notion of cyber attacks, before the effective application of IHL and especially the regulations concerning targeting are discussed.

4.1 Definition and Clarification of Terms

Cyber attacks and operations in cyber space are an instrument of warfare that is to some extent still in the dark. Differently labelled, it has been debated upon throughout the last decades, sometimes addressing synonym concepts, sometimes similar and sometimes different developments.[161]

---

[159] HPCR Manual Commentary, *supra* note 100, rule 39 III, at 135.

[160] For more information regarding the major techniques used and a discussion of recent deployment see 1.2. of the annex to this thesis.

[161] The denomination "Network-centric warfare" for instance has been more or less replaced by a deviating terminology in most academic research. The term cyberwarfare, can be understood as a military doctrine that relates to both offensive as well as defensive, operations in cyberspace. This term however has some unscientific connotation and is often used outside of academia, which is why it will not be used in this thesis. S. Handler, *The New Cyber Face of Battle, Developing a*

According to the Tallinn Manual on the International Law Applicable to Warfare of the NATO Cooperative Cyber Defence Centre of Excellence[162]Cyber operations are "employment(s) of capabilities where the primary purpose is to achieve objectives in or though cyberspace"[163]. It has been sometimes used as an umbrella term, incorporating cybercrime activities, and herewith led to confusion because of its broad application. For the application of IHL the distinction between cyber attacks and criminal activities is essential. One clearly has to separate criminal activities in cyber space from those intended to be part of a military strategy. Cyber crime is "a crime that is enabled by or that targets computers", but it is an activity falling under a different set of legal rules; those of criminal law and law enforcement as parts of the domestic law of States but not part of IHL.[164] Due to the unique nature of cyber space, those operations are extremely complicated to distinguish from each other. Using similar or even the same computer techniques such as viruses, emphasized in detail in the annex, criminal hacking and possible enemy attacks over cyber space are not only difficult to detect but also raises the question how one can be sure about the intentions of the perpetrator? A cruise missile launch will clearly be assessed under the IHL framework. If the same mechanism in cyber space however, is used to commit credit card fraud or is shutting down the ministry of defence's website, than how can one be a) sure to distinguish and b) in cases of non-physical effects, can one compare activities in cyber space to conventional attacks and apply the same legal framework? What criteria have to be fulfilled for a cyber operation to become an armed attack in cyber space?[165] Given the challenges of the practice a narrowly constructed definition of the controversial term cyber attack is necessary, one that will be used consistently in the subsequent analysis. Since no consensus on a comprehensively accepted or legal definition has been reached yet, this thesis will understand cyber attacks in

---

Legal Approach to Accommodate Emerging Trends in Warfare, Stanford Journal of International Law 48 (2012), at 212. Other terms used are for example by M. Schmitt, *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework*, in M. Schmitt (Ed.), Essays on Law and War at the Fault Lines (2012), at 7 *et seq.* and M. Schmitt, *Wired Warfare: Computer Network Attack and Jus in Bello*, in M. Schmitt (Ed.), Essays on Law and War at the Fault Lines (2012), at 485; Computer network attacks: "operations to disrupt, deny, degrade, or destroy information resident in computers and networks themselves" and information warfare: "information operations conducted during times of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries".

[162] Comparable to the Harvard Manual on Air and Missile Warfare, the new Cyber-Manual, still is in its draft version but will be published by Cambridge University Press at the end of 2012. It cannot be considered a legally binding document. Nonetheless, is the three years work of an international committee of experts, led by Michael Schmitt, that intensively examined the application of existing law to this new phenomenon and is therefore a scientific source and prominent reference, mirroring the prevailing view and interpretation of the law, draft version available online: http://www.ccdcoe.org/379.html (12 September 2012).

[163] Handler, *supra* note 141, at 210

[164] *Cf.* C. Wilson, CRS Report for Congress: Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress (2008), www.fas.org/sgp/crs/terror/RL32114.pdf (26 June 2012), at 4.

[165] At this point one again has to clarify that an armed attack in the sense of IHL is not comparable to the armed attack and its understanding in the *jus ad bellum* context.

accordance with the Tallinn Manual, to further discuss solely those operations that meet the threshold necessary for the application of IHL.[166] Cyber attacks should subsequently be understood as "[…] a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or damage to persons or damage or destruction to objects."[167]

4.2 Types of Cyber Operations and Cyber Attacks

A variety of non-consensual techniques can be engaged to execute cyber attacks by *inter alia* altering, hampering or destroying data and data-flows[168], of which the most prominent ones should be shortly discussed to give an overview and highlight the complexity of identifying an attack as such: One major technique is the attack by Denial of Service (DoS): "an assault on a network that floods it with so many additional requests that regular traffic is either slowed or completely interrupted".[169] This method is explicitly used to hinder the regular users from using the offered service of websites. Especially employed in armed conflict context is a variation of the DoS attack: the distributed Denial of Service (DDoS), in which a multitude of infected computers attack an individual server to sabotage it.[170]

Another form is the use of malicious programs, with which normal computer functions are used to disable computers, for instance by introducing time delays or inserting backdoors to allow others to remotely control the target server from a dislodged place.[171] For this purpose different programs can be inserted, for example viruses, worms and Trojan-horses.[172] While viruses spread from server to server by attaching itself to a program or a file, a worm comparably spreads though computers but, differently to a virus, can travel without human involvement by replicating itself, sending hundreds or even thousands of copies of itself to other computers. A Trojan-horse is "a program in which malicious or harmful code is contained inside apparently harmless programming or data in such a way that [one] can control and its chosen form of damage."[173] Other instruments for attacks through cyber space are logic bombs, activating themselves at a chosen event and for example starting to delete data or "explode" at times of reserve forces call-ups, thereby disrupting the military

---

[166] Tallinn Manual on the International Law Applicable to Warfare of the NATO Cooperative Cyber Defence Centre of Excellence (Tallinn Manual), comparable to the HPCR, is expected to clarify and further coalesce the diverging definitions and terms; *see infra* note 147.

[167] Tallinn Manual on the International Law Applicable to Warfare of the NATO Cooperative Cyber Defence Centre of Excellence (Draft version), http://www.ccdcoe.org/379.html (12 September 2012), at 92.

[168] *Cf.* The USAF Intelligence Targeting Guide. AF Pamphlet 14-210 (1998), at para. 11.4.3.

[169] A. Schaap, *Cyber Warfare Operations: Development and Use under International Law*, Air Force Law Review 64 (2009), at 134.

[170] *Cf. Ibid.*

[171] *Cf.* Wilson, *supra* note 150, at 29.

[172] Techterms.com, The Tech Terms Computer Dictionary, Malware, http://www.techterms.com/definition/malware (26 June 2012).

[173] SearchSecurity.com, Trojan Horse, http://searchsecurity.techtarget.com/sDefmition/0,,sidl4_gci213221,00.html (2 June 2012).

logistics and supply. Or for the purpose of disrupting information flows or providing false or collect classified information as codes, so-called sniffer programs can be utilized.[174]

4.3 Deployment of Cyber Operations and Cyber Attacks

The interconnectedness of all major critical components of national and transboundary infrastructures is an essential element for the vulnerability towards cyber attacks:

"The public telephone network, for example, relies on the power grid, the power grid on the transportation, and all the sectors on telecommunications and financial structures […] Most of today's cybernetic networks are actually combinations of networks, interconnected and interdependent. Interaction among these subsystems is critical to overall network performance, indeed they are the essence of network performance."[175]

In comparison to conventional weaponry, cyber attacks provide enormous benefits especially for non-State actors or less developed States, traditionally afflicted by the asymmetrical distribution of power in favour of highly industrialized States. The RAND Corporation published a study concerning the low costs of developing cyber warfare technology, as within the budget of nearly ever State in the world.[176] Cyber war is "war on the cheap".[177] Knowledge and equipment necessary for conduct in cyber space is to some extent available to the public and affordable, but also offers a high probability to cause extensive damage in the technological dependent industrialized States.

Already in the 1990s the employment of cyber attacks was recognised as an increasing problem to the security of States. In 2000 John Serabinam stated that the Central Intelligence Agency was "detecting with increasing frequency, the appearance of doctrine and dedicated offensive cyberwarfare programs in other countries",[178] a development that was equally referred to by the NATO Chief of Cyber Defence, emphasizing that cyber terrorism, cyber operations and cyber attacks pose an as great threat to national security as missile attacks. Nowadays one can assume that nearly 140 nations are actively involved in "cyber warfare" programs in different stages of development.[179] However, the fear of a lonesome hacker bringing down a States whole infrastructure is, at this point, exaggerated. For a large –scale cyber attack highly developed military

---

[174] *Cf.* Schaap, *supra* note 166, at 135.

[175] Schmitt, *supra* note 147 (Computer Network Attack), at 10.

[176] *Cf.* M. Libicki, Cyberdeterrence and Cyberwar, RAND Corporation (2009), at 177; K. Coleman, The Cyber Arms Race Has Begun, CSO, 28 January 2008, <3va;7aè/ea/http://www2.csoonline.com/exclusives/column.html?CID=33496. (18 June 2012).

[177] Schmitt, *supra* note 147 (Computer Network Attack), at 13.

[178] J. Serabian, Jr., Statement for the Record Before the Joint Economic Committee on Cyber Threats and the US Economy (23 February 2000), https://www.cia.gov/news-information/speeches-testimony/2000/cyberthreats_022300.html (2 June 2012).

[179] C. Billo/W. Chang, Cyber Warfare – An Analysis of the Means and Motivation of Selected Nations States (2004), http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf (8 June 2012).

capabilities are needed, capabilities that for now only a few nations, as China, India, Russia or the USA posses.[180]

In recent years there have been some prominent incidents that should illustrate the increasing technical expertise and the will to employ these new means.[181] Prominent and recent examples of the use of operations in cyber space comparable to traditional military means are the major DDoS–operations against Estonian communication infrastructure in March and April 2007, as well as Stuxnet, the computer worm that was programmed to sabotage Iranian nuclear facilities in 2009/2010.[182] These incidents have all happened in times of peace. This explains the amount of literature on the topic of whether and under which circumstances such an operation can be considered an armed attack under *jus ad bellum* and be assessed as a violation of Article 2(4) UN Charter and therefore establishing the right to self-defence under Article 51 UN Charter.[183]

But there are other examples of comparable activities during times of armed conflict and consequently under the application of IHL. The Russian-Georgian War in 2008 marked the shift in the use of this modern warfare technology: cyber attacks, as Handler states, joint the conventional kinetic "triad of air, ground and naval operations"[184], and demonstrated the vulnerability of a State to attacks of this new type.[185] The primary goal of these parallel cyber attacks and -operations, so the experts, was to limit the Georgian military reaction to the Russian conventional operations. By hampering the governments and the military`s ability to exercise command and control, Russia enhanced the damaged caused by its traditional means of warfare.[186] These operations have to be evaluated under IHL since they were conducted during an on-going armed conflict.

---

[180] Turns, *supra* note 149, at 280 and *ibid.*

[181] For instance attacks on the Pentagon in 2007, M. Sklervov, *Solving the Dilemma of State Reponses to Cyberattacks*, Military Review 201 (2009), at 5.

[182] *Cf.* K. Ziolkowski, *Stuxnet. Legal Considerations*, 3 Humanitäre Informationsschriften 24, 139-148.

[183] *See* recently published, M. Waxman, *Cyber-attacks and the use of force: back to the future of article 2(4) of the UN Charter*, in: 2 Yale Journal of International Law 36 (2011); A. Wortham, *Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?*, 3 Federal Communications Law Journal 64 (2012); R. Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 2 Journal of Conflict and Security Law 17 (2012).

[184] Handler, *supra* note 147, at 210.

[185] Following conventional military operations in August 2008 were cyber-attacks launched by Russia to target Georgian critical infrastructure. According to several sources around 54 Georgian governmental websites were attacked, mostly by the above mentioned Distributed Denial of Service (DDoD) attacks, […], including news media and communication facilities which originally would have been attacked by missiles or bombs during the first phase of invasion"; J. Markoff, Before the Gunfire: Cyberattacks, New York Times, 12 August 2008, http://www.nytimes.com/2008/08/ (2 June 2012).

[186] U.S. Cyber Consequences Unit, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008 (2009), www.registan.net/.../US-CCU-Georgia-Cyber-Campaign.pdf (2 June 2012), at 5.

4.4 Legal Framework Governing the Use of Cyber Attacks

How is the traditional framework equipped to react to new challenges, which were, at the time of drafting and entry into force of major IHL-treaties, maybe unimaginable, today's advanced technology not yet invented? Cyber techniques may be deployed to cause actual physical damage, for instance by causing military aircrafts to crash. However, there is also another kind of attacks: non-kinetic cyber attacks rarely kill, injure or damage, but hamper informationflows, communicationlines and corrupt data.[187] The established regime of the law of armed conflict does not address the issues of cyber attacks explicitly, there is no case law, one can refer to, and although some State practice might be identified, clear *opinio juris* regarding cyber attacks does not exist yet.[188] But by no means is their use unrestricted or conducted in a legal vacuum. The question is how traditional IHL may be applied and whether cyber attacks may alter the current application of IHL principles, especially keeping the subject of targeting in mind.

4.4.1 Threshold of Cyber Attacks under International Humanitarian Law

Traditionally and rooted in the nature of conventional warfare and weaponry, IHL has paid less attention to the question whether single operations of a party constitute armed attacks in the meaning of IHL, as the answer was usually obvious and non-controversial. Cyber attacks to some extent constitute a new form of attack, as they may not necessarily cause direct kinetic effects. Some argue that since IHL does not address cyber activities or comparable technology and its invention postdates treaty law and has therefore not been "within the contemplation of the parties to those instruments, its exempt from the coverage thereof."[189] But one strongly has to counter this line of argumentation. Even thought the binding law might be silent on the exact matter that does not create a legal void for this new means. The Martens' Clause, as a last resort and as discussed in the beginning of this thesis, is a reminder of the significance of the premises of IHL, even if it is not explicitly addressing certain new issues. The ICJ in its *Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons* in 1996 citied its modern version of Article 1(2) AP I as "effective means of addressing the rapid evolution of military technology".[190] In addition to this notion, the ICJ Statute in Article 38(1)(b) refers to international custom as one source of law, supporting the applicability of the legal framework despite a lack of explicit *lex scripta* on this topic. Similarly the ICJ in the Advisory Opinion rejected the argument of inapplicability because "principles and rules

[187] A detailed analysis of the two different kinds of cyber attacks can be found *inter alia* Handler, *supra* note 141.

[188] *Cf.* D. Turns, *Cyber Warfare and the Notion of Direct Participation in Hostilities*, 2 Journal of Conflict and Security Law 17 (2012), at 282.

[189] Schmitt, *supra* note 141 (Wired Warfare), at 486.

[190] Nuclear Weapons Advisory Opinion, *supra* note 6, at para. 78.

had evolved prior to the invention of nuclear weapons."[191] The bench announced that there could be no doubt on the applicability of humanitarian law as well as core provisions of the UN charter, as they do not refer to specific weapons but are generally binding: "They apply to any use of force, regardless of the weapon employed […] to all forms of warfare and to all kinds of weapons, those of the past, those of the present and those of the future"[192], a reasoning that can be applied analogous to cyber attacks, especially as one can be certain that the drafters of the Additional Protocol I envisaged an application to future technological developments, *inter alia* the review of new weapons and means of warfare, enshrined in Article 36 AP I.

Although this argumentation by no doubt supports the application of IHL to cyber attacks, the threshold question still needs to be answered. The commencement of an "armed conflict" is the requirement to activate IHL, "to all cases of declared war or any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized between one of them", by virtue of Common Article 2 GC and similarly adopted by AP I. The commencement of hostilities as initiator for IHL application is now part of customary humanitarian law. The ICRC`s commentary to the Geneva Convention refers to the criterion of the "intervention of armed forces"[193], as activities of a specific nature and intensity (historically associated with the deployment of states armed forces).[194] This approach was sufficient for a long time to regulate certain conduct, since States' armed forces had a unique and undisputed key role.

That however has changed. No longer can conventional attacks by armed forces be considered the exclusive trigger for IHL application. To adapt to the transformation of conflicts one has to analyse the term 'armed attack', as it is understood in IHL, and IHL itself is not silent on the determination: AP I defines in Article 49 attacks "to include acts of violence against the adversary, whether in offense or in defence". Traditionally the term 'violence' has always been a narrow concept, usually associated with direct physical effects. Cyber attacks may, however, not cause direct physical effects or sometimes merely temporarily, but not constantly.[195] Therefore, the classical understanding must be seen as outdated. A new effective interpretation, able to meet the challenge and cover new scenarios can be found in the effects-or consequence-based approach.[196] The approach is based on the following derivation: The conduct IHL is restricting, can be deduced from its protection standards, as it governs means and methods to injure, kill, damage or destroy. Other IHL regulations support

---

[191] *Id.*, at para. 85.

[192] *Id.*, at para. 39.

[193] Common Art. 2 GCs.

[194] *Cf.* Schmitt, *supra* note 141 (Wired Warfare), at 488.

[195] *Cf.* M. Schmitt, *Wired Warfare: Computer Network Attack and the Jus in Bello*, in M. Schmitt/ B. O'Donnell (Eds.), Computer Network Attack and International Law (2002), at 194 *et seq.*

[196] *See* C. Dunlap, *Perspectives for Cyber Strategists on Law for Cyberwar*, Strategic Studies Quarterly (2011), at 85; For a discussion of competing approaches, *see further* D. Graham, *Cyber Threats and the Law of War*, 1 Journal of National Security 1 (2010), at 91 *et seq.*

this reading, as for instance the principle of proportionality refers to the loss of life or injury of civilians or damage and destruction of civilian objects. And consulting the *travaux preéparatoires* of AP I as subsidiary source for interpretation, Article 32 Vienna Convention on the Law of Treaties (VCLT) in conjunction with Article 38(1)(a) ICJ-Statute, one can establish another analogy. The laying of landmines, as it is said, constitutes an armed attack, whenever a person is directly endangered by it.[197] Therefore, one can assume that whenever a cyber attack endangeres protected person or objects, the threshold of an armed attack in understanding of the *jus in bello* is reached. At this point the effects-based approach delivers the way to address the threshold question for a cyber operation to amount to an armed attack and become a subject to IHL. The respective conduct must be an act of violence. This includes violent acts against targets, but even more, and essential to evaluate cyber activities, also acts with violent effects. Therefore, as the effects-based approach consistently argues, whenever a cyber operation is more than a sporadic and isolated incident and is employed to cause injuries, death, damage or destruction (as well as imaginable analogous consequences),[198] IHL has to be applied equally.[199]

4.4.2 Military Necessity and the Principle of Humanity

Military Necessity permits attacks on hostile military computer networks, as it clearly offers a military advantage. The use of means of cyber space against individual military personnel by interfering with personal finances or invading privacy, in general by attacking the private sphere instead of attacking its military capacity however would highly probable violate the principle of humanity.[200]

4.4.3 The Principle of Distinction

The principle of distinction in its wording and interpretation is broadly applicable and not limited to specific types of weapons or means of warfare. Therefore, one can definitely assert that the regulations, as discussed in detail under Chapter 2.2.2 are applicable to cyber attacks. Cyber attacks are launched by computers, a code and a way by which the code is transmitted. The example of sending an email shows that the computer itself can very discriminately target specific targets. But perpetrators can also write codes that are by their nature or unintentionally very indiscriminate, that travel from computer to computer by replicating itself. This different nature is manifested in viruses and worms, the latter replicating itself, as is in detail discusses in the annex. In its

---

[197] *Cf.* Sandoz/Swinarski/Zimmermann, *supra* note 18, at para. 1881.

[198] E.g. the attack on airports air traffic control systems or destruction of oil pipeline by remotely controlling computer system or using computers to release toxic gas, Schmitt, *supra* note 141 (Wired Warfare), at 490.

[199] *Cf.* Y. Dinstein, *The Principle of Distinction and Cyber War in International Armed Conflicts*, 2 Journal of Conflict and Security Law 17 (2012), at 261.

[200] *See* Y. Alexander, *Terrorism in the Twenty-First Century: Threats and Responses*, 12 DePaul Business Law Journal 59 (1999/2000), at 83; Brown, *supra* note 1, at 200.

consequence although not by itself, a specific and offensive code can be illegally indiscriminate. Here the principle of distinction is violated. The following subsection, however, will concentrate on those attacks that can be launched against specific attacks in a controlled manner.

4.4.3.1 Targeting: Distinction between Military Objectives and Civilian Objects

Combatants and military objectives are both by their very nature legitimate and classical targets for armed attacks. Those in charge of planning the operation have to conduct everything "feasible" to verify the legitimacy of their targets but then, combatants and military objectives can be directly attacked, by conventional but also by cyber attacks. For instance, launching a cyber attack against a military air traffic control leading to the crash of a combatants troop transport is as legitimate as the use of a missile would have been.[201] Comparably to the equipment and support of conventional weapons, those networks and computersystems contributing to military attacks or being the source of the cyber attack themselves, can be considered lawful targets under IHL. Contrariwise the prohibition not to target civilians and civilian objects directly is nearly absolute, although there are cases in which they are an indirect subject to attack. In context of cyber attacks one can imagine scenarios in which a military objective is targeted but the effects are so broad civilians will be heavily affected, analogous to a missile launch against a highly populated area. That means the principle of proportionality has to be upheld strictly, as will be discussed in the next subsection.

Problematic with computer-systems and networks is that they themselves might be considered so called dual use objects, since the path information takes over the internet cannot clearly distinguish between military and civilian, for instance if international telecommunication providers or satellites like INTELSAT, EUROSAT or ARABSAT are used.[202] With the increasing use of advanced technology it becomes more and more important to "avoid losing sight of the humanitarian principles",[203] especially if one looks at the militarization of civilians and civilians activities. The military increasingly depends on civilians but also civilian infrastructure in their operations and herewith blurring the distinction to a critical extent, as for instance computer networks used by the military are to rather more than less extent based on civilian networks.[204] Due to this technological interconnectedness of computer systems, networks and the internet, so called dual use objects are of special importance with regard to targeting by cyber attacks, and a final classification into legitimate military objective or protected civilian object is often highly controversial.

---

[201] *Cf.* Sandoz/Swinarski/Zimmermann, *supra* note 18, at 2020-2023.

[202] Owned by an international consortium. On the Question of Neutrality, *see discussion* in G. Intoccia/J. Moore, *Communications Technology, Warfare and the Law of War: Is the Network a Weapon System?*, 2 Houston Journal of International Law 28 (2006), at 487.

[203] Schmitt, *supra* note 141 (Wired Warfare), at 509.

[204] *Cf.* Brown, *supra* note 1, at 183.

A variety of objects depend highly on computer-technology and the internet, as computernetworks for research or medical facilities, electronic power grid networks, traffic control, gas and oil distribution centres. They all can be considered civilian objects in light of Article 52(2) AP I. But, under certain circumstances they may effectively contribute to military action. As with the mentioned examples, some objects may serve civilian and military purposes both at one time; this complicates the application of the principle of distinction. Although being used for civilian purposes their effective contribution to military efforts as secondary use transforms them from civilian object to military objective.[205] And if their destruction provides a definite military advantage, they might become legitimate targets themselves.[206] One must be aware that the nature of objects can change repeatedly depending on the circumstances and the conflict itself. An airfield that is used for military logistical purposes in one conflict could be classified a military objective. At another time or in another conflict it may not serve any military purposes and remain a purely civilian object.[207] A potential dual-use object that is currently classified as being merely civilian but could potentially be used for military aims, must be reclassified as military objective if the "likelihood of military usage is reasonable and not remote to conflict under way".[208]

Attacks that, for instance, lead to starvation of the population or deny it indispensible objects are prohibited and therefore cyber attacks on food storage or water distribution causing such effects would also be unlawful, even if the hostile armed forces were the intended primary victims. These examples illustrate that the targeting of dual-use objects must be thoroughly assessed in the actual planning phase of an operation to ensure a correct labelling as some objects cannot be generally assessed or change their character.

4.4.3.2 Status of Persons Involved in Cyber Attacks

Also problematic to evaluate is the involvement of civilian personnel in the cyber attacks. An important issue that must be mentioned in this regard is the problem of attribution and State responsibility. The advanced technical nature of cyperoperations *per se* – underlined by Kellenberger, stating "Digitalisation ensures Anonymity"[209] and cyber attacks specifically makes it more or less

---

[205] *Cf.* Kelsey, *supra* note 8, at 1437; *See* for further discussion, M. Sassôli, *Legitimate Targets of Attacks Under International Humanitarian Law*, International Humanitarian Law Research Initiative, Background Paper 7 (2003), www.hpcrresearch.org/sites/.../files/.../Session1.pdf (2 June 2012).

[206] That is in cases, in which the principle of proportionality is also respected and the collateral damage to civilians and civilian objects is not excessive.

[207] Art. 56(1) AP I.

[208] Schmitt, *supra* note 141 (Wired Warfare), at 487.

[209] J. Kellenberger, International Humanitarian Law and New Weapons Technology, Keynote address at the 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 09 August 2011, http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm (2 August 2012).

impossible to attribute an attack to any State or non-State actor.[210] Where does the attack originate from? Linked to the identification of the perpetrator is the question at what point and under which circumstances State responsibility can be evoked for the conduct of private individuals, an issue controversially debated among legal scholars as well as international institutions.[211] If one tries to apply those standards to the cyber attack-scenario one clearly has to state that both control-standards, but even more the effective control test are in this form not applicable to cyber attacks. That question, however, is one that cannot be answered by IHL and within the scope of this thesis and is therefore not discussed further.[212]

But granted that the one could identify the source of a cyber attack within an armed conflict situation, one possibly has to deal with the involvement of civilians. Due to the general trend in out-sourcing military branches to private contractors or technical experts, also aspects of cyber warfare might be conducted by civilian specialists, not by military personnel. They might be supporting essential military operations by maintaining computer equipment, that itself can be considered a legitimate military target or even conducting the cyber attacks themselves.[213] It is imminent that solely members of the regular forces are entitled to employ the use of force against their enemies.[214] Contractors, civilian technicians or the involvement of any other civilian personnel in the deployment of any weapons and means of warfare, including cyber attacks, is prohibited and they will lose their protected status and may be prosecuted for unlawful participation in hostilities. The level of involvement however is difficult to evaluate, as has been similarly asserted in Chapter 3.2.3.2., with regard to UCAV strikes. Civilian personnel introducing for instance a virus on a hostile computer system to exploit some vulnerability, or civilian personnel conducting DDoS attacks on enemy computer systems, or activating harmful computerprogramms within the targets computer system, undisputedly take a direct participation in hostilities with all consequences describes in the chapters above. Designing malware, maintaining for computersystems used for cyber attacks or identifying possible backdoors for inserting malware into the enemy's system however is a different matter.[215] In this case, one can surely argue that not all three ICRC criteria, the threshold of

---

[210] *See* on the difficulties of attribution *inter alia* N. Tsagourias, *Cyber Attacks, Self-Defense and the Problem of Attribution*, 2 Journal of Conflict and Security Law 17 (2012).

[211] Effective control test applied as established by the ICJ in its Nicaragua Judgment and later affirmed in the Genocide case in 2007; Military and Paramilitary Activities (Nicaragua *v.* United States of America), ICJ Reports 1986 (27 June 1986), Summary of the Judgment, at para. 5; Application of Convention on Prevention and Punishment of Crime of Genocide (Bosnia and Herzegovina *v.* Serbia and Montenegro), ICJ Reports 2007 (27 February 2007). Or rather the ICTY's overall control test, as raised in the *Tadic*-Judgment; Prosecutor *v.* Tadic, *supra* note 33, at para. 120 *et seqq.*

[212] This assessment in practice is highly difficult because of the serious attribution problem, which makes the identification of the perpetrator or controller of the cyberattack nearly impossible.

[213] Art. 4(4) GC III.

[214] *Cf.* Brown, *supra* note 1, at 190.

[215] *Cf.* Turns, *supra* note 149, at 295.

harm, the causal link between the civilian's action and the subsequent harmful effects, or the belligerent nexus are fulfilled to amount to an unlawful participation in hostilities and the loss of the protected status.[216]

As we have seen it is difficult to adhere to the principle of distinction as the majority of non-human possible targets, especially hostile computersystems, depend largely on civilian components. This aggravates or even precludes a classification as lawfully targetable military objective. If however, the object is nonetheless classified as being such a lawful military objective, the principle of proportionality and the question of collateral damage have to be considered in a next step.

4.4.4 The Principle of Proportionality

As with all other types of weapons used in armed conflict, cyber attacks have to comply with the principle of proportionality, the balancing act between military advantage and collateral damage caused by the attack. If one considers possible scenarios of cyber attacks at one end of the line, IHL will probably permit the use of cyber attacks on purely military objectives only. At the other end of the line, IHL will prohibit attacks, as with any kind of weapon, that are deemed to cause intentional civilian death or destruction, as for instance the alteration of air traffic control causing the crash of a civilian airplane or corrupting medical facilities and databases. Considering the risks one can assess the following: The principle of proportionality in its traditional interpretation is very likely to be violated by cyber attacks due to the interconnectedness of civilian and military systems and the uncontrollable effects on civilian infrastructures, and would therefore render such attacks unlawful under IHL.

In this regard a current debate should be highlighted: the possible advantages of military cyber operations that might result in a more flexible application of relevant provisions, an argumentation that is pushed especially by military lawyers and practitioners and clearly rejected by the peace research community. The potential non-lethal and non-kinetic nature of cyber attacks might be seen as an advantage and basis for an increase in deployment. It is on the other site a problem to IHL principles and conduct in armed conflict since belligerents might feel inclined to ignore the application of certain principles, as the principle of distinction and attack objects that are traditionally protected by IHL. In deploying conventional attacks, high numbers of civilian injuries or damage to property can sometimes not be prevented which is why legitimate military targets is a restricted category and only indirect military purposes no justification. Cyber attacks increase the option to minimize collateral damage, as physical destruction can now be replaced by "turning off" the target, or just setting out of service temporarily.[217] As seen in the previous chapter the spectrum of potential military objectives might get expanded as one could attack

[216] *See further examples* Tallinn Manual, *supra* note 146, at 103.
[217] *Cf.* Schmitt, *supra* note 141 (Wired Warfare), at 505.

certain objects without causing a comparable high danger to civilians and objects.

However the knock-off-effects caused by this technology are problematic; those effects not directly and immediately caused by the attack, but product thereof, and the effects caused by effects of the attack. As factual example the attacks on the Iraqi electrical grid during the Gulf War 1990-1991 can be referred to. Attacks that firstly disrupted Iraqi command and control (direct effect) but also denied civilian population access to electricity and thereby affecting hospitals and emergency response et cetera (indirect effect). Those are effects that one can imagine to be caused by a cyber attack as well, even more realistic due to the interconnectedness of computersystems. Assessing the proportionality-equation of an attack is further aggravated in cases of cyber attacks since on cannot always clearly identify network connections: "Given the complexity of cyber attacks and the high probability of impact on civilian systems and relatively low understanding of its nature and effects is a challenge […]."[218] Even if the possibility of attacking effectively with cyber means but causing more harmless effects exits in theory, the technology and the consequences of its use can currently not be appraised let alone be controlled.

4.4.5 Precautionary Measures

The overall objective to protect civilians from the waging of war finds a major instrument in the fundamental obligation of all parties to the conflict to take all precautions prior to attack. It has sometimes been stated that cyber instruments would reduce or at least limit collateral damage in comparison to conventional weapons.[219] As previously argued, the deployment of cyber attacks should no be used to attenuate or bend the traditional rules of IHL due to some new elements in this technology. The previous analysis already crystallized some major problems with regard to the application of especially the principle of distinction and proportionality, problems that again emerge when discussing precaution in attack.

Regarding for instance the obligation of Art. 57(2) (b) AP I, to cancel or suspend attacks if the targeted object/person is not or no longer a legitimate military target differences between the two technologies discussed in this thesis can be identified. One could possibly even better follow the obligation by using UAV/UCAVs due to their advanced (surveillance) technology and last-minute-abort option of the attack. That however is different with regard to cyber attacks due to two factors: The interconnectedness of computernetworks and the internet, as already discussed under section 4.2.3.1., seriously exacerbates a distinction between military and civilian objects. The distinction is firstly blurred and secondly not definite, as the character of the so-called dual use

[218] *Ibid.*

[219] K. Jastram/A. Quintin, The Internet in Bello: Cyber War Law , Ethics & Policy. Seminar held 18 November 2011, Berkeley Law, cybewarfare_seminar—summary_032612.pdf (25 October 2012).

objects may change rapidly. So one has to question whether they are sufficiently separated prior as well as during the attack. And furthermore, the nature of the cyber technique chosen also determines whether the obligation can be fulfilled. To abort attacks if the target was wrongly classified is solely possible if the attacker is able to control the weapon or means deployed. Going back to the previous example: If a worm, replicating itself without further control of the person that launched the attack, is used to target, then due to the technical nature of the means the obligation cannot be adhered to, leading to a violation of IHL.

5. Conclusion: Is IHL Effectively Applicable to Modern Technologies or Do We Need New Rules?

Modern technologies and the alterations they provide for targeting operations have to be reviewed for compliance with the legal framework applicable to armed conflicts. So far IHL has met the challenges provided by technological developments over the last centuries, whether in its general form or by additional specific treaty law. During the last decades, however, concise shifts in technological evolution once again questioned the effectiveness of IHL in regulating contemporary armed conflicts and nowadays warfare. Advancing robotic technology as well as the use of cyber space as a new battlefield are, step by step, repressing conventional means and methods. IHL was not designed explicitly to be applied to these modern technologies, but it is nonetheless the legal field applicable. The challenge lays in adapting it constantly to the ever changing here and now. This thesis focussed on the application of IHL, specifically the regulations on targeting, to two types of modern technology, unmanned (combat) aerial vehicles and cyber attacks. By analysing the compliance of their use with the fundamental principles of IHL and its specific regulations on targeting the law of armed conflict was also analysed for its ability to adapt and its effectiveness as restricting framework.

This conclusion, after giving a resumée on the applicability of the existing IHL regulations on the two chosen types of modern weaponry, will take an onward looking perspective. IHL provides for a comprehensive legal framework to not only uphold its primary notion of protecting civilians and regulating the conduct of hostilities through a general legal matrix. During the last decades it has furthermore shown its ability to adapt to new technological innovations, as can be proven by the drafting and ratification of new treaties regulating specific types of weapons: “International humanitarian law has proven to be flexible in the past and will further evolve taking into account the new realities of

warfare."[220] Nonetheless, the creation of new treaty law by the international community presents a major obstacle. On the still State-centric plane, lacking the presence of a global leviathan, the drafting of a universally binding instrument through which its creators – the States – themselves give away their autonomy in a certain area is far from easy.[221] Keeping the complexity of treaty evolution in mind, one therefore has to think about whether it is actually necessary to draft new conventions. One should not forget there are both advantages but also disadvantages and risks involved in this process: codification and clarification may be assessed as major advantage to the establishment of a new treaty regime, which helps to fill existing lacunae. But fragmentation of international law and losing sight of the general application of the law due to the variety and plurality of highly specialized regimes might work counterproductively and could eventually increase legal uncertainty. Especially with regard to the legal framework applicable during times of armed conflict, the interpretation and application of legal rules and the protection of legal certainty is of utmost importance. For this reason one firstly has to assess whether IHL has failed to address the new developments surrounding contemporary armed conflicts or whether it is flexible enough to adapt: Do we need new regulations concerning the employment of new weapons or is the traditional framework still effectively functioning?

5.1 Application of International Humanitarian Law to Unmanned (Combat) Aerial Vehicles

Chapter 3 addressed UCAV/UAVs as one prominent example of modern weaponry, in particular focussing on targeting operations by UCAV strikes. The employment of increasingly automated weaponry initiated a major shift in contemporary conduct of hostilities, with robotic technology replacing humans more and more. The employment of UCAV/UAVs can be considered a key step in this direction, already highly dependable on robotic technology but leaving the final decisions to the human operator and commander in charge of the operation. But although using an advanced technology, the employment of UCAV/UAVs can still be compared to their conventional counterparts, as for instance fighter jets, with a human as commander. The use of UCAV/UAVs as a means of armed conflict *per se* is not presenting an obstacle to IHL, since the fundamental principles especially relevant for targeting operations are undisputedly binding and can without difficulties be applied to UCAV/UAV technology in general. If the concrete deployment however is in compliance with the law completely depends on the specific scenario and has to be assessed on a case-by-case basis.

---

[220] ICRC, International Humanitarian Law and Challenges of Contemporary Armed Conflicts, 28th International Conference of the Red Cross and Red Crescent, Geneva (2003), www.icrc.org/.../ihlcontemp_armedconflicts_final_ang.pdf. (29 August 2012), at 26.

[221] *Cf.* H. Thirlway, *The Sources of International Law*, in: M. Evans (Ed.), International Law (2010), at 100.

This assessment leads to the conclusion that no specific treaty for the use of UCAV/UAVs in times of armed conflict is necessary to fulfil the premise of protecting civilians and regulating the conduct of hostilities. From an interdisciplinary perspective one could consider the usefulness of a multilateral arms control or disarmament agreement. Its increasing purchase by States worldwide countervails an overall effort of minimizing military solutions to political disputes. This question, however, as well as the application of IHL to already envisaged completely autonomous operating UCAV/UAVs, is left for another analysis.

5.2 Application of International Humanitarian Law to Cyber Attacks

The analysis in Chapter 4 stressed the difficulties and debates surrounding the deployment of cyber attacks during armed conflict. The application of the fundamental principles has led to an outcome, deviating from the conclusion that was drawn with regard to UCAV/UAV technology. While its use, if performed in accordance with the legal requirements, do not violate IHL in general; cyber attacks present themselves as a bigger challenge. One can also state that their use *per se*, if performed legally, does not violate IHL – but is that even possible with this kind of technology? As the analysis has shown, especially the principles of distinction and proportionality may easily be violated by the character of a cyber attack-deployment or by the general nature of such an attack: since the vast majority of computer networks are primarily civilian and may become military secondary, the identification of lawful non-human targets is highly difficult. Due to the interconnectedness of almost all computer-based infrastructures, solely targeting military components becomes almost impossible.

Some scholars, as for example Handler, argue for a broader interpretation of the definition of military targets, since the chances in modern technology and warfare capabilities would have eroded the distinction between civilian and military targets anyway.[222] AP I, as a major legal basis enshrining binding provisions on targeting, has been criticized in this regard as "focus[sing] to narrowly on definite military advantage and paying too little heed to war sustaining capabilities".[223] The critique is supported by those arguing for an increased employment of cyber attacks instead of conventional weaponry causing physical injury, following a similar line of argumentation than we already saw with regard to a possible humanitarian aspect of UCAV/UAV technology. The Bush Administration announces in its Security Directive 16 for example that IHL should encourage the use of cyber over conventional weaponry.[224] And also Kelsey states, one needs to avoid "prematurely limiting

[222] *Cf.* Handler, *supra* note 141, at 219.

[223] OTP Report, *supra* note 55, at 86.

[224] *Cf.* B. Graham, Bush Orders Guidelines for Cyber-Warfare, Washington Post, 7 February 2003, http://www.stanford.edu/class/msande91si/www-spr04/readings/week5/bush_guidelines.html (20 August 2012).

weapons that could potentially offer some measure of non-lethality to armed conflict".[225]

Maybe the employment of cyber operations does cause less direct physical harm but the expansion of possible targets to all those civilian assets used for military purposed which includes almost all computer regulated infrastructure, would completely deviate from the premise of the IHL principles. Considering the rapidness of modern days technological developments on one hand and the ability with which IHL has over the last century adapted to the transformation of armed conflict on the other hand – albeit all difficulties and controversies, that appear from time to time – one should not easily dilute the rules that are interpreted narrowly to strictly protect civilians and regulate the conduct of the parties of the conflict. Therefore to broaden the definition of military objectives and include formerly civilian objects seems to be a short term and not convincing suggestion. And even if one reflects upon a less narrow interpretation, the principle of proportionality in its traditional application would subsequently prohibit massive involvement of civilian infrastructure and even more the targeting of such. If one strictly applies the existing principles and articles, the use of cyber methods is rather severely restricted by IHL.

Nonetheless, as O'Donnel and Kraska highlight, "information warfare weapons will displace kinetic weapons as preferred means of warfare".[226] For those reasons a debate among international lawyers was initiated: Do we need a new treaty to regulate cyber attacks?

States have cooperated over the last decades to create new restrictive treaty regimes for new types of weapons, but so far they have not shown enthusiasm to draft a new cyber treaty.[227] That results from the paradox of cyber technology. At this moment it offers enormous advantages to States and non-State actors, but on the other hand with an increasing dependency the risks of negative impacts and vulnerabilities raise. As Muir stresses with the US as example, "the technology that put the United States in a position of strength may also be its Achilles' heel".[228]

Therefore some scholars pressure for a new treaty designed to regulate cyber attacks. Brown is one advocate, pushing towards an international convention on cyber attacks, as discussed in its 2006 article in the Harvard International Law Journal. He envisages specific cyber rules, modelled after traditional IHL regulations, slightly modified to explicitly address cyber attacks. [229] He

---

[225] Kelsey, *supra* note 8.

[226] B. O'Donnell/J. Kraska, *Humanitarian Law: Developing International Rules for the Digital Battlefield*, Journal of Conflict and Security Law 8 (2003), at 145 *et seq.*

[227] A. Schaap, *Cyberwarfare Operations: Development and Use under International Law*, Air Force Law Review 64 (2009), at 124.

[228] L. Muir, *The Case against an International Cyberwarfare Convention*, Wake Forest Law Review Online 5 (2011), at 7.

[229] Others are D. Hollis, *Why States Need an International Law for Information Operations,* Lewis and Clark Law Review 11 (2007); K. Geers, *Cyber Weapons Convention*, 5 Computer Law and Security Law Review 26 (2010); D. Elliot, Weighting the Case of a Convention to Limit Cyberwarfare, Arms Control Association (2009); S. Shackleford/R. Andres, *State Responsibility for*

imagines a convention with a layout comparable to API, encompassing definitions of the terms in question and restating the importance of IHL principles. Following a general introduction, specific rules on cyber attacks expected to cause unnecessary suffering, prohibitions to target specifically protected sites as well as regulations concerning the matter of neutrality would be listed. Important in this regard, Shulman adds, the inclusion of enforcement mechanisms in such a treaty, herewith referring to individual criminal responsibility as well as State responsibility. He suggests including a clause conferring the prosecution of cyber warcrimes to the jurisdiction of the ICC.[230] Another enforcement mechanism, one could consider, is a compromissory clause to the ICJ, by virtue of Article 36 ICJ Statute, giving the court the power to adjudicate questions regarding the interpretation and application of a convention, and also claims for injury of States that are for instance victims of cyber attacks; both suggestions essential to ensure the implementation and enforcement of a possible treaty.

On the other hand, opponents of a new treaty, as for instance Kelsey, argue it would be "neither possible nor necessary"[231]. The analysis in this thesis supports this statement. Firstly no intention within the international community to draft and eventually ratify a new treaty on cyber warfare can be observed: There is increasing political awareness of the uncertainties and vulnerabilities surrounding that new phenomenon, on the national level, with States establishing centres and departments in their governments in charge of cyber technology and defence research. And also on the international level, for instance within the UN, the severity of the problem and possible regulations has been acknowledged. Ban Ki Moon announced in 2009, that the disarmament board will "[…] be considering cyber warfare and its impact on international security. As you know, there have been many widely reported breaches of information systems in recent years. With both the public and private sectors growing increasingly dependent on electronic information, […] work in this area is very timely."[232] However, these efforts can be considered under the umbrella of disarmament affairs and regulations concerning internet security in times of peace; they are not concerned with the application of the law of armed conflict and cyber warfare.[233] In general, one can find that drafting an international

Cyber Attacks: Competing Standards for a Growing Problem, Georgia Journal of International Law 42 (2011).

[230] To date, no such regulation is incorporated into the Rome Statute's Art. 8; Mark R. Shulman, *Discrimination in the Laws of Information Warfare*, Columbia Journal of Transnational Law 37 (1999), at 965.

[231] Kelsey, *supra* note 8, at 1449.

[232] K. Ban, Secretary-General's remarks to the Advisory Board on Disarmament Matter (2009), http://www.un.org/apps/sg/sgstats.asp?nid=3717 http://www.un.org/apps/dsg/sgstatsarchive.asp (2 July 2012).

[233] One major multilateral instrument concerning the use of cyber operations during times of peace is the European Convention on Cybercrime that opened for signature in November 2001, entered into force in 2004, and has to date 35 European state parties and with Japan and USA two non-European members. For further information see

treaty is always a long term project with unclear outcome and in the area of cyber space there still exist many technological uncertainties and legal disagreements, further adding to the general reluctance of States to bind themselves. The problem of attributing cyber operations, protecting national sovereignties or private data, considerably enhances the problem of compliance and enforcement of possible treaty obligations.[234]

Secondly and regarding the question of necessity: Within the legal framework of IHL, new regulations are not needed. The principles and specific regulations can be applied, although it will probably cause irritation among those deploying the technology themselves. A strict interpretation of the rules renders a majority of deployments unlawful and in violation of the IHL principles. A new treaty on the deployment of cyber attacks in armed conflicts, reinforcing the traditional premises of IHL, would not change this assessment.

Discussing the specific difficulties surrounding cyber technology, for times of peace and times of armed conflicts, it nonetheless becomes obvious that cooperation on the international plane and assistance in attributing impairing operations is essential. For this reason it might be wise to consider other instruments to increase control over cyber technology on a multilateral basis. Apart from creating soft law mechanism, as for instance rules of engagement and codes of conducts, it is also efficient to focus on the evolvement of State practice and *opinio juris*, to eventually form specific binding law of customary nature to support and strengthen the contemporary applicable legal framework. For the time being however, the existing IHL framework is flexible enough to adapt to the new circumstances and two modern technologies.

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (20 August 2012).

[234] *Cf.* Geers, *supra* note 190, at 550.

6. References

*

Aerial Bombardment and Related Claims between the State of Eritrea and The Federal Democratic Republic of Ethiopia, Partial Award – Western Front, Eritrea-Ethiopia Claims Commission, 10 December 2005.

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

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

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

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

Convention (IV) Respecting the Laws and Customs of War on Land, 18 October 1907, and its Annex: Regulations Concerning the Laws and Customs of War on Land.

Convention on the Prohibitions or Restrictions on the Use of Certain Conventional Weapons, Geneva, 10 October 1980.

European Convention on Cybercrime, http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (20 August 2012).

Federal Ministry of Defence, *Humanitarian Law in Armed Conflict - Manual*, 2 Zentrale Dienstvorschrift 15 (1992).

Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign against The Federal Republic of Yugoslavia (2000), http://www.un.org/icty/pressreal/nato061300.htm (2 August 2012).

Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion of 8 July 1996, ICJ Reports 1996 (Dissenting Opinion Judge Weeramantry).

Military and Paramilitary Activities in and Against Nicaragua (Nicaragua *v.* United States), Merits, ICJ Reports 1986.

Public Committee against Torture in Israel *v.* Government of Israel *et al.*, High Court of Justice 769/02, Judgment of 13 December 2006.

Program on Humanitarian Policy and Conflict Research at Harvard University, Manual on International Law Applicable to Air and Missile Warfare (2009), ihlresearch.org/amw/HPCR%20Manual.pdf (10 July 2012).

Prosecutor *v.* Galic, Decision on the Motion for the Entry of Acquittal of the Accused Stanislav Galic, Case No IT-98-29-T, 5 December 2003, T. Ch. II.

Prosecutor *v.* Kunarac, Kovac and Vukovic, Case No IT.96-23&23/1, 12 June 2000, A. Ch.

Prosecutor *v.* Tadic, Opinion and Judgment, Case No IT-94-1-T, T.Ch. II, 7 May 1997, T. Ch.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts of 8 June 1977.

Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of Non-International Armed Conflicts.

The Public Committee against Torture in Israel *v.* The Government of Israel, High Court of Justice 769/02, 13 December 2006.

Declaration Renouncing the Use, in Time of War, of Explosive Projectiles under 400 Grammes Weight of 29 November/11 December 1868.

Tallinn Manual on the International Law Applicable to Warfare of the NATO Cooperative Cyber Defence Centre of Excellence (Draft version), http://www.ccdcoe.org/379.html (12 September 2012).

The USAF Intelligence Targeting Guide. Air Force Pamphlet 14-210 (1998).

**

Abi-Saab, R., 1984. *The Specifications of Humanitarian Law*, in C. Swinarski (Ed.) Studies and Essays on International Law and Red Cross Principles in Honour of Jean Pictet.

Agenda for Humanitarian Action adopted by the 28th International Conference of the Red Cross and Red Crescent, Geneva, 2-6 December 2003.

Alexander, Y., 1999/2000. *Terrorism in the Twenty-First Century: Threats and Responses*, 12 DePaul Business Law Journal 59, 59-96.

Asa, K., 2007. *The Principle of Distinction*, 2 Journal of Military Ethics 6, 168-171.

Ban, K., 2009,.Secretary-General's remarks to the Advisory Board on Disarmament Matter, http://www.un.org/apps/sg/sgstats.asp?nid=3717 http://www.un.org/apps/dsg/sgstatsarchive.asp (2 July 2012).

Bialke, J., 2004. *Al-Qaeda & Taliban. Unlawful Combatant Detainees, Unlawful Belligerency, and the International Law of Armed Conflict*, 1 Air Force Law Review 55, 1-85.

Billo, C./Chang, W., 2004. Cyber Warfare. An Analysis of the Means and Motivations of Selected Nation States, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf (8 June 2012).

Binz, G., 1960. *Die Martens`sche Klausel*, Wehrwissenschaftliche Rundschau-Zeitschrift für die Europäische Sicherheit, 139-160.

Blank, L./Farley, 2010. B., *Characterizing United States Operations in Pakistan: Is the U.S. Enganged in An Armed Conflict?,* Fordham International Law Journal 34, 151-189.

Blum, G./Heymann, P., 2010. *Law and Policy of Targeted Killing*, 1 Harvard National Security Journal 45, 145-170.

Boor, F., 2011. *Der Drohnenkrieg in Afghanistan und Pakistan*, 2 Humanitäre Informationsschriften 24, 97-104.

Boothby, B., 2010. *`And for Such Time As´: The Time Dimension to Direct Participation in Hostilties*, New York University International Law and Policy 42, 741-767.

Boothby, B., 2011. *The Law Relating to Unmanned Aerial Vehicles, Unmanned Combat Air Vehicles and Intelligence Gathering from the Air*, 2 Humanitäre Informationsschriften 24, 81-91.

Bothe, M./Partsch, K./Solf, W., 1982. New Rules for Victims of Armed Conflicts: Commentary on the Two 1977 Protocols Additional to the Geneva Conventions of 1949.

Bowcott, O., Drone Strikes Threaten 50 Years of International Law, Says UN Rapporteur, The Guardian, 21 June 2012, http://www.guardian.co.uk/world/2012/jun/21/drone-strikes-international-law-un (18 August 2012).

Braybrook, R., 2009. *Strike Drones: Persistent, Precise and Plausible*, 4 Armada International 33, 20-23.

Brown, B., 1976. *The Proportionality Principle in the Humanitarian Law of Warfare: Recent Efforts in Codification,* Cornell International Law Journal 10, 134-155.

Brown, D., 2006. *A Proposal for an International Convention to Regulate the Use of Information Systems in Armed Conflict*, 1 Harvard International Law Journal 47, 179-221.

Buchan, R., 2012. *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 2 Journal of Conflict and Security Law 17, 212-227.

Callen, J., 2004. *Unlawful Combatants and the Geneva Conventions*, 4 Virginia Journal of International Law 44, 1025-1072.

Cassese, A., 2000. *The Martens Clause: Half a Load of Simply Pie in the Sky?*, European Journal of International Law 11, 187-216.

DeCock, C., 2010. *Counterinsurgency Operations*, in: M. Schmitt/T. McCormack/L. Arimatsu (Eds.), Yearbook of International Law.

DeYoung, K./Warrick, J., Under Obama, More Targeted Killings than Captures in Counterterrorism Efforts, Washington Post, 14 February 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/02/13/AR2010021303748.html?nav = emailpage (16 July 2012).

Dinstein, Y., 2004. The Conduct of Hostilities under the Law of International Armed Conflict.

Dinstein, Y., 2012. *The Principle of Distinction and Cyber War in International Armed Conflicts*, 2 Journal of Conflict & Security Law 17, 261-277.

Dörrmann, K., 2003. *The Legal Situation of 'Unlawful/Unprivileged Combatants'*, in 85 International Review of the Red Cross 849, 45-74.

Dunant, H., 1862. A Memory of Solferino, in ICRC Publication 1986.

Dunlap, C., 2011. *Perspectives for Cyber Strategists on Law for Cyberwar*, 2 Strategic Studies Quarterly, 81-99.

Elliot, D.S., 2009. Weighting the Case of a Convention to Limit Cyberwarfare, Arms Control Association.

Expert Meeting, Targeting Military Objectives (2005), University Centre for International Humanitarian Law,

http.://www.ucihl.org/research/military_objective_symposium_report.pdf. (3 July 2012).

Fenrick, W., 1997. *Attacking the Enemy Civilian as a Punishable Offense*, 2 Duke Journal of Comparative and International Law 7, 539-570.

Focus, 25 September 2010, http://www.focus.de/politik/deutschland/verteidigung-bundeswehrverband-draengt-auf-beschaffung-von-drohnen_aid_826082.html (25 September 2012).

Franklin, M., 2008. Future Weapons Foe Unmanned Combat Air Vehicles.

Frau, R., 2011. *Unbemannte Luftfahrzeuge im internationalen bewaffneten Konflikt*, 2 Humanitäre Informationsschriften 24, 60-72.

Geers, K., 2010. *Cyber Weapons Convention*, 5 Computer Law and Security Law Review 26, 547-551.

Gogarty, B./Hagger, M., 2008. *The Laws Of Man over Vehicles Unmanned: The Legal Response to Robotic Revolution on Sea, Land and Air*, Journal of Law, Information and Science 19, 73-145.

Gormley, D., 2003. *New Developments in Unmanned Air Vehicles and Land-Attack Cruise Missiles*, SIPRI Yearbook.

Graham, B., Bush Orders Guidelines for Cyber-Warfare, Washington Post, 7 February 2003, http://www.stanford.edu/class/msande91si/www-spr04/readings/week5/bush_guidelines.html (20 August 2012).

Graham, D., 2010. *Cyber Threats and the Law of War*, 1 Journal of National Security 4, 87-102.

Gutman, R./Kuttab, D., 2007. *Indiscriminate Attacks*, in: R. Gutman/D. Rieff/A. Dworkin (Eds.), Crimes of War: What the Public Should Know.

Hayashi, N., 2010. *Requirements of Military Necessity in International Humanitarian Law and International Criminal Law*, 28 Boston University International Law Journal 1, 39-140.

Hakimi, M., 2012. *A Functional Approach to Targeting and Detention*, Michigan Law Review 110, 1365-1420.

Henckaerts, J.M., 2005. *Study on Customary International Humanitarian Law: A Contribution to the Understanding and Respect for the Rule of Law in Armed Conflict*, 87 International Review of the Red Cross 857, 176-212.

Henckaerts, J.-M./Doswald-Beck, L. (Eds.), 2005. Customary International Humanitarian Law, Vol. 1: Rules.

Henderson, I., 2009. The Contemporary Law of Targeting. Military Objectives, Proportionality and Precautions in Attack under Additional Protocol I.

Hollis, D., 2007. *Why States Need an International Law for Information Operations,* Lewis and Clark Law Review 11, 1023-1063.

Hughes, R., 2010. Towards a Global Regime for Cyber Warfare.

Human Rights Watch, 1991. Needless Deaths in the Gulf War: Civilian Casualties During the Air Campaign and Violations of the Laws of War, http://www.hrw.org/reports/1991gulfwar/ (18 July 2012).

ICRC, A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977, 2006, www.icrc.org/eng/.../irrc_864_icrc_geneva.pdf. (21 August 2012).

ICRC, *What Is International Humanitarian Law*, Legal Fact Sheet 7 (2004), http://www.icrc.org/eng/resources/documents/legal-fact-sheet/humanitarian-law-factsheet.htm (8 October 2012).

ICRC, International Humanitarian Law and Challenges of Contemporary Armed Conflicts, 28th International Conference of the Red Cross and Red Crescent, Geneva (2003), www.icrc.org/.../ihlcontemp_armedconflicts_final_ang.pdf. (29 August 2012).

ICRC, Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law (2009), www.icrc.org/eng/.../review-872-p991.htm (18 July 2012).

ICRC, Review of New Weapons (29 October 2010), http://www.icrc.org/eng/war-and-law/weapons/new-weapons/overview-review-of-new-weapons.htm (20 August 2012).

ICRC, Summary Report, Second Expert Meeting on the Notion of Direct Participation in Hostilities, The Hague (2004), www.icrc.org/.../2004-07-report-dph-2004-icrc.pdf (2 August 2012).

ICRC, Statement at the UN Diplomatic Conference of Plenipoteniaries on the Establishment of an International Criminal Court, 8 July 1998, UN Doc. A/Conf.183/INF/10, 13 July 1998.

International Human Rights and Conflict Resolution Clinic at Stanford Law School and Global Justice Clinic at NYU School of Law, Living under Drones: Death, Injury, and Trauma to Civilians from the US Drone Practices in Pakistan (2010), http://livingunderdrones.org/download-report/ (3 October 2012).

Intoccia, G./Moore, J., 2006. *Communications Technology, Warfare and the Law of War: Is the Network a Weapon System?*, 2 Houston Journal of International Law 28, 467-498.

Jastram, K./Quintin, A., The Internet in Bello: Cyber War Law , Ethics & Policy. Seminar held 18 November 2011, Berkeley Law, cybewarfare_seminar—summary_032612.pdf (25 October 2012).

Jenks, C., 2009. *Law from Above: Unmanned Aerial Systems, Use of Force, and the Law of Armed Conflict*, North Dakota Law Review 85, 649-671.

Kellenberger, J., International Humanitarian Law and New Weapons Technology, Keynote address at the 34th Round Table on Current Issues of International Humanitarian Law, San Remo, 09 August 2011, http://www.icrc.org/eng/resources/documents/statement/new-weapon-technologies-statement-2011-09-08.htm (2 August 2012).

Kellenberger, J., International Humanitarian law at the Beginning of the 21 Century, Keynote address at the 26th Round Table in San Remo on Current Problems of International Humanitarian Law, 05 September 2002, http://www.icrc.org/eng/resources/documents/misc/5e2c8v.htm (2 August 2012).

Kelsey, J., 2008. *Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare*, Michigan Law Review 106.

Kleffner, J., 2007. *From „Belligerents" to „Fighters" and Civilians Directly Participating in Hostilities*, Netherlands International Law Review 54, 315-336.

Koh, H., Keynote Address at the American Society for International Law Annual Meeting: The Obama Administration and International Law (21 March 2010), http://www.state.gov/s/l/releases/remarks/139119.htm (12 July 2012).

Kurbjuweit, D., Smarter Sensemann, Deutschland will Kampfdrohnen anschaffen. Sind sie eine humane Waffe?, der Spiegel 32, 6. August 2012.

Laursen, A., 2002. *NATO, the War over Kosovo, and the ICTY Investigation*, American University International Law Review 17, 765-814.

Lauterbach, H., 1953. *Hostages Trial*, in: H. Lauterbach (Ed.), Annual Digest and Reports of Public International Law Cases: a Selection from the Decision of International Courts and Tribunals and Military Courts Given During the Year 1948.

Libicki, M., 2009. Cyberdeterrence and Cyberwar, RAND Corporation.

Llezna, M., 2011. *Targeted Killings in Pakistan: A Defense*, 2 Global Security Studies 2, 47-59.

Lord Wright, Foreword, in *Law Reports of Trials of War Criminals*, Volume XV, www.loc.gov/rr/frd/Military_Law/pdf/Law-Reports_Vol-15.pdf (2 August 2012).

Lubell, N., 2007, *Parallel Application of International Humanitarian Law and International Human Rights Law: An Examination of the Debate*, Israel Law Review 40, 648-660.

Markoff, J., Before the Gunfire, Cyberattacks, New York Times, 12 August 2008, http://www.nytimes.com/2008/08/ (2 June 2012).

Marsh, J./Glabe, S., 2011, *Times for the United States to Participate*, 1 Virginia Journal of International Law 13, 13-25.

Mayer, J., The Predator War, What are the Risk of the CIA's Covert Drone Program, New Yorker, 26 October 2009, http://www.newyorker.com/reporting/2009/10/26/09102

McDonald, A., 2004. The Challenges to International Humanitarian Law and The Principle of Distinction and Protection from the Increased Participation of Civilians in Hostilities, Expert Analysis of the T.M.C. Asser Institute, http://www.asser.nl/default.aspx?site_id=9&level1=13337&level2=13379 (18 August 2012).

McNab, M./Matthews, M., 2010-2011. *Clarifying the Law Relating to Unmanned Drones and the Use of Force: the Relationship between Human Rights, Self-Defence, Armed Conflict and International Humanitarian Law,* Denver Journal of International Law and Policy 39, 661-730.

Melzer, N., 2009. Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, http://www.icrc.org/eng/resources/documents/publication/p0990.htm (7 October 2012).

Melzer, N., 2010. *Keeping the Balance between Military Necessity and Humanity: A Response to the four Critiques of the ICRC's Interpretative Guidance on the Notion of Direct Participation in Hostilities*, New York University Journal of International Law and Policy 42, 833-916.

Meron, T., 2000. *The Martens Clause, Principle of Humanity, and Dictates of the Public Conscience*, American Journal of International Law 94, 78-89.

Muir, L., 2011. *The Case against an International Cyberwarfare Convention*, Wake Forest Law Review Online 5, 5-12.

Murphy, R., 2000. *International Humanitarian Law Training for Multinational Peace Support Operations – Lessons from Experience*, International Review of the Red Cross 840.

Murphy, R./Radsan, J., 2009. *Due Process and Targeted Killing of Terrorists*, Cardozo Law Review 31, 405-453.

NASA Fact Sheet (22 March 2012), http://www.nasa.gov/centers/dryden/news/FactSheets/FS-098-DFRC.html; US Air Force Fact Sheet (21 January 2012), http://www.af.mil/information/factsheets/factsheet.asp?id=13225 and http://www.globalsecurity.org/intell/systems/global_hawk.htm (All seen on 8 July 2012).

Newman, R., 2002. *The Little Predator That Could*, 3 Air Force Magazine 85, 48-53.

O'Connell, M., 2012. *Cyber Security without Cyber War*, 2 Journal of Conflict and Security Law 17, 187-209.

O'Connell, M., Rise of Drones II: Unmanned Systems and the Future of Warfare: Hearing before the U.S. House Subcommittee on National Security and Foreign Affairs (28 April 2010), Written testimony of Mary Ellen O'Connell, http://oversight.house.gov/images/stories/subcommittees/NS -Subcommittee/4.28.10-Drones Il/OConnell Statement.pdf (8 June 2012).

O'Connell, M., 2010. *Unlawful Killing with Combat Drones. A Case Study of Pakistan, 2004-2009*, Notre Dame Law School Legal Studies Research Paper 7.

O'Donnell, B./Kraska, 2003. J., *Humanitarian Law: Developing International Rules for the Digital Battlefield*, Journal of Conflict and Security Law 8, 133-160.

Rogers, A.,2004. Law on the Battlefield.

Röhling, B., 1960. International Law in an Expanded World.

Rudolf, P./Schaller, 2012. C., *Targeted Killing. Zur völkerrechtlichen, ethnischen und strategischen Problematik in der Terrorismus- und Aufstandsbekämpfung*, SWP-Studie 1.

Sandoz, Y./ Swinarski, C./Zimmermann, B. (Eds.), 1987. Commentary on the Additional Protocols of 8 June 1977 to the Geneva Conventions of 12 August 1949.

Sassôli, M., 2003. *Legitimate Targets of Attacks Under International Humanitarian Law*, International Humanitarian Law Research Initiative, Background Paper 7, www.hpcrresearch.org/sites/.../files/.../Session1.pdf (2 June 2012).

Schaap, A., 2009..*Cyber Warfare Operations: Development and Use under International Law*, Air Force Law Review 64, 121-173.

Schmitt, M., 2004. 'Direct Participation in Hostilities' and 21st Century Armed Conflict, http://www.michaelschmitt.org/images/Directparticipationpageproofs.pdf (15 July 2012).

Schmitt, M., 1988. *Bellum Americanum: The US View of Twenty-first Century War and Its Possible Implications for the Law of Armed Conflict*, Michigan Journal of International Law 19, 1051-1090.

Schmitt, M., 2012. *Classification of Cyber Conflict*, 2 Journal of Conflict & Security Law 17, 245-260.

Schmitt, M., 2012. *Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative* Framework, in M. Schmitt (Ed.), Essays on Law and War at the Fault Lines.

Schmitt, M., 2010. *Military Necessity and Humanity in International Humanitarian Law: Preserving the Delicate Balance*, 4 Virginia Journal of International Law 50, 795-839.

Schmitt, M., 2005. *Precision Attack and International Law*, 87 International Review of the Red Cross 859.

Schmitt, M., 2004. *Targeting and Humanitarian Law: Current Issues*, 34 Israel Yearbook on Human Rights 59.

Schmitt, M., 2010. *The Interpretive Guidance on the Notion of Direct Participation in Hostilities: A Critical Analysis*, Harvard National Security Journal Online 1.

Schmitt, M., 1999. *The Principle of Distinction in 21st Century Warfare*, Yale Human Rights and Development Law Journal 2, 143-182.

Schmitt, M., 2002. *Wired Warfare: Computer Network Attack and the Jus in Bello*, in M. Schmitt/ B. O'Donnell (Eds.), Computer Network Attack and International Law.

Schwarzenberg, G., 1958. The Legality of Nuclear Weapons.

SearchSecurity.com, Trojan Horse, http://searchsecurity.techtarget.com/sDefmition/ 0,,sidl4_gci213221,00.html (2 June 2012).

Serabian, J., Jr., Statement for the Record Before the Joint Economic Committee on Cyber Threats and the US Economy (23 February 2000), https://www.cia.gov/ news-information/speeches-testimony/2000/cyberthreats_022300.html (2 June 2012).

Shackleford, S./Andres, R., 2011. *State Responsibility for Cyber Attacks: Competing Standards for a Growing Problem*, Georgia Journal of International Law 42.

Shulman, M., 1999. *Discrimination in the Laws of Information Warfare*, Columbia Journal of Transnational Law 37, 939-968.

Singer, P., 2009. *Military Robots and the Laws of War*, The New Atlantis 23, 25-45.

Singer, P., 2009. Wired For War.

Sklervov, M., 2009. *Solving the Dilemma of State Reponses to Cyberattacks*, Military Review 201,1-85.

Solf, W., 1986. *Protection of Civilians Against the Effects of Hostilities under Customary International Law and under Protocol I*, 1 American University Journal of International Law and Policy 117, 117-135.

Stone, J., 1954. Legal Controls of International Conflict: A Treatise on the Dynamics of Disputes and War Law.

Strebel, H., 1997. *Martens Clause*, in R. Bernhard (Ed.), Encyclopedia of Public International Law.

Stroh, P., 2011. *Der Einsatz von Drohnen im nicht-internationalen bewaffneten Konflikt*, 2 Humanitäre Informationsschriften 24, 73-77.

Swiney, G., 2006. *Saving Lives: the Principle of Distinction and the Realities of Modern War*, 3 The International Lawyer 39, 733-758.

The Tech Terms Computer Dictionary, Malware, http://www.techterms.com/definition/malware (26 June 2012).

Third Expert Meeting on the Notion of Direct Participation in Hostilities: Summary Report, International Committee of the Red Cross (2005), www.icrc.org/.../2005-09-report-dph-2005-icrc (15 August 2012).

Thirlway, H., 2010. *The Sources of International Law*, in: M. Evans (Ed.), International Law.

Turns, D. 2012. *Cyber Warfare and the Notion of Direct Participation in Hostilities*, 2 Journal of Conflict and Security Law 17, 279-297.

Turns, D., 2010. *The Law of Armed Conflict*, in M. Evans (Ed.) International Law.

Tsagourias, N., 2012. *Cyber Attacks, Self-Defense and the Problem of Attribution*, 2 Journal of Conflict & Security Law 17, 187-209.

U.S. Cyber Consequences Unit, Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008 (2009), www.registan.net/.../US-CCU-Georgia-Cyber-Campaign.pdf (2 June 2012).

US Army Centre of Excellence, Eyes of the Army: US Army Roadmap for UAS 2010-2035 (2010), Report No. ATZQ-CDI-C-72, http://www.fas.org/irp/program/collect/uas-army.pdf (12 July 2012).

Vogel, R., 2011. *Drone Warfare and the Law of Armed Conflict*, Denver Journal of International Law and Policy 39, 101-138.

Von Bernstorff, J., 2009. Martens Clause, http://www.mpepil.com/subscriber_article?Script=yes&id=/epil/entries/law-9780199231690-e327&recno=1&searchTyoe=Quick&query=martens+clause (2 August 2012).

Von Buttlar, C./ Stein, T., 2009. Völkerrecht.

Waxman, M., 2001. *Cyber-attacks and the use of force: back to the future of article 2(4) of the UN Charter*, 2 Yale Journal of International Law 36, 421-459.

Waxman, M., 2000. International Law and the Politics of Urban Air Operations, RAND Corporation, http://www.rand.org/publications/MR/MR1175 (12 July 2012).

Weiner, J., 2012. *Targeted Killings and Double Standards*, Strategic Perspectives 9.

Wilson, C., 2008. *CRS Report for Congress: Botnets, Cybercrime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*, www.fas.org/sgp/crs/terror/RL32114.pdf (26 June 2012).

Wortham, A., 2012. *Should Cyber Exploitation Ever Constitute a Demonstration of Hostile Intent That May Violate UN Charter Provisions Prohibiting the Threat or Use of Force?*, 3 Federal Communications Law Journal 64, 643-660.

Ziolkowski, K., 2011. *Stuxnet. Legal Considerations*, 3 Humanitäre Informationsschriften 24, 139-148.

IFHV Working Paper Series

URL: http://www.rub.de/ifhv/6-publications/6-workingpapers.html

ISSN: 2199-1367

List of published IFHV Working Papers

Vol. 1, No. 1
03/2011
Huseyn Aliyev
Aid Efficiency in an Armed Conflict
The Role of Civil Society in the Escalation of Violence in the North Caucasus
http://www.rub.de/ifhv/documents/workingpapers/wp1_1.pdf

Vol. 1, No. 2
08/2011
Matteo Garavoglia
Germany's Humanitarian Aid and Media Reporting on Natural Catastrophes
An Investigation of the Relationship between Issue Salience and the Provision of Humanitarian Aid at the Beginning of the 21st Century
http://www.rub.de/ifhv/documents/workingpapers/wp1_2.pdf

Vol. 2, No. 1
05/2012
Jan Wulf
A Balanced Scorecard for the Humanitarian Sector?
Adaptability of the Balanced Scorecard Model to Sector-Wide Performance Management in Humanitarian Aid – Feasibility and Implications
http://www.rub.de/ifhv/documents/workingpapers/wp2_1.pdf

Vol. 2, No. 2
08/2012
Johannes Beck
Contested Land in the Eastern Democratic Republic of the Congo
Anatomy of the Land-Related Intervention
http://www.rub.de/ifhv/documents/workingpapers/wp2_2.pdf

Vol. 3, No. 1
10/2013
Markus Koth
Civil-Military Cooperation and lts Impact on Human Security – Chances and Limits
The Example of the Australian Defence Forces in East Timor (1999 and 2006)
http://www.rub.de/ifhv/documents/workingpapers/wp3_1.pdf

Vol. 3, No. 2
10/2013
Heiko Fabian Königstein
The Influence of Mental Health on Reconciliation in Post-War Lebanon
An Explorative Field Based Study Using Grounded Theory Research
http://www.rub.de/ifhv/documents/workingpapers/wp3_2.pdf

Vol. 3, No. 3
12/2013
Charlotte Lülf
Modern Technologies and Targeting under International Humanitarian Law
http://www.rub.de/ifhv/documents/workingpapers/wp3_3.pdf

IFHV Working Paper Series

URL: http://www.rub.de/ifhv/6-publications/6-workingpapers.html

ISSN: 2199-1367

Manuscripts can be submitted to the editors:

Prof. Dr. Pierre Thielbörger, ifhv@rub.de
Dr. Kerstin Rosenow-Williams, ifhv@rub.de

IFHV Working Paper Series

URL: http://www.rub.de/ifhv/6-publications/6-workingpapers.html

ISSN: 2199-1367

Institute for International Law of Peace and Armed Conflict (IFHV)

The Institute for International Law of Peace and Armed Conflict (Institut für Friedenssicherungsrecht und Humanitäres Völkerrecht, IFHV) was established in 1988 by decision of the University Senate as a central research unit ('Zentrale Wissenschaftliche Einrichtung') of the Ruhr University Bochum. The IFHV is responsible directly to the Rector and the Senate of the Ruhr University Bochum, but works in close cooperation with the different faculties, in particular the faculties of law, social science, geosciences and medicine.

The IFHV carries out research and teaching on the problems of peace and armed conflict from an inter-disciplinary perspective. Based on its strong international humanitarian law tradition, the IFHV is the only institute in Germany, and one of very few in Europe and the world, which is dedicated to the discipline of humanitarian studies. The IFHV combines its strong emphasis on international humanitarian law, the law of peace and human rights law with sociological and political perspectives on humanitarian crises, actors and activities.

IFHV Working Paper Series

In 2011, the IFHV and the Ruhr University Bochum decided to set up an IFHV Working Paper Series in humanitarian studies. In line with the IFHV's multidisciplinary profile, we intend to publish a broad range of papers in the field of humanitarian studies. Our Working Paper Series publishes 'work in progress'. The Working Paper Series intends to stimulate the humanitarian discourse, contribute to the advancement of the knowledge and understanding of the practices, policies and norms of humanitarian action, and last but not least seeks to attract comments, which improve the content of the working paper for further publications.

The Working Paper Series allows IFHV staff and students, and like-minded researchers in the field of humanitarian studies to bring their work and ideas to the attention of a wider audience. In order to publish high level working papers, the papers offered for publication will be technically screened by the editors of the working paper series and subjected to an internal blind peer review process.

Contact:

Institute for International Law of Peace and Armed Conflict (IFHV)
NA 02/33
Ruhr University Bochum
Universitätsstraße 150
44780 Bochum
Germany

Telephone: +49(0)234 32 27366
Fax: +49(0)234 32 14208
Email: ifhv@rub.de
Web: www.ifhv.de
Facebook: www.facebook.com/rub.ifhv