TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Teemu Tapio Kärki

Drones, autonomous weapons and cyber warfare: Is Additional Protocol I art. 36 still able to govern contemporary weapons?

Bachelor Thesis

Supervisor: Evhen Tsybulenko, Ph.D.

Tallinn 2017

Statement on plagiarism

I hereby declare that I am the sole author
of this Bachelor Thesis and it has
not been presented to any other
university of examination.

Teemu Kärki
……..... 2017

The Bachelor Thesis meets the established requirements

Supervisor Evhen Tsybulenko
……..... 2017

Accepted for examination 2017

Board of Examiners of Law Bachelor's Theses

.....

Table of contents

Introduction 4

1. General principles of international humanitarian law and international security 6

1.1. Superfluous injury and unnecessary suffering 6

1.2. Indiscriminate attacks and principle of distinction 7

1.3. Damage to natural environment 8

1.4. Principles of proportionality and precautions 9

1.4.1. Principle of proportionality 9

1.4.2. Principle of precautions 10

1.5. Geneva Convention Additional Protocol I article 36 - New weapons 11

1.6. Principles of sovereignty and neutrality 12

2. General overview of weapons in question 14

2.1. Unmanned aerial vehicles also known as drones 14

2.2. Autonomous weapons 16

2.3. Cyber warfare 17

3. Legal analysis of above-mentioned weapons 19

3.1. Legal problems 19

3.1.1. Drones 19

3.1.1.1. Principles of precautions, distinction and proportionality 19

3.1.1.2. Targeted killings 20

3.1.2. Autonomous weapons 21

3.1.2.1. Distinction and precautions 21

3.1.2.2. Proportionality 22

3.1.3. Cyber warfare 23

3.1.3.1. Distinction and proportionality 23

3.1.3.2. Sovereignty and neutrality 25

3.4. Responsibility 27

3.4.1. Pecuniary accountability 27

3.4.2. Criminal liability 30

3.5 Proposals to the legal problems 34

Conclusion 40

Abbreviations

AP I	Additional Protocol I to the Geneva Conventions
AWS	Autonomous weapons system
CIA	Central Intelligence Agency
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
UAV	Unmanned aerial vehicle

Introduction

Warfare live in a period of transition. Conventional means of warfare have been joined with new means and methods. Robots are not just part of the future discussion and science fiction. Even civil persons can acquire an robot to protect himself.[1] War is not longer just human power, but the machines and artificial intelligence play a role in forming modern warfare. In the future, the role of machines and artificial intelligence presumably grow and, therefore, it is necessary to consider the ability of the current legislation to manage new types of weapons.

Current rules of international humanitarian law are dozens of years old or even much older. This raises questions whether the existing legislation is capable of governing the contemporary weapons such as drones, autonomous weapons and cyber warfare. The purpose of the thesis is to find out whether the existing legislation is adequate, and what should be done to improve the situation.

Thesis seeks to ascertain what legal problems the above-mentioned weapons are creating within the framework of the current legislation. Is there a need to change the existing laws or create entirely new ones? Thesis will also discuss how these weapons should be regulated, by treaty, State practice or in some other way.

In the first part, the author goes through the most essential and the most important rules and principles of international humanitarian law and international security. This is intended to outline what kind of means and methods of warfare are permitted and prohibited. Next, the author introduces the weapons, which are dealt in the thesis. This gives a broader picture of what kinds of weapons the thesis is dealing with, and makes it easier to understand why weapons fulfill certain conditions and may cause problems for the fulfillment of other rules. This chapter is very technical, but structured that way on purpose and needed for the better understanding of the legal implications. This is followed by the main part of the thesis, which analyzes the rules of international humanitarian law and international security presented at the beginning, and how

[1] Terzian, D. Right to Bear (Robotic) Arms. Penn State Law Review, 2013, 117, (3), pp 755-796, p 756.

above-mentioned weapons comply with these rules. This contribution brings out what problems these weapons will create within the framework of the current legislation. Lastly, the author elicits the experts' and his own proposals how the current regulations should be changed, so that ambiguities considering legislation presented in the thesis will be settled.

As research methods the author uses explanatory and doctrinal legal research methods. The aim is to clear the current legislation to the reader and then analyse problems in the light of known legislation. Finally, the author discloses alternatives to the current legislation how it could or should be changed.

The author has selected sources from the experts in their fields. This has ensured that the sources deal with things in a versatile and they are accurate. The author has also tried to select mostly a relatively new articles, so that the thesis has been possible to use the current knowledge of the subjects covered.

The thesis deals with three weapons, which are already widely in use or will be in the near future. Therefore, these weapons are very topical question and it is necessary to pay attention to their legal problems. The existence of the weapons is discharged through Additional Protocol I, article 36, which in itself is quite a vast article. It tells States to ensure the legality of a weapon according Additional Protocol I, but in addition State must also consider the legality according to any other rule of international law.

1. General principles of international humanitarian law and international security

1.1. Superfluous injury and unnecessary suffering

The prohibition of the use of means and methods of warfare which are of a nature to cause superfluous injury or unnecessary suffering is a rule which arises in a variety of international agreements.[2] The idea is that means and methods do not cause unnecessary suffering to persons in relation to military purposes.[3] Generally speaking, this is considered a norm of customary international law, which is binding, regardless of whether or not the State is within the scope of the agreement. The first time it was mentioned in the Saint Petersburg Declaration and the Hague Convention and is later confirmed, inter alia, in Article 35 of Additional Protocol I to the Geneva Convention (AP I) and the Ottawa Convention Banning Anti-personnel landmines.[4] It is also included in military manuals of many States as well as State practices.[5]

When talking about the means of warfare, there is no absolute consensus on the manner in which it is determined.[6] Others think that the weapon is forbidden which has no military purpose. Also, the Red Cross Wound Classification system has been utilized in assessing the severity of injuries.[7] Others stress the importance of military advantage, while the third balance between suffering and military necessity.[8] A simple way of defining such means of warfare is through permanent disability.[9] In this respect, good examples of prohibited weapons are such as blinding lasers[10] and anti-personnel mines.[11] On the other hand, the idea of a weapon that would bring the

[2] Rule 70. Weapons of a Nature to Cause Superfluous Injury or Unnecessary Suffering. International Committee of the Red Cross.
www.ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter20_rule70 (4.2.2017). (Hereinafter Rule 70)
[3] Coupland, R. The Effect of Weapons: Defining Superfluous Injury and Unnecessary Suffering 1996.
www.ippnw.org/pdf/mgs/3-coupland.pdf (2.3.2017).
[4] Henckaerts, J-M. et al. Customary international law, volume I, Rules. Cambridge, Cambridge University Press 2005, p 237.
[5] Rule 70, *supra* nota 2.
[6] Gardam, J. Necessity, proportionality and the Use of Force by States. Cambridge, Cambridge University Press 2004, p 67.
[7] Coupland, *supra* nota 3.
[8] Henckaerts, J-M. et al. *supra* nota 4, p 240.
[9] *Ibid*.
[10] Rule 70, *supra* nota 2.
[11] *Ibid.*

inevitable death, is thought to be prohibited. These include, for instance, explosive bullets, which are also known as “dum-dum bullets" and poison.[12]

1.2. Indiscriminate attacks and principle of distinction

Civilians enjoy special protection against hostilities.[13] In any case, civilians must be excluded from military operations.[14] Dissemination of terror among civilians is prohibited. Civilians be subjected to attacks only if they take direct part in hostilities, and only this particular time. Article 51 of AP I, paragraphs 4 and 5 states:

“4. Indiscriminate attacks are prohibited. Indiscriminate attacks are:
(a) those which are not directed at a specific military objective;
(b) those which employ a method or means of combat which cannot be directed at a specific military objective; or
(c) those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol; and consequently, in each such case, are of a nature to strike military objectives and civilians or civilian objects without distinction.

5. Among others, the following types of attacks are to be considered as indiscriminate:
an attack by bombardment by any methods or means which treats as a single military objective a number of clearly separated and distinct military objectives located in a city, town, village or other area containing a similar concentration of civilians or civilian objects; and

an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated.”

[12] *Ibid*.
[13] Sandvik-Nylund, M. Caught in Conflicts: Civilian Victims, Humanitarian Assistance and International Law. Turku, Institute for Human Rights, Åbo Akademi University 2003, p 14.
[14] Rogers, A. Law on the battlefield. Manchester, Manchester University Press 2012, p 11.

Belligerents cannot bomb the entire city to the ground, even if there would be a number of military objectives, because the civilian objects must be distinguished from military objectives. In cases where a State is not part of a separate convention, which limits the use of a particular weapon, for example, the use of cluster bombs,[15] the previous rule still applies. Remarkable is also the fact that belligerents are prohibited to destroy the objects which are essential for the survival of civilians, such as food and water supplies, livestock and irrigation systems.[16] Special consideration must also keep in mind when attacking installations containing dangerous forces, such as dams, and nuclear power plants because these might cause grave danger to civilian lives.[17]

Some objects may be used to both a civilian, and military use. These so-called dual-use targets make it more difficult to apply the principle of distinction. Such applications are, for example, power plants, bridges, and telecommunications. If the above-mentioned objects are used for the benefit of military, they might be subject to change from civilian targets to military targets.[18]

1.3. Damage to natural environment

Article 35 paragraph 3 of AP I lays down a rule to protect the environment: "It is prohibited to employ methods or means of warfare which are intended, or may be expected, to cause widespread, long-term and severe damage to the natural environment." In addition to the above-mentioned rules to protect people from misuse of means and methods of warfare, it has been considered necessary to protect the environment itself. Principle of distinction also applies to the environment. The natural environment is not to be attacked, unless it is a military objective.[19] Protocol III to the Convention on Certain Conventional Weapons states that "it is prohibited to make forests or other kinds of plant cover the object of attack by incendiary weapons except when such natural elements are used to cover, conceal or camouflage combatants or other military objectives, or are themselves military objectives."

[15] The Convention on Cluster Munitions. www.clusterconvention.org/the-convention/convention-text/ (4.2.2017).
[16] Article 54 of Protocol I Additional to Geneva Conventions, International Committee of the Red Cross. ihl-databases.icrc.org/applic/ihl/ihl.nsf/ART/470-750069?OpenDocument (4.2.2017).
[17] Kelsey, J. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the age of Cyber Warfare. Michigan Law Review, 2008, pp 1427-1451, p 1437.
[18] *Ibid*.
[19] Henckaerts, J-M. et al. *supra* nota 4, p 144.

The war itself, and the weapons used during the war, of course, can cause great damage to nature. Attention must also be paid at the times after the war. Booby-traps or mines cause headache after the end of the war, as the clearance is time consuming. Furthermore, that they pose a threat to people, mostly civilians, they pose a threat to environment as well. The matter has been noted as an important, and it is thus regulated.[20]

1.4. Principles of proportionality and precautions

1.4.1. Principle of proportionality

Even if the subject would otherwise be a legitimate military target, and could therefore be attacked, the principle of proportionality limits the means and methods of warfare, which may be used. Article 51 (5)(b) of AP I states that "an attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated." Additional Protocol does not in itself include the term proportionality but may be interpreted as referring to this.[21] This is rule of customary international humanitarian law, which everyone is obliged to comply with.[22]

Some experts consider the principle of proportionality in the context of weapons causing superfluous injury and unnecessary suffering.[23] Some experts have criticized this view. In their view, one must think incidental injury to civilians and collateral damage to civilian objects in proportion to achieved military advantage.[24]

[20] Protocol on Explosive Remnants of War (Protocol V to the 1980 CCW Convention, 28 November 2003), International Committee of the Red Cross. ihl-databases.icrc.org/applic/ihl/ihl.nsf/Treaty.xsp?action=openDocument&documentId=22EFA0C23F4AAC69C1256E280052A81F (4.2.2017).
[21] Liu, H. Categorization and legality of autonomous and remote weapons systems. International Review of the Red Cross, 2012, 94 (886), pp 627-652, p 642.
[22] Henckaerts, J-M. et al. *supra* nota 4, p 46.
[23] Liu, *supra* nota 21, p 642.
[24] *Ibid.*

In some situations, there is no time to think about whether the attack is disproportionate or not, while in other cases there may be more time to think. In such a situation the advantage of civilians should be the first priority.[25]

The principle of proportionality does not mean that civilians must not be targeted in attack at all, but this needs to be carefully justified. Jenks stresses that the idea behind the principle is that civilians may be harmed during the attacks against legitimate military targets.[26] The application of the principle of proportionality is not as simple as comparing the number of civilians injured or killed with those of combatants.[27] Military advantage is always under consideration and personal assessment of the current commander and normally they enjoy a high degree of discretion with regard to the principle of proportionality.[28]

1.4.2. Principle of precautions

Precautions in attacks are directly related to the rules, such as the principle of proportionality, the principle of distinction and means or methods of warfare which cause superfluous injury and unnecessary suffering and the primary idea is the protection of civilians.[29] According to Article 57 paragraph 2 of AP I:

"(a) those who plan or decide upon an attack shall:

(i) do everything feasible to verify that the objectives to be attacked are neither civilians nor civilian objects and are not subject to special protection but are military objectives within the meaning of paragraph 2 of Article 52 and that it is not prohibited by the provisions of this Protocol to attack them;

[25] Casey-Maslen, S. Pandora's box? Drone strikes under jus ad bellum and jus in bello, and international human rights law. International Review of the Red Cross, 2012, 94 (886), pp 597-625, p 612.
[26] Jenks, C. Law from above: unmanned aerial systems, use of force, and the law of armed conflict. North Dakota law review, 2009, 85 (649), pp 649-672, p 667 cited in Beard (Beard J. Law and war in the virtual era. American Journal of International Law 2009, p 409, 427).
[27] Jenks, *supra* nota 26, p 667.
[28] *Ibid*.
[29] Casey-Maslen, *supra* nota 25, p 606.

(ii) take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects;

(iii) refrain from deciding to launch any attack which may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects, or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated;"

Precautions may include, for example, large-scale reconnaissance of the area concerned, the assessment of the collateral damage caused and "no strike lists."[30] Today, the different computer programs can be used to visualize and assess the destruction by the selected weapon in the attack.[31]

1.5. Geneva Convention Additional Protocol I article 36 - New weapons

Additional Protocol I, Article 36 states that:

"In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under an obligation to determine whether its employment would, in some or all circumstances, be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party."

In practice, this means that States need to be taken into account, whether they are subject to any international agreement that would prohibit the development or use of a weapon.[32] Next, States must evaluate whether the weapon is permissible according to customary international law. This assessment includes the above-mentioned principles of the Laws of War.[33] It should be noted that the assessment of the legality of weapons is left fully to the Contracting States' own practice.

[30] Jenks, *supra* nota 26, p 668 cited in Jackson (Jackson, R. Willamette university college of law panel: Empirical approaches to to the international Law of War, 2009).
[31] Jenks, *supra* nota 26, p 668.
[32] Cass, K. Autonomous weapons and accountability: seeking solutions in the Law of War. Loyola of Los Angeles law review, 2015, 48 (1017), pp 1017-1067, p 1041.
[33] *Ibid*.

Contracting Parties are not obligated to publish their findings what comes to the assessments and tests. When one is dealing with national security and defence, it is very natural that publications are not revealed in large quantities.[34]

1.6. Principles of sovereignty and neutrality

Although these two principles are not part of international humanitarian law, the author sees them relevant as they are an integral part of cyber warfare since cyber warfare has no borders and these principles are easily violated. Principle of territorial sovereignty means that the State has full and exclusive power over his own territory.[35] There are many definitions including the following "…the inherent supremacy of the State in its territory and independence in international relations."[36] In *Corfu Channel* case, International Court of Justice (ICJ) has ruled that "Between independent States, respect for territorial Sovereignty is an essential foundation of international relations."[37] Furthermore, the State has, under international customary law the right to practice the jurisdiction over objects and persons in the form of national legislation, as well as to monitor and enforce these rules.[38] The State also has the right to decide within its borders of all the incoming and outgoing movement.[39] Perhaps most importantly, it protects the State from all forms of interference from other States. In addition to protection, the principle also rises obligations, such as protecting the interests of other States within its own borders.[40]

Neutrality gives non-belligerents the opportunity to maintain relations with the belligerents.[41] The rules of neutrality are listed in the Hague Conventions.[42] Neutral State's territory is

[34] Rappert, B. et al. The roles of civil society in the development standards around new weapons and other technologies of warfare. International Review of the Red Cross, 2012, 94 (886), pp 765-785, p 781.
[35] Heintschel von Heinegg, W. Territorial Sovereignty and Neutrality in Cyberspace. International Law Studies, US Naval War College, 2013, 89, pp 1-156, p 124.
[36] Gevorgyan, K. Concept of State sovereignty: Modern Attitudes. ysu.am/files/Karen_Gevorgyan.pdf (8.4.2017), p 433 cited in Tunkin (Tunkin G.I. Basics of Contemporary International Law. Moscow, 1956, p 15.)
[37] ICJ 9.4.1949, Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania).
[38] Heintschel von Heinegg, *supra* nota 35, p 124.
[39] *Ibid*.
[40] Permanent Court of Arbitration 4.4.1928, Island of Palmas (or Miangas) (United States v. The Netherlands), p 839.
[41] Kelsey, *supra* nota 17, p 1442.
[42] Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. The Hague, 18 October 1907. International Committee of the Red Cross ihl-databases.icrc.org/ihl/INTRO/200?OpenDocument (4.2.2017) and

inviolable. Belligerents do not have permission to carry troops or other material across a neutral State, and aircrafts must not penetrate a neutral State's jurisdiction. A neutral State must also take the necessary steps to ensure that belligerents do not take advantage of the neutral State's territory. However, a neutral State does not need to prevent the export of military equipment or transportation out of the neutral State.[43] Additionally, the Convention defines an exception related to communications in Article 8 which states: "A neutral Power is not called upon to forbid or restrict the use on behalf of the belligerents of telegraph or telephone cables or of wireless telegraphy apparatus belonging to it or to companies or private individuals."[44] Naturally, a neutral State may not take part in hostilities, or it will lose its neutrality.[45]

Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War. The Hague, 18 October 1907. International Committee of the Red Cross
ihl-databases.icrc.org/applic/ihl/ihl.nsf/INTRO/240 (4.2.2017).

[43] Article 7 of Hague Convention V .

[44] Kelsey, *supra* nota 17, p 1442.

[45] The law of armed conflict, neutrality. International Committee of the Red Cross 2002. www.icrc.org/eng/assets/files/other/law8_final.pdf (6.4.2017), p 8.

2. General overview of weapons in question

2.1. Unmanned aerial vehicles also known as drones

Many terms such as "unmanned aerial vehicles" (UAV), "remotely piloted aircraft" (ROA) and "remotely piloted weapons" (RPW) refer to similar kinds of aerial vehicles but at the moment lacks of single legal definition to these aircrafts. US Department of Defence defines UAV as

"[a] powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and [] carr[ies] a lethal or nonlethal payload. Ballistic or semi ballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles."[46]

Instead, term "drone" has been used very widely.[47] Henceforth in this thesis all aerial vehicles, except autonomous weapons, will be referred to by the term drone or UAV.

First drones were originally used for intelligence, surveillance and reconnaissance.[48] USA used drones for reconnaissance already in the time of Vietnam War and after this, inter alia, in Bosnia and Herzegovina and Kosovo.[49] By the present day, drones have evolved tremendously. As a result, also their sizes have decreased significantly and today they vary in size according to their purposes. The smallest drones are the size of a wasp[50] and can land on a very small surface,[51] while the bigger drones are several meters long and can carry large loads, for instance in the form of Hellfire missiles.[52] Although while watching the news it may seem that the drones are used primarily for targeting purposes, in reality, surveillance and reconnaissance has even today greater role.[53]

---

[46] Jenks, *supra* nota 26, p 653 cited in Department of Defence (Joint Publication 1-02, Department of Defence Dictionary of Military and Associated Terms 2001).
[47] Takemura, H. Unmanned aerial vehicles: Humanization from international humanitarian law. Wisconsin International Law Journal, 2014, 32 (3), pp 521-546, p 523.
[48] Casey-Maslen, *supra* nota 25, p 598.
[49] Casey-Maslen, *supra* nota 25, p 599.
[50] Graham, D. The U.S. employment of unmanned aerial vehicles (UAVs): An abandonment of applicable international norms, Texas A&M law review, 2015, 2, pp 675-694, p 677.
[51] Casey-Maslen, *supra* nota 25, p 599.
[52] Jenks, *supra* nota 26, p 653.
[53] Graham, *supra* nota 50, p 677.

Drones have many different capabilities. A single UAV can monitor a specific area or building of up to nearly whole day consecutively.[54] The smallest of these UAVs are almost impossible to distinguish in the dark. In addition to the ability to monitor opposing functions, they are useful also in terms of force protection. If one possesses more than one UAV, he can have round-the-clock surveillance station around.

The biggest US-owned drones, called Predator and Reaper, use usually missiles like Hellfire II or Scorpion which has range of several miles. These drones can also possess many different guidance systems which enable extremely accurate targeting, even in the dark.[55] Moreover, drones are also used to contribute to humanitarian assistance in response to natural disasters.[56]

Despite the fact that the drones seem to be a very good option with its many capabilities, and manufacturing is many times cheaper than fighter aircraft, the use of the drones air space in which the United States does not control air superiority, is appreciably more difficult. As a result, airplanes may not be fully suitable for conventional warfare, in where resistance is to be expected.

A total of at least forty States are in possession of drones. The greatest interest is seen in the United States, but also in Israel.[57] Most of drones are used for observation. It should also be noted that more and more newer players step forward what comes to drones. Countries such as Iraq and also non-State actors, such as Hezbollah, have developed their own drones.[58] However, there are States like Japan, which because of the aftermath of the Second World War was forced to sign a constitution which only allows military vehicles and personnel for national defence purposes. This is the reason why inter alia Japan uses their drones only for surveillance purposes.[59]

[54] *Ibid*.
[55] *Ibid*.
[56] Takemura, *supra* nota 47, p 524.
[57] Jenks, *supra* nota 26, p 654.
[58] *Ibid*.
[59] Takemura, *supra* nota 47, p 543.

2.2. Autonomous weapons

Autonomous weapons systems (AWS) is a system which is capable of making independent decisions, like selecting and engaging targets, based on gathered information and preprogrammed constraints.[60] The United States Department of Defence defines AWS as "a weapon system(s) that, once activated, can select and engage targets without further intervention by a human operator."[61]

Autonomous weapons development began in earnest in the 1980s, when US sought to oust the Soviet Union in armaments. At the end of the Cold War, the development suffered a bit of a discontinuity but recovered quickly due to their versatility and new purposes. Although development has been going on for decades, not until the innovations of recent years have made it possible for completely new technologies.[62]

Generally speaking, autonomous weapons can be classified into three different groups. These groups are remotely controlled, automated or fully autonomous.[63] In the first case, a system, a robot, is guided by human through some form of transmitter via radio signals. The robot has a receiver, sensors or other devices that are necessary.[64] Examples of these are already above-mentioned drones Predator and Reaper. As a result, all decisions, such as the destruction of the object, is fully behind human decision.[65] Instead, automated robots are not reliant to direct human control. Automated robots perform pre-programmed tasks or moves in the planned surroundings.[66] As an example of this can be used the United States Navy MK-15 Phalanx Close-In Weapons System, which automatically detects, evaluates and destroys the approaching

[60] Crootof, R. War torts: Accountability for autonomous weapons. University of Pennsylvania Law Review, 2016, 164 (6), pp 1347-1402, p 1372 cited in Crootof (Crootof R. The Killer robots are here: Legal and policy implications, Cardozo Law Review 2015).
[61] The Ethics of autonomous weapons systems, University of Pennsylvania Law School. www.law.upenn.edu/institutes/cerl/conferences/ethicsofweapons/ (6.2.2017).
[62] Liu, *supra* nota 21, p 632.
[63] Cass, *supra* nota 32, p 1023.
[64] Cass, *supra* nota 32, p 1023 cited in Murphy (Murphy, R. An introduction to AI robotics, 2000).
[65] Asaro, P. On banning autonomous weapon system: human rights, automation, and the dehumanization of lethal decision-making. International Review of the Red Cross, 2012, 94 (886), pp 687-709, p 690.
[66] Cass, *supra* nota 32, p 1023 cited in Sharkey (Sharkey, N. Automating warfare: Lessons learned from the drones, J.L Inf. & Sci. 2011).

ship missiles and agile flying objects, such as airplanes.[67] Fully autonomous robots come to have artificial intelligence and thus to be fully self-help, without human guidance. Fully autonomous weapons would be able to make their own decisions considering targeting and approaching.[68] They would have the ability to learn through experience.[69] These kind of systems are in developing phase and yet, do not exist.[70] Some experts are of the opinion that artificial intelligence can be developed by the end of the century when some experts argue that such a fully autonomous robots will never exist.[71] This thesis deals with the three levels of autonomy as two elements, drones and "other" autonomous weapons.

Countries other than the United States which develop autonomous weapons are Israel, South Korea, the United Kingdom, France, Germany, Denmark, Sweden, China and India.[72] Furthermore, dozens of States have bought autonomous weapons.

2.3. Cyber warfare

Cyber attacks are defined differently depending the source. Some entities does not even distinguish between cyber attacks and cyber intrusions. The National Research Council's 2009 report defines cyber attack as "the use of deliberate actions - perhaps over an extended period of time - to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and/or programs resident in or transiting these systems or networks."[73]

---

[67] The United States Navy, MK-15 - Phalanx Close-In Weapons System, www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2 (6.4.2017).
[68] Cass, *supra* nota 32, p 1024 cited in Sparrow (Sparrow, R. Killer robots, Journal of Applied Philosophy 2007, 24 (1)).
[69] *Ibid.*
[70] Human Rights Watch and Harvard Law School's International Human Rights Clinic. Fully Autonomous Weapons: Questions and Answers, 2013. www.hrw.org/sites/default/files/supporting_resources/10.2013_killer_robots_qa.pdf (8.4.2017), p 2. (Hereinafter Human Rights Watch)
[71] Cass, *supra* nota 32, p 1025.
[72] Cass, *supra* nota 32, p 1031 cited in Sparrow (Sparrow, R. Building a better warbot: Ethical Issues in the Design of Unmanned Systems for Military Applications, Science & Engineering Ethics 2009).
[73] Kesan, J. et al. Mitigative Counterstriking: Self-defence and Deterrence in Cyberspace. Harvard Journal of Law and Technology, 2012, 25 (2), pp 429-544, p 439 cited in Owens (Owens W. et al. Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, Washington D.C., The National Academies Press 2009).

Cyber operations began to generate interest in legal circles in the 1990s. Nonetheless, the development ceased after the 9/11 terrorist attack and the interest shifted to counter-terrorism activities.[74] It took until Estonia experienced a major cyber attack in 2007 and Georgia in the following year that the interest was transferred back among the cyber security.[75]

Variety of destruction can be achieved through cyber attacks. The attacker can create a computer virus or malicious code which can disable air defence systems without any physical destruction. Weapon can be delivered via Internet or the attacker can beam the weapon from the aircraft. The attack can also include messages that contain false information, which purpose can be for instance to hinder the work of command center.[76] The attacks can also target the infrastructure that serves the civilian and military purposes. Such attacks include, for instance, power plants, telecommunications and transportation. In this way, the energy yield can be interrupted for extended periods of time. One way may also be taking over media broadcasts. An attacker could either stop or prevent the transmission of the message flow, or alternatively, to capture the transmission and replace it with their own propaganda. This can produce false information of, for instance, movements of their own forces.[77]

At present, approximately thirty countries produce offensive cyber programs. Most significant of these are Israel, China, Russia and the United States. Remarkable is also the fact that States which do not possess large army as conventional weapons, can have vast resources in the field of cyber warfare.[78]

[74] Schmitt, M. et al. The decline of international humanitarian law opinio juris and the law of cyber warfare. Texas international law journal, 2015, 50 (2), pp 189-231, p 221.
[75] *Ibid*.
[76] Kelsey, *supra* nota 17, p 1434.
[77] Kelsey, *supra* nota 17, p 1435.
[78] Sher, J. Comment anonymous armies: Modern "cyber-combatants" and their prospective rights under humanitarian law. Pace international law review 2016, 28 (1), pp 233-275, p 250.

3. Legal analysis of above-mentioned weapons

3.1. Legal problems

3.1.1. Drones

3.1.1.1. Principles of precautions, distinction and proportionality

Principle of precaution may be better followed thanks to the characteristics of UAVs. Due to the real-time video image, environment can be monitored more reliably, and the identification of the objective can be done from a distance, which makes it possible the objective to be assured, and collateral damage is reduced. In many cases, the objectives are provided with tracking device and are thus labeled as target.[79] This, too, contributes to reduce the collateral damage. If one does not take into account Hellfire missiles, missiles launched from drones generally have lower blast radius than other conventional munitions launched from jet fighter.[80]

However, collateral damage has been occurred. Moreover, even own soldiers have died as a result of the US UAV attacks.[81] Nonetheless, according to Special Rapporteur of the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, UAVs, if used strictly according to International Humanitarian Law (IHL), their use may reduce civilian casualties.[82] Thus, it seems that the fulfillment of the principle of precautions would not impose a problem.

The core idea of the principle of distinction is to protect civilians and civilian objects. This, however, can be waived if civilians take direct part in hostilities. Though, there is no consensus as to what constitutes direct participation in hostilities.[83] Drones has been in little use in international armed conflicts.[84] For this reason, the distinction between civilians and combatants poses problems especially in non-international armed conflict. As an aid has been used the International Committee of the Red Cross (ICRC) Interpretative Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law.[85] According to it,

[79] Casey-Maslen, *supra* nota 25, p 607.
[80] Takemura, *supra* nota 47, p 532.
[81] Takemura, *supra* nota 47, p 533.
[82] Takemura, *supra* nota 47, p 532 cited in Emmerson (Emmerson B. Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism 2013).
[83] Jenks, *supra* nota 26, p 666.
[84] Casey-Maslen, *supra* nota 25, p 608.
[85] Takemura, *supra* nota 47, p 534.

organized armed group of non-State actor can be attacked if the group fulfils the criteria of *"*continuous combat function.*"*[86] However, this has been criticized by the Special Rapporteur of Extrajudicial, Summary or Arbitrary Executions because the nomenclature is different from the treaty and may thus give rise to confusion.[87] This can lead to a broader interpretation of the State to use force, and innocent, persons who might have been disengaged from hostilities may suffer. [88] If there is uncertainty as to whether civilian takes part in hostilities, people should be treated as a civilian and therefore not to be shot.[89] In addition, it should be taken into account that if States fail to fulfil the principle of distinction, that might be subject to war crime.[90]

When considering the principle of proportionality the question to arise is what is considered to be excessive damage to civilians and civilian objects.[91] Different States can have very different scales while measuring the principle of proportionality. There is examples even between close military allies the UK and the USA.[92] Measurement of proportionality is also more difficult by the fact that the UAV attacks are often secret, and the information is not disclosed to third parties. Moreover, because of the secrecy, statistics on civilian casualties are not available.[93] Thus, intelligence has a very important role in the implementation of the principle of proportionality.

3.1.1.2. Targeted killings

Controversy is also caused by so called "targeted killings". The term has no solid definition, but the former ICRC Legal Advisor defines it as "the use of lethal force attributable to a subject of international law with the intent, premeditation and deliberation to kill individually selected persons who are not in the physical custody of those targeting them".[94] When Israel brought this conduct to the public's attention, it was right away condemned widely, but despite of this, later

[86] *Ibid*.
[87] *Ibid*.
[88] *Ibid*.
[89] Casey-Maslen, *supra* nota 25, p 611.
[90] Takemura, *supra* nota 47, p 534.
[91] Takemura, *supra* nota 47, p 535.
[92] Casey-Maslen, *supra* nota 25, p 613.
[93] Takemura, *supra* nota 47, p 535.
[94] Liu, *supra* nota 21, p 643 cited in Melzer (Melzer N. Targeted Killing in International Law, Oxford, Oxford University Press, 2008, p 5).

used by other States as well.[95] The question is, above all, whether or not these attacks are legitimate according to Article 36 of AP I. Liu suggests that the drone attacks on another State's territory in the form of targeted killings require a re-evaluation within the framework of Article 36.[96] He raises three problems; first, while attacking, the objects are defined as "suspected terrorists". Since the machine can not differentiate between civilians and combatants, this causes the problem to a principle of distinction.[97] Secondly, the machines pose a risk to excessive use of force.[98] Other author share the view asking are the targets legitimate; does these attacks cause harm to civilians and if so, are they proportionate to military advantage.[99] Suspected terrorists can mix with civilians or stroll among the civilians. Central Intelligence Agency (CIA) claims that there are no collateral damage caused, but this is is doubtful.[100] Thus, it is questionable whether the machines are able to comply with the principles of proportionality and distinction.[101] Thirdly, it is unclear whether the machine is able to control its behavior when a combatant is *hors de combat* or aiming to surrender.[102]

3.1.2. Autonomous weapons

3.1.2.1. Distinction and precautions

At least for now, there is no way how AWS can comply with the principles of distinction and precautions. This is because AWS make all decisions based on algorithms and metrics and currently there is no such system which would make AWS able to decipher between legitimate and non-legitimate targets.[103] Various sensors and facial recognition systems are useless, because any database of the enemy combatants does not exist.[104] Although AWS could detect faces it still does not help distinguishing between civilians and combatants. It would only help them to recognize own troops.[105] One could argue that uncertainty is increased by the fact that the

[95] Rosenzweig, I. Targeted Killings during High and Low Intensity Warfare. Law and National Security: Selected Issues 2014, 138, pp 41-52, p 41.
[96] Liu, *supra* nota 21, p 645.
[97] *Ibid*.
[98] *Ibid*.
[99] Rosenzweig, *supra* nota 95, p 43.
[100] Liu, *supra* nota 21, p 645.
[101] *Ibid*.
[102] Liu, *supra* nota 21, p 646.
[103] Roff, H. To ban or to regulate autonomous weapons A US response. Bulletin of Atomic Scientists, 2016, 72(2), pp 122-124, p 122.
[104] Cass, *supra* nota 32, p 1035.
[105] Roff (2016), *supra* nota 103, p 122.

definition of civilian is not clear. AP I announces that a person is a civilian, if he is not a combatant. This creates problems concerning distinction for people, understandably, not to mention the autonomous weapons. These dilemmas speak for themselves that the human being is required to make decisions, so that the principles are accomplished. Proponents, namely professors Anderson and Waxman argue that especially as technology advances AWS can be used in conflicts. Examples include situations where there is not human combatants but only AWS, for instance undersea attacks. They find that AWS can comply with the principle of distinction because weapons can distinguish between objects.[106]

3.1.2.2. Proportionality

The principle of proportionality is very context-dependent concept and that is why it will create a legal problem to AWS.[107] Noel Sharkey writes that "there is no sensing or computational capability that would allow a robot such a determination [of proportionality], and nor is there any known metric to objectively measure needless, superfluous or disproportionate suffering. They require human judgement."[108] On the other hand, people either are not error-free, with regard to discretion of the proportionality and understandably every situation on the battlefield is different. Thus, one can also think that when AWS is making a mistake while assessing the proportionality, the same error could occur with the human decision-making.[109] Anderson and Waxman argue that in the same way as with the principle of distinction, AWS are operational in areas where there is little or no civilians, or AWS only.[110]

Autonomous weapons are also different in the sense that in conventional warfare there is an imminent threat against human fighters.[111] In case of autonomous weapons opponent does not cause threat to human combatants, which means that the use of AWS should be justified by

[106] Cass, *supra* nota 32, p 1036.
[107] Cass, *supra* nota 32, p 1037.
[108] Liu, *supra* nota 21, p 643.
[109] Cass, *supra* nota 32, p 1038.
[110] Cass, *supra* nota 32, p 1038 cited in Anderson (Anderson K. Law and ethics for autonomous weapons systems: Why a ban won't work and how the laws of war can 2013).
[111] Roff, H. Lethal autonomous weapons and jus ad bellum proportionality. Case Western Reserve Journal of International Law, 2015, 47, pp 37-52 p 44.

opponent causing damage to property.[112] What causes a legal problem is that for instance common law and US jurisprudence does not allow the use of lethal force to protect property.[113]

3.1.3. Cyber warfare

3.1.3.1. Distinction and proportionality

It seems that there is no doubt why IHL should not be applied when attacking legitimate military targets. In addition, the attack on air-defense center through cyber operation can even be considered a better alternative than conventional bombing, since collateral damage is probably smaller, if it even exists.[114] However, the situation should be assessed differently if paralysis of the air defense system would pose a danger to commercial flights.[115]

On behalf of the fulfillment of principle of distinction speaks the fact that various malwares and viruses, can be programmed in such a way that they destroy only the desired object or system, and even when spreading elsewhere, they will not cause destruction to others. This way, for instance, Stuxnet was designed.[116]

However, as mentioned above, if there is no information as to whether it is a military target or not, one should refrain from attacking it. Problems occur with the dual-use infrastructure. Diamond argues that the present tendency shows that dual-use infrastructure is kept as serving military purposes which causes problems because virtually every aspect of the cyber infrastructure could be considered on this basis as military objective.[117]

Features of internet cause headache. The majority of Internet's data is unencrypted and communication of armies passes through the same routes with commercial contacts. Therefore,

[112] Roff (2015), *supra* nota 111, p 45.
[113] *Ibid*.
[114] Kelsey, *supra* nota 17, p 1438.
[115] *Ibid*.
[116] Kovach, C. Beyond Skynet: Reconciling increased autonomy in computer-based weapons systems with the laws of war. Air Force Law review, 2014, 71, pp 231-277, p 245.
[117] Diamond, E. Applying International Humanitarian Law to Cyber Warfare. Law and National Security: Selected Issues 2014, 138, pp 67-84, p 77.

one should consider that if a previous attack disrupts civilians' access to the Internet, whether it is a violation of Laws of War?[118]

The principle of proportionality is a very difficult issue to estimate among conventional weapons, let alone the cyber warfare. This is due to the fact that cyber warfare is a relatively new phenomenon, of which very little is known, and moreover, interconnectivity makes it difficult to evaluate all the consequences of the attacks.[119]

Furthermore, non-lethal impact of cyber operations can bring incentive to break the principle. Attacks on targets which destruction does not create ample military advantage, the temptation to use cyber weapons can be great.[120] This is because cyber weapons do not cause damage to civilians or environment, which is used as a justification to the attack. This would not, of course, be the case with conventional weapons.[121]

In order the principle of distinction to be fulfilled, it is proposed, among other things, that in the same way as the human combatants wear an emblem, computers used in cyber warfare could be marked.[122] In addition, computers could inquire the counterparty's computer in advance, so that it would not be connected to the computers of civilians, and only after that to attack.[123]

Moreover, following safeguards are proposed. Weapon designers should take into account the fact that, while the weapons such as Stuxnet are designed for attacking specific objective, they tend to spread.[124] Additionally, special attention should be given critical infrastructure.[125] If a cyber weapon threatens huge masses of civilian people, human intervention must be possible.[126] It is also considered important that these safeguards must exist before the weapon is used.[127]

---

[118] Kovach, *supra* nota 116, p 246.
[119] Diamond, *supra* nota 117, p 77.
[120] Kelsey, *supra* nota 17, p 1440.
[121] *Ibid*.
[122] Kovach, *supra* nota 116, p 247.
[123] *Ibid*.
[124] Computerworld. Why did Stuxnet worm spread?, 2010 www.computerworld.com/article/2516109/security0/why-did-stuxnet-worm-spread-.html (6.4.2017).
[125] Kovach, *supra* nota 116, p 248.
[126] *Ibid*.
[127] *Ibid*.

3.1.3.2. Sovereignty and neutrality

Material damage to the cyber infrastructure is a universally accepted as a violation of sovereignty.[128] Some are of the view that it need not be material, but only a severe.[129] However, if there is no material damage, or the damage is only scarce, there is no consensus does this kind of attack violate the principle of sovereignty.[130] It can also be argued that, despite the fact does the attack cause damage, the mere intrusion of another State cyber infrastructure can be regarded as a violation of territorial sovereignty.[131] However, it is also stated that "when Belligerent Parties use for military purposes a public, internationally and openly accessible network such as the Internet, the fact that part of this infrastructure is situated within the jurisdiction of a Neutral does not constitute a violation of neutrality."[132]

There is a concern that a State may perform cyber strike in another State, without their knowledge. Consequently, it is aligned, that if the a State does not have actual or presumptive knowledge, the duty of prevention does not occur.[133] Jensen also raises questions about the applicability of the law of neutrality in cyber conflicts.[134] However, there is no consensus, and some say that the purpose of the duty is to prevent cyber attacks generally.[135] If the States would be obliged to prevent cyber attacks on the basis that they knew or should have known, it would be very difficult or even impossible considering the technology involved.[136] Cyber weapon can be transferred in small parts, of which a single part does not constitute harm, and therefore does not attract attention, but together they form a powerful cyber weapon.[137]

[128] Heintschel von Heinegg, *supra* nota 35, p 129.
[129] *Ibid*.
[130] *Ibid*.
[131] *Ibid.*
[132] Jensen, E. Sovereignty and Neutrality in Cyber conflict. Fordham International Law Journal, 35 (3), 2012, pp 814-841, p 825 cited in Research (Humanitarian Policy & Conflict Research, Manual on International Law Applicable to Air and Missile Warfare, Harvard University Edition, 2009).
[133] Heintschel von Heinegg, *supra* nota 35, p 136.
[134] Jensen, *supra* nota 132, p 824.
[135] Heintschel von Heinegg, *supra* nota 35, p 136.
[136] Heintschel von Heinegg, *supra* nota 35, p 137.
[137] Heintschel von Heinegg, *supra* nota 35, p 138.

Due to the international nature of the Internet cyber attacks may pass through neutral countries. Attack from one State to another may go through two totally other States, even though the belligerents would be neighboring States. Although the strike would not have any visible effects to neutral States, IHL might force them to start action to stop the attack.[138]

Kelsey says that this will lead inexorably to infringements of the principle of neutrality.[139] Even if the communication is permitted, he believes that cyber operations will belong to the forbidden list because it is forbidden to move arms and forces in the territory of a neutral State.

Kelsey further argues that cyber attack can also lead to the loss of neutrality inadvertently.[140] When cyber attack sent by belligerent passes through the neutral State, this can lead to widening the conflict. He continues that if a neutral State does not prevent, or is unable to prevent belligerent's attacks, the other belligerent may attack a neutral State's communication network in order to prevent a cyber attack passage through this State. Thus, without physical damage to the neutral State, it might be forced into the war, unintentionally.

A Neutral State is obliged to observe its own territory, in order to prevent belligerents for using it for their advantage.[141] In case of cyber attacks, this can be tricky, because no practical instrument exists.[142] The only sure way is to disconnect all connections with other States, and this would obviously be unreasonable. States have an incentive to break the principle of neutrality via Internet. First of all, cyber operation is more cheaper than conventional warfare. Belligerents could avoid breaking the principle by sending a airplane to launch the cyber attack. This is unlikely, since many States are not willing to risk any human lives. Secondly, instead of belligerent avenge the neutral State when neutral State is struck after not been able to prevent attacks through its own domain, belligerent would use the cyber attack instead of physical attack. [143] Third, the internet allows one to make attacks without getting caught. Although, it would leave some traces, they do not necessarily lead to ever track down the culprit.

[138] Kelsey, *supra* nota 17, p 1441.
[139] Kelsey, *supra* nota 17, p 1443.
[140] Kelsey, *supra* nota 17, p 1444.
[141] Jensen, *supra* nota 132, p 826.
[142] Kelsey, *supra* nota 17, p 1444.
[143] Kelsey, *supra* nota 17, p 1445.

3.4. Responsibility

Civilian victims are regrettable, but inevitable part of the armed conflict.[144] As noted earlier, under certain conditions, the civilian victims are not necessarily unlawful. In this case, they are considered as collateral damage. On the other side are the deaths, such as the so-called willful killings which are prohibited.[145] If a person is not acting right according to the Laws of War, the responsibility is predetermined.[146] Accountability for breach of IHL is important. When people see that the offenses incur sanctions, it may prevent them from committing war crimes.[147] In addition, the accountability provides value and recognition for the victims of the crimes, when they see that the wrongdoers will be punished.[148] When one is talking about the responsibility considering the above-mentioned weapons, the author considers two issues; pecuniary accountability and criminal liability.

3.4.1. Pecuniary accountability

There are three entities which could be financially responsible for the breach of Laws of War by AWS; manufacturer, programmer or the State which employs the autonomous weapons system.

The manufacturer has hired designers and sold the machine, so the manufacturer bears the responsibility for the harm caused by their products. However, keeping the manufacturer responsible is proved to be extremely difficult because of the existence of a product liability issue which is a civil lawsuit.[149] The court should have jurisdiction against the manufacturer and in case of a foreign manufacturer, it would be difficult.[150] Asaro has mentioned that suing of the manufacturer may be possible to the US military, but not in case of individual.[151] An example of

[144] Cass, *supra* nota 32, p 1048.
[145] *Ibid*.
[146] *Ibid*.
[147] Human Rights Watch, *supra* nota 70, p 5.
[148] Human Rights Watch, *supra* nota 70, pp 5-6.
[149] Cass, *supra* nota 32, p 1050.
[150] *Ibid*.
[151] Future of Life Institute. Who is Responsible for Autonomous Weapons? futureoflife.org/2016/11/21/peter-asaro-autonomous-weapons/ (5.4.2017).

this is case *J. McIntyre Machinery, Ltd. v. Nicastro*[152], in which a British manufacturer called for compensation, but the United States Supreme Court ruled that New Jersey had no jurisdiction. Under the current legislation, it is unclear whether the victims of autonomous weapons are able to sue manufacturers to court in their home country.[153] The fact that the victims would sue the manufacturer in manufacturer's home country is often virtually impossible. This is because the victims of war are often vulnerable, especially financially, and suing somebody in another country would cause an insurmountable burden.

Secondly, product liability issues are governed by domestic law. As a result, the nation-State can greatly limit the circumstances in which the manufacturer would be responsible for the weapon's breaches.[154] An example of this, is the case *Boyle v. United Technologies Corp.*, in which the United States Supreme Court decided that, subject to certain conditions, "liability for design defects in military equipment can not be imposed, pursuant to State law."[155] Although the case considers national legislation, and is not applicable at the international level, it gives an idea of how national legislation may limit the cases in which the manufacturer would be responsible for the actions of autonomous weapon systems. Thus, it is clear that individuals can bring a charge against the manufacturer, but it may incur as a major challenge to get the manufacturer responsible for the fact.

When considering a programmer's responsibility, there is disagreement among the experts. However, one can think that the programmer is responsible for the weapon system's disorder, because when programmed machine makes a mistake, it is considered a technical fault.[156] In addition, if the programmer does not encode the machine properly, for instance, to distinguish between lawful and unlawful objects and the harm occurs, the programmer can be held responsible. Despite this, the same problems of jurisdiction arise in the case of programmer as previously mentioned manufacturer. Secondly, programmers are working very often in teams. This means that one programmer is responsible for only a small piece of code, and therefore is not necessarily aware of the remaining parts. This means that individual programmer might not

[152] Supreme Court of the United States, No. 09–1343., J. McIntyre Machinery, Ltd. v. Robert Nicastro.
[153] Cass, *supra* nota 32, p 1050.
[154] Cass, *supra* nota 32, p 1051.
[155] Supreme Court of the United States, No. 86-492, Boyle v. United Technologies Corp.
[156] Cass, *supra* nota 32, p 1052.

know how the machine will act.[157] As a result of this lack of information it is difficult to attribute responsibility to the programmer.

If the States are using drones in violation of international law, it will lead to State responsibility. [158] According to Article 91 of AP I ”A Party to the conflict which violates the provisions of the Conventions or of this Protocol shall, if the case demands, be liable to pay compensation. It shall be responsible for all acts committed by persons forming part of its armed forces.” Furthermore, ”[a] State responsible for violations of [the Law of War] is required to make full reparation for the loss or injury caused.”[159] This shows that the State which utilizes the autonomous weapon is responsible for the actions of the machine according to State responsibility. Due to noncompliance with the rules by autonomous weapon and resulting compensation payment, professors Anderson and Waxman suggest that for the weapons should be made legal assessments on a regular basis and assess their suitability for operational conditions.[160] Moreover, the personnel of the weapons should be well trained, which would include the strengths and weaknesses of the weapon.[161] This would ensure as far as possible that the Law of War is being followed.

Crootof would take the State compensation a step further and create a new system, the so-called *“War torts”*[162]. She argues that war torts would make the applicability of the law of s
State responsibility in armed conflicts more clear, especially the obligation to make full reparation.[163] If the responsibility of the State would be more recognized in public, it would promote the lawful behaviour. As the most important issue she considers that it would ensure compensation to the victims. She argues that the criminal law has focused on the moral iniquity and guilt, as well as the prohibition of certain activities. War Torts instead focuses on harmful injustices, guilt and a certain, regulation of sometimes hazardous activities. It appears that countries are reluctant to admit their guilt because of moral blame, not so much because of

[157] Future of Life Institute, *supra* nota 151.
[158] Takemura, *supra* nota 47, p 539.
[159] Henckaerts, J-M. et al. *supra* nota 4, p 537.
[160] Cass, *supra* nota 32, p 1053.
[161] *Ibid*.
[162] Crootof, *supra* nota 60, p 1386.
[163] *Ibid*.

escaping liability. States have suggested compensation for victims even before they are publicly demanded.[164]

Already existing contracts, Status of Forces Agreements[165], such as the NATO Status of Forces Agreement shows that States could be of interest to enter into a more formal agreement that would define their responsibilities of War Torts, at least in the case of autonomous weapons.

Although the State can be seen right entity to pay compensation for the wrongdoings, some consider the mere monetary compensation is inadequate. An example of this is the Boston Marathon bombing, where the accused said that the attack was justified, as retribution for crimes committed by US to Muslims in places like Iraq and Afghanistan.[166]

3.4.2. Criminal liability

War crimes can be prosecuted in three different court systems. The first one is national court. The fact that war crimes have universal jurisdiction is well supported by many military manuals and State practises as well as national legislation and treaty law.[167] International or mixed tribunals can also be found to prosecute war crime perpetrators.[168] Over the years there have been several of these, to name few, the International Criminal Tribunal for the former Yugoslavia (ICTY), International Military Tribunals of Nuremberg and Tokyo and the Special Court for Sierra Leone. The newest system is the International Criminal Court (ICC), which was established under the Rome Statute. This is the first system, which has no direct connection with criminal offenses or offenders.[169] If States are unwilling or unable to prosecute the perpetrators, ICC can deal the matter on behalf of the States.

---

[164] Crootof, *supra* nota 60, p 1392.
[165] International Security Advisory Board, Report of Forces Agreements, www.state.gov/documents/organization/236456.pdf (4.4.2017).
[166] The Sydney Morning Herald, Boston bombings revenge against US: Tsarnaev, 17.5.2013. www.smh.com.au/world/boston-bombings-revenge-against-us-tsarnaev-20130516-2jpv0.html (4.4.2017).
[167] Henckaerts, J-M. et al. *supra* nota 4, pp 604-605.
[168] Cass, *supra* nota 32, p 1055.
[169] Henckaerts, J-M. et al. *supra* nota 4, p 610.

When observing criminally liable for drone strikes, many persons have been under consideration; operator, area observers on the ground, the ones who indicate the objective to be lawful or lawyers who give the permission for the strike.[170] In case of autonomous weapons; programmer, the ones who build and sell the hardware, military commanders, subordinates who deploy the weapons system or political leaders.[171] Drone attacks are associated with previously mentioned lack of transparency. Takemura considers the lack of transparency the worst threat to the division of responsibility for drone attacks.[172]

Peter Cane has proposed a responsibility which considers both the historic and the prospective perspectives.[173] The first perspective examines the accountability after the fact and the latter obligations and duties before the fact.[174] In his opinion, it is clear that in the case of autonomous weapons, prospective is the most reasonable practice. This is because only obligation to obey the relevant law provisions can be programmed into weapons systems. Further, he argues that historical concepts of accountability are unusable. This is because although there is a possibility that artificial intelligence may lift its ontological level, issues in this context still need answers. After all, it is doubtful and meaningless to think about punishing a machine.[175]

Although there is no consensus considering the allocation of criminal responsibility, three entities can be considered as the most probable alternatives; the robot itself; combatant, who deployed the autonomous weapons system; and the commander.

The robot can not be criminally liable. According to Article 30 of the Rome Statute person may be convicted of war crimes, if he has appropriate mental state to be judged a war crime. First of all, a robot is not a person. And secondly, as discussed above, the robot does not think independently but all of its activities are based on a pre-programmed codes, so it can not have sufficient knowledge and intent which the fulfillment of Article 30 requires. Furthermore, Cane

[170] Takemura, *supra* nota 47, p 540.
[171] *Ibid*.
[172] Takemura, *supra* nota 47, p 539
[173] Liu, *supra* nota 21, p 650.
[174] *Ibid*.
[175] Kathleen Lawand, Fully autonomous weapons systems.
www.icrc.org/eng/resources/documents/statement/2013/09-03-autonomous-weapons.htm (4.4.2017).

argues that punishing the people for machines' actions instead of the machines themselves would make them scapegoats and furthermore, the causal link is broken because the machines have the opportunity to make autonomous decisions.[176] This leads to the fact that the autonomous weapons have a greater chance to comply with IHL, but lower probability of punishment when infringing the rules. This results impunity in armed conflict.

If certain conditions are met, the operator can be held liable of any war crimes committed by a robot.[177] The operator is able to make independent decisions using the knowledge and the intent and is thus able to carry out a war crime. Indiscriminate attack can serve as an example. Although the Rome Statute does not expressly define the indiscriminate attack as war crimes, the ICJ and ICTY has indicated that way in *Advisory opinion*[178] and in the *Prosecutor v. Galić.*[179] In addition, the above-mentioned entities have mentioned in their reasonings that they consider indiscriminate attacks the same as attacks against civilians.[180] While decisions of these bodies does not bind the ICC's decisions, they work as very convincing guidelines. Thus, if the ICC selects to follow the example of ICJ and ICTY operator can be held criminally liable.[181]

Some experts are of the opinion that the commander is ultimately responsible. The commander is the one who is responsible for the adequate precautions, regardless of time or space.[182] Individual and State responsibility attaches to those who authorize the use of the autonomous weapons.[183] There are two ways to keep commander criminally liable: Article 25(3) of the Rome Statute elicits that "a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the Court if that person … [o]rders … the commission of such a crime which in fact occurs or is attempted."[184] Thus, if a commander instructs the indiscriminate autonomous weapons attack and is executed or attempted, the commander may be held responsible.

[176] Liu, *supra* nota 21, p 650.
[177] Cass, *supra* nota 32, p 1058.
[178] ICJ 8.7.1996, Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion.
[179] International Criminal Tribunal for the Former Yugoslavia, no. IT-98-29-T, Prosecutor v. Galić, Judgment and Opinion, 5.12.2003.
[180] Cass, *supra* nota 32, p 1060.
[181] Cass, *supra* nota 32, p 1064.
[182] Backstrom, A. et al. New capabilities in warfare an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. International Review of the Red Cross, 2012, 94 (886), pp 483-514 p 498.
[183] *Ibid*.
[184] Cass, *supra* nota 32, p 1064 cited in Rome Statute (Rome Statute, article 25(3)(b)).

According to customary international law and Article 28 of the Rome Statute commander can be held liable for war crimes committed by his subordinates, if certain conditions are met:

"i) the existence of a superior-subordinate relationship;
ii) that the commander had the requisite knowledge that his subordinate was about to commit a war crime or had done so; and
iii) that the commander failed to take the necessary and reasonable measures to prevent or punish his subordinate's criminal conduct."[185]

Thus, the commander can be held directly criminally liable of a violation committed by autonomous weapons system or indirectly, through the command responsibility.

When cyber warfare is used for damaging purposes, ICRC is of the opinion that IHL is applicable in the same way than in case of any other weapon.[186] Therefore, the above-mentioned prosecuting procedures are useful also in the case of cyber warfare. However, cyber warfare is characterized by anonymity.[187] Applicability of IHL is based on the fact that the responsibility can be demonstrated.[188] Thus, if the responsibility cannot be indicated, the applicability of IHL leaves as a question mark.

[185] Cass, *supra* nota 32, p 1064 cited in Smidt (Smidt, M. Yamashita, Medina, and Beyond: Command Responsibility in Contemporary Military Operations, 2000).
[186] 31st International Conference of the Red Cross and Red Crescent, International Humanitarian Law and the challenges of contemporary armed conflicts Report Document prepared by the International Committee of the Red Cross 2011, pp 36-37. (Hereinafter International Conference).
[187] International Humanitarian Law and New Weapon Technologies, 34th Round Table on current issues of international humanitarian law, San Remo, 8–10 September 2011, International Review of the Red Cross. 2012, 94 (886), p 814.
[188] International Conference, *supra* nota 186, p 37.

3.5 Proposals to the legal problems

Of how the above-mentioned weapons should currently and in the future be regulated, there is no unanimity. One is of the opinion that at least in case of UAVs the current legislation is fully sufficient, so IHL can be applied. Another wants to ban the autonomous weapons, at least for the time until the rules are clear. There has also been a debate as to whether IHL is even available to cyber warfare or not.

The current legislation is sufficient to the drones, if the rules are not left ignored or misinterpreted or misused.[189] Takemura is sharing the view as well.[190] Instead, it would be good to pay attention to increase transparency. CIA's and other such entities' secret conduct and undocumented activity causes uncertainty, insecurity and doubts about the legality. The United States' own interpretation of the rules, and the creation of its own rules cause headaches.[191] United States chooses the best suitable rules for them and interpret them in the manner most advantageous to them. When other States discloses their opinions, they seem to fall on deaf ears.

Asaro proposes a ban on the use of autonomous weapons until the IHL and international human rights law is clear enough to regulate these weapons.[192] Professors Anderson and Waxman argue that the internal State regulation and identification of best practices are the most appropriate means to start regulating autonomous weapons.[193] This would develop debate and discussion around the world, and development of international customary norms would start its progress. The bottom for the legislation could be the principles of distinction and proportionality.

The author argues that "human-in-the-loop" system would be good to maintain even though autonomous weapons became more common. This would ensure that lethal decisions are made by human being instead of a machine which is before all morally dubious. This does not of

[189] Graham, *supra* nota 50, p 679.
[190] Takemura, *supra* nota 47, p 527.
[191] Graham, *supra* nota 50, p 679.
[192] Asaro, *supra* nota 65, p 693.
[193] Anderson, K., Waxman, M. Law and Ethics for Robot Soldiers. Policy review, 2012-2013, (176), pp 35-49, p 46.

course eliminate the possibility of an error and the resulting war crime but at least it would be clear who to be held guilty and start the prosecuting him or her. This idea is also supported by Asaro.[194] Noteworthy in this new type of regulatory approach would be that instead of regulating the weapon, rule regulates how the weapon should be used.

There exists several different ideas how cyber warfare should be governed. One opinion is that there has to be utilitarian cooperation between designers and operators. This includes the attorney who reviews the weapon and the attorney who decides the lawfulness of the target.[195] The ways and tests how the weapons are evaluated must be approved by both attorneys. Extremely urgent issue with regard to the cyber weapons is that all personnel who are dealing with cyber weapons have to be trained properly. Cyber weapons are quite different compared to conventional weapons, and it can lead to unfortunate consequences if the whole staff is not aware of this.

Taddeo says that cyber-regulation has followed two main points of view; the first one believes that the current legislation, such as the UN Charter, the Convention on Certain Conventional Weapons and AP I and II are adequate to regulate cyber weapons, they just need interpretation and in-depth analysis, such as the Tallinn Manual does.[196] Tallinn Manual is one great example of international cooperation and additionally it encapsulates the most comprehensive overview of the applicable legislation for cyber warfare so far.[197] Others argue that the old laws do not work in case of non-kinetic strikes, because they are intended for the old-fashioned bloody warfare.[198]

Some experts suggest that the international community should prepare a treaty. This is because, without it, the definition of cyber-attack is not clear, and secondly, it would provide better cooperation in the collection of evidence and the prosecution process between the countries in the attacks.[199]

---

[194] Asaro, *supra* nota 65, p 696.
[195] Kovach, *supra* nota 116, p 275.
[196] Taddeo R. Should we use old or new laws to regulate warfare in the information age 2015. blogs.oii.ox.ac.uk/policy/should-we-use-old-or-new-rules-to-regulate-warfare-in-the-information-age/ (18.04.2017).
[197] Schmitt, M. et al. *supra* nota 74, p 222.
[198] Taddeo, *supra* nota 196.
[199] Hathaway, O. et al. The Law of Cyber-Attack. Forthcoming in the California Law review, 2012. p 71 law.yale.edu/system/files/documents/pdf/cglc/LawOfCyberAttack.pdf (22.4.2017).

This view is also questioned. Treaty is not in sight, so one have to rely on the interpretation of IHL.[200] Kelsey argues that treaty is not possible or even necessary.[201] The rules should evolve through practice and experience. This is because States do not agree to regulate something whom capabilities they know so little about. In addition, cyber warfare makes it possible to lower the costs of warfare, so treaty hardly would get support at least for now. This is something that also applies especially militarily weaker States. Preparing of a treaty would be problematic because the preparation process need to include experts who possess knowledge and skills from other fields than law as well.[202] For this reason, the conventional courts whose configuration consists mainly of lawyers, would not be the best option for the enforcement of judgments either.[203] Additionally, it is noteworthy that also non-State actors, inter alia, terrorist groups certainly would ignore the new treaty.

Schmitt argues that governments should act now and start drafting the rules, because passivity can lead to the fact that non-State actors will decide on the issues and it may not be in the interests of the States.[204] He says that one reason for the passivation of the *opinio juris* is that States may see the ambiguities in cyber warfare rules as advantage and exploit the situation by interpreting the law as the best suits for them. The situation is a double-edged sword; if the matter is permissively regulated, it would allow the military operations, but at the same time it would also jeopardize State's own troops, the military and the civilians; and if the matter is strictly regulated or banned, their forces would be more secure, but the State could not execute cyber operations.[205] None of IHL rule is made for cyber warfare in mind[206] and therefore opinio juris is needed at least to clear what attack means in the cyber context, as well as who can be attacked against in the cyber context.

[200] Schmitt, M. et al. *supra* nota 74, p 222.
[201] Kelsey, *supra* nota 17, p 1449.
[202] *Ibid*.
[203] *Ibid*.
[204] Schmitt, M. et al. *supra* nota 74, p 230.
[205] Schmitt, M. et al. *supra* nota 74, p 224.
[206] Schmitt, M. et al. *supra* nota 74, p 230.

In addition to these, it is also proposed changes to national legislation as well as countermeasures.[207] The authors believe that, for example, the United States has a number of laws, which could be extended to give them extraterritorial reach. If other countries did the same, it would enable a very comprehensive field of enforcement. The authors argue that problems with the jurisdiction would be solved with more powerful extradition relationships.[208] In addition, one should think about countermeasures. These would be a good way to prevent attacks, especially as cyber attacks rarely rise at the level of armed attack, and as mentioned above, the definition is controversial. States should consider in advance, which means would be effective countermeasures, and in particular, which will fulfill the principle of proportionality.[209]

As previously discussed, the assessment of new weapons under article 36, is fully left under States' own discretion. This creates a challenge for sharing information, as State's own weapon development is often seen as a security aspect. Although State actors would assess the weapons as they should, there is always huge pressure on lawyers to pass the weapon.[210]

Article 36 has led to discussion of what "weapons, means and methods of warfare" really means. This causes several problems when assessment is carried out by the States. States may focus only on the fact that certain weapon is not expressly prohibited; the wording might be interpreted to cover only the weapons and not the mode of operation; or such lawyers and experts might be used, who evaluate weapons too unilaterally.[211] Besides all that, assessments are conducted in secret, so that no one, including other states could learn from any mistakes.

The regulation of new technology is overshadowed by the so-called *Collingridge dilemma*.[212] Technology, in this case, weapons, is easy to control in their early stages, but the real problems are not exactly known at that stage. The problems will only be known when something serious has happened, and at that point their controlling is more problematic and more expensive.

[207] Hathaway, O. et al. *supra* nota 199, pp 67-68.
[208] Hathaway, O. et al. *supra* nota 199, pp 68-69.
[209] Hathaway, O. et al. *supra* nota 199, p 70.
[210] Rappert, B. et al. *supra* nota 34, p 783.
[211] Rappert, B. et al. *supra* nota 34, p 782.
[212] Morozov, E. 2012: What is your favourite deep, elegant or beautiful explanation? www.edge.org/response-detail/10898 (19.04.2017).

As a solution is seen, for instance, co-operation. By combining experts in various fields in the evaluation phase, obtained multi-industry expertise and perspective is broad, extending beyond mere legislative aspects. This is done, for example, in Sweden, where a certain committee, namely *The Swedish Delegation for International Law Monitoring of Arms Projects* was founded in the 1970s, which assesses weapons the State develops or acquires.[213] Of such a committee in operation, it is essential that in addition to already prohibited weapons there is a reason to look to the future and think about what regulation should be considered in advance. The bad side is, the larger the group to execute the evaluations, the less they are able to meet and conduct evaluations.

Author of the thesis argues that the assessment of the legality of weapons could be transferred to a third party, neutral party, such as the ICRC. States could continue to be primarily responsible for dealing with evaluations, but a third party could make surprise inspections with full rights. This could change the evaluations made by the States for more precise and stringent.

As another option, individual reviewers can be used. This, however, can cause delays if there are many weapons to be evaluated. On the other hand, this makes it possible to arrange a certain meetings more flexibly for evaluations with many experts.[214]

In addition to experts in various fields, cooperation between different countries and civil society would be desirable, meaning all States, not just allies.[215] This would require transparency with regard to the findings made by the States, which of course may result in opposition from States. This, however, would make it possible that other countries have already solved the same problem that other States are only just discovered. Moreover, countries could work together to resolve legal and technical problems and learn from mistakes.

[213] Jacobsson, M. Modern Weaponry and Warfare: The Application of Article 36 of Additional Protocol I by Governments. International Law Studies, US Naval War College, 2006, 82, pp 183-192, p 185.
[214] McClelland, J. The review of weapons in accordance with Article 36 of Additional Protocol I. International Review of the Red Cross, 2003, 85 (850), pp 397-415, p 403.
[215] Jacobsson, *supra* nota 213, p 189.

In spite of these proposals McClelland considered the most important that countries comply with the obligation referred to them to perform the required evaluations and tests considering new weapons.[216] In addition, the tests should be continued despite the fact that the weapon would be in common use.

[216] McClelland, *supra* nota 214, p 415.

Conclusion

This thesis sought to ascertain what legal problems the above-mentioned weapons are creating within the framework of the current legislation as well as is there a need to change the existing laws or create entirely new ones. It seems that the legislation is partly sufficient but some of the rules need to be edited to be more suitable for contemporary weapons and to ensure there is no interpreting problems.

The use of drones has many great features from the military but from the law perspective as well. UAVs are much cheaper, than, for example jet fighters. Drones are controlled from a distance which causes no threat to own troops. Thanks to the drones' capacities, principles of precaution and distinction can be followed more properly. Collateral damage will be reduced significantly when the cameras and other sensors provide real-time material for the intelligence. Devices can also be used as marking military targets, so the target can be demonstrated with certainty. Excluding Hellfire missiles, drones' weaponry also causes smaller explosion radius, which reduces the potential harm to bystanders.

In spite of this, collateral damage occurs. Suspicion is raised because of activities by entities like the CIA, which is claimed to cause collateral damage, but in the absence of the official statistics and reports this is difficult to ensure. This lack of transparency has caused concern among many experts and it is called to create a threat to public safety. Secondly, it is presumable that the secretiveness does not inspire confidence towards the CIA.

However, the Special Rapporteur of the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism has said that the drones are feasible, if compliance with IHL is confirmed. This speaks in favor of it, that the current rules are sufficient. In contrast, differences in the interpretation of the rules will cause problems. For example, the United States interpret between the rules according to their own needs. Secondly, the assessment of the principle of proportionality, for example, is very often decided case-by-case, and

furthermore, different countries use different scale when considering the principle of proportionality.

A further concern stems from targeted killings. Persons are usually suspected terrorists, so who has ensured their guilt? Moreover, legal problems are caused by the principle of distinction, excessive use of force and the situation hors de combat.

The advantages of autonomous weapons are often similar, as UAVs. Circumstances where superhuman reaction time is required, an autonomous weapon is superior to humans. Autonomous weapon can use one second more time to identify the objective, even if it is threatened by a weapon, and use force only after recognition of the target. The precision rate is also growing significantly, thereby reducing the collateral damage, and these things together enhance the principle of proportionality and distinction. Other benefits include operations, where conditions are extremely harsh. Operations, where the loss of human lives are certain it is also politically preferred option, because the machine is expendable rather than human being. Machines also follow orders better than humans, because emotions do not affect the decisions. For this reason, machines may be even more humane, than the people.

Also, the problems are very similar, as with drones. At least at the moment, AWS can not comply with the principles of distinction and precautions. This is due to the fact that all the functions of the autonomous weapons are pre-encoded, and this does not enable the distinction between civilians and combatants. Although in the future there would be fully autonomous weapons, what will happen when the situation is not pre-encoded in the machine's system? In addition, when an error occurs, it would be good, if a man could intervene in some way. It is also only a matter of time before these weapons will be hacked, so such situations should be prepared for.

The defenders of the autonomous weapons say that even if the weapon is not able to distinguish between the civilian and combatants, weapons can be used in areas where there is no human fighters. This is because the weapons is able to decipher between the two objects. Also the

principle of proportionality raises its own problems. However, as mentioned above, this principle is always context-dependent and raises problems in the conventional warfare as well.

Cyber warfare is the latest addition to the forms of warfare. Also, this form of warfare is much cheaper compared to the conventional warfare and therefore has increased its popularity. Furthermore, cyber attacks can be done without risking human lives, their own and the opposing party's. For this reason, for cyber warfare it can also be easier to get people's permission as well as for the other above-mentioned weapons. The destruction can be caused, for example, to adversary's a communication system or energy source, so cyber attacks are very useful from military aspect.

Experts have raised questions, whether IHL applicable to cyber warfare. ICRC and many other experts say that it is applicable. The Internet is the most problematic feature of cyber warfare. Civilians and soldiers use the same routes in the world of the Internet. This enables the infringement of the principles of neutrality and sovereignty. Additionally, the impact is very difficult, if not impossible, to trace and therefore culprits often remain unpunished. Also, monitoring of the situation and prevention of attacks is particularly difficult in the cyber world. Individual codes does not in themselves do any harm, but when combined with other codes, they can compile a dangerous weapon. For this reason, it is almost impossible to notice, for example, by neutral States, if in their national territory, there would occur a preparations for cyber attack. The non-lethal nature of the cyber attacks also lower the threshold for illegal attacks, because human life is not in danger.

In the allocation of responsibilities there would be room for improvement. Theoretically, compensation from other entities than the State is possible, but may incur arduous for several reasons, especially in the individual case. State liability should be disclosed more clearly. Also, constituting a new system, War Torts, have been proposed.

According to the thesis, criminal liability may be placed on the person who deployed the weapon or the commander, or both. Moreover, the use of weapons would also be good to keep such on a

level, that the decision would at the end be on the hands of a human. This would make it possible that the search for the culprit would not be complicated. And of course, it would improve compliance with the rules, at least presumably.

Drones are regulated well enough, if the rules are not abused or interpreted wrongly. In case of UAVs the transparency should definitely be endeavoured more in order to strengthen people's trust. This would also increase the punity of wrong-doers, and hence support the justice system. The author of the thesis is of the opinion that behind the lethal decision must ultimately be a human being, even if in the future it would be possible to build a fully autonomous weapon. This would make it possible to prosecute the perpetrators and enable better complying with the rules.

Cyber warfare is a new form of warfare, and for this reason it requires specialists from many fields. It is not enough that the lawyers discuss solutions but rather there is a need for cooperation between different countries from different fields of experts. Proposed solutions include a treaty, a state practice, as well as countermeasures and editing national laws.

Article 36 of AP I would need re-consideration. Again, this Article as well calls for cooperation in various fields in different countries. The author argues that it is worth considering the establishment of a neutral third party, which would assess the States' weapons development and construction. The current operating model enables the circumvention of the rules, because States do not have any kind of notification obligation. If such third party is established, it would be desirable that the compliance of that Article by the States should be of public knowledge. Despite the existence of an independent body, the States itself could bear the main responsibility for the inspection and evaluation of weapons under Article 36. However, the group would be good to keep as an appropriate size to enable it to assess weapons potentially in a timely manner. The most important thing would be to get states to undertake their duties considering weapon assessments.

Was the solution no matter what, now would be the right time to begin to discuss how to edit the rules for these weapons, or the creation of entirely new rules. As mentioned, the national debate

would spread into a global discussion and the development of rules would this way get started. There are concerns that the rules are established only after the damage has already occurred, and the overall pressure in the elaboration of rules is large enough.

List of sources:

Books:

1. Gardam, J. Necessity, proportionality and the Use of Force by States. Cambridge, Cambridge University Press 2004

2. Henckaerts, J-M., Doswald-Beck, L. Customary international law, volume I, Rules. Cambridge, Cambridge University Press (2005)

3. Rogers, A. Law on the battlefield. Manchester, Manchester University Press 2012

4. Sandvik-Nylund, M. Caught in Conflicts: Civilian Victims, Humanitarian Assistance and International Law. Turku, Institute for Human Rights, Åbo Akademi University 2003

Legal materials:

5. Convention on Cluster Munitions (2008)

6. Convention (XIII) concerning the Rights and Duties of Neutral Powers in Naval War. The Hague, 18 October 1907

7. Convention (V) respecting the Rights and Duties of Neutral Powers and Persons in Case of War on Land. The Hague, 18 October 1907

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

9. Protocol on Explosive Remnants of War (Protocol V to the 1980 CCW Convention, 28 November 2003)

Journal articles:

10. Anderson, K., Waxman, M. Law and Ethics for Robot Soldiers. Policy review, 2012-2013, (176), pp 35-49

11. Asaro, P. On banning autonomous weapon system: human rights, automation, and the dehumanization of lethal decision-making. International Review of the Red Cross, 2012, 94 (886), pp 687-709

12. Backstrom, A., Henderson, I. New capabilities in warfare an overview of contemporary technological developments and the associated legal and engineering issues in Article 36 weapons reviews. International Review of the Red Cross, 2012, 94 (886), pp 483-514

13. Casey-Maslen, S. Pandora's box? Drone strikes under jus ad bellum and jus in bello, and international human rights law. International Review of the Red Cross, 2012, 94 (886), pp 597-625

14. Cass, K. Autonomous weapons and accountability: seeking solutions in the Law of War. Loyola of Los Angeles law review, 2015, 48 (1017), pp 1017-1067

15. Crootof, R. War torts: Accountability for autonomous weapons. University of Pennsylvania Law Review, 2016, 164 (6), pp 1347-1402

16. Diamond, E. Applying International Humanitarian Law to Cyber Warfare. Law and National Security: Selected Issues 2014, 138, pp 67-84

17. Graham, D. The U.S. employment of unmanned aerial vehicles (UAVs): An abandonment of applicable international norms, Texas A&M law review, 2015, 2, pp 675-694

18. Heintschel von Heinegg, W. Territorial Sovereignty and Neutrality in Cyberspace. International Law Studies, US Naval War College, 2013, 89, pp 1-156

19. International Humanitarian Law and New Weapon Technologies, 34th Round Table on current issues of international humanitarian law, San Remo, 8–10 September 2011, International Review of the Red Cross. 2012, 94 (886), pp 809-817

20. Jacobsson, M. Modern Weaponry and Warfare: The Application of Article 36 of Additional Protocol I by Governments. International Law Studies, US Naval War College, 2006, 82, pp 183-192

21. Jenks, C. Law from above: unmanned aerial systems, use of force, and the law of armed conflict. North Dakota law review, 2009, 85 (649), pp 649-672

22. Jensen, E. Sovereignty and Neutrality in Cyber conflict. Fordham International Law Journal, 35 (3), 2012, pp 814-841

23. Kelsey, J. Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the age of Cyber Warfare. Michigan Law Review, 2008, pp 1427-1451

24. Kesan, J. et al. Mitigative Counterstriking: Self-defence and Deterrence in Cyberspace. Harvard Journal of Law and Technology, 2012, 25 (2), pp 429-544

25. Kovach, C. Beyond Skynet: Reconciling increased autonomy in computer-based weapons systems with the laws of war. Air Force Law review, 2014, 71, pp 231-277

26. Liu, H. Categorization and legality of autonomous and remote weapons systems. International Review of the Red Cross, 2012, 94 (886), pp 627-652

27. McClelland, J. The review of weapons in accordance with Article 36 of Additional Protocol I. International Review of the Red Cross, 2003, 85 (850), pp 397-415

28. Rappert, B. et al. The roles of civil society in the development standards around new weapons and other technologies of warfare. International Review of the Red Cross, 2012, 94 (886), pp 765-785

29. Roff, H. Lethal autonomous weapons and jus ad bellum proportionality. Case Western Reserve Journal of International Law, 2015, 47, pp 37-52

30. Roff, H. To ban or to regulate autonomous weapons A US response. Bulletin of Atomic Scientists, 2016, 72(2), pp 122-124

31. Rosenzweig, I. Targeted Killings during High and Low Intensity Warfare. Law and National Security: Selected Issues 2014, 138, pp 41-52

32. Schmitt, M. et al. The decline of international humanitarian law opinio juris and the law of cyber warfare. Texas international law journal, 2015, 50 (2), pp 189-231

33. Sher, J. Comment anonymous armies: Modern "cyber-combatants" and their prospective rights under humanitarian law. Pace international law review 2016, 28 (1), pp 233-275

34. Takemura, H. Unmanned aerial vehicles: Humanization from international humanitarian law. Wisconsin International Law Journal, 2014, 32 (3), pp 521-546

35. Terzian, D. Right to Bear (Robotic) Arms. Penn State Law Review, 2013, 117, (3), pp 755-796

36. 31st International Conference of the Red Cross and Red Crescent, International Humanitarian Law and the challenges of contemporary armed conflicts Report Document prepared by the International Committee of the Red Cross 2011, pp 1-53

Newspaper articles:

37. The Sydney Morning Herald, Boston bombings revenge against US: Tsarnaev, 17.5.2013. www.smh.com.au/world/boston-bombings-revenge-against-us-tsarnaev-20130516-2jpv0.html

Case law:

38. ICJ 9.4.1949, Corfu Channel (United Kingdom of Great Britain and Northern Ireland v. People's Republic of Albania)

39. ICJ 8.7.1996, Legality of the Threat of Use of Nuclear Weapons, Advisory Opinion

40. International Criminal Tribunal for the Former Yugoslavia, no. IT-98-29-T, Prosecutor v. Galić, Judgment and Opinion, 5.12.2003

41. Permanent Court of Arbitration 4.4.1928, Island of Palmas (or Miangas) (United States v. The Netherlands)

42. Supreme Court of the United States, No. 09–1343., J. McIntyre Machinery, Ltd. v. Robert Nicastro

43. Supreme Court of the United States, No. 86-492, Boyle v. United Technologies Corp.

E-materials:

45. Computerworld. Why did Stuxnet worm spread?, 2010
www.computerworld.com/article/2516109/security0/why-did-stuxnet-worm-spread-.html

46. Coupland, R. The Effect of Weapons: Defining Superfluous Injury and Unnecessary Suffering 1996. www.ippnw.org/pdf/mgs/3-coupland.pdf

47. Future of Life Institute. Who is Responsible for Autonomous Weapons?
futureoflife.org/2016/11/21/peter-asaro-autonomous-weapons/

48. Gevorgyan, K. Concept of State sovereignty: Modern Attitudes.
ysu.am/files/Karen_Gevorgyan.pdf

49. Hathaway, O., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., Spiegel, J. The Law of Cyber-Attack. Forthcoming in the California Law review, 2012
law.yale.edu/system/files/documents/pdf/cglc/LawOfCyberAttack.pdf

50. Human Rights Watch and Harvard Law School's International Human Rights Clinic. Fully Autonomous Weapons: Questions and Answers, 2013.
www.hrw.org/sites/default/files/supporting_resources/10.2013_killer_robots_qa.pdf

51. International Security Advisory Board, Report of Forces Agreements, www.state.gov/documents/organization/236456.pdf

52. Kathleen Lawand, Fully autonomous weapons systems. www.icrc.org/eng/resources/documents/statement/2013/09-03-autonomous-weapons.htm

53. Morozov, E. 2012: What is your favourite deep, elegant or beautiful explanation? www.edge.org/response-detail/10898

54. Rule 70. Weapons of a Nature to Cause Superfluous Injury or Unnecessary Suffering. International Committee of the Red Cross. www.ihl-databases.icrc.org/customary-ihl/eng/docs/v1_cha_chapter20_rule70

55. Taddeo R. Should we use old or new laws to regulate warfare in the information age 2015. blogs.oii.ox.ac.uk/policy/should-we-use-old-or-new-rules-to-regulate-warfare-in-the-information-age/

56. The Ethics of autonomous weapons systems, University of Pennsylvania Law School. www.law.upenn.edu/institutes/cerl/conferences/ethicsofweapons/

57. The law of armed conflict, neutrality. International Committee of the Red Cross 2002. www.icrc.org/eng/assets/files/other/law8_final.pdf

58. The United States Navy, MK-15 - Phalanx Close-In Weapons System, www.navy.mil/navydata/fact_display.asp?cid=2100&tid=487&ct=2