TALLINN UNIVERISTY OF TEHCNOLOGY

School of Business and Governance

Department of EU and International Law

HAJB08/14

Igor Tsverkunov

IMPLICATION OF INTERNATIONAL HUMANITARIAN LAW IN FIELD OF CYBERSPACE WARFARE

Bachelor's thesis

Programme HAJB08/14

Supervisor: Evhen Tsybulenko, PhD

Tallinn 2020

I declare that I have compiled the paper independently and all works, important standpoints and data by other authors have been properly referenced and the same paper has not been previously presented for grading.

The document length is 15 796 words from the introduction to the end of summary.

Igor Tsverkunov ……

(signature, date)

Student code: 153998HAJB

Student e-mail address: tsverkunov.ingvarr@gmail.com

Supervisor: Evhen Tsybulenko, PhD:

The paper conforms to requirements in force

……

Chairman of the Defence Committee:

Permitted to the defence

……

(name, signature, date)

TABLE OF CONTENTS

ABSTRACT

Today, cyber weapons, as a way of warfare, including autonomous weapons systems, are a problematic area that is covered by law either partially or with a certain number of gray zones or legal gaps. Some of the sources of law like IHL and Customary IHL have become outdated by now, so their application in area of cyberwarfare is controversial. In addition, despite the fact that states independently improve their cyber strategies at the national level, there is no specific legally binding document at the international level. The main aim of this thesis is to find out how international humanitarian law can be applied in the field of cyber war by detecting outdated norms and principles and suggesting alternative ways to solve this problem. As a result of the work done, an answer was found to the main question of the thesis. International humanitarian law may apply to cyber weapons, drones, and autonomous weapons systems, but states can use these types of weapons to their advantage, bypassing the law because of its vague wording. As a solution, it was suggested that the interpretation of certain rules, principles and definitions shall be revised in order to avoid potential violation by states. In addition to this, as a result of the analysis, outdated norms of the law were revealed, which to this day cannot be the subject of international humanitarian law. Thus, it was proposed to revise the existing law and create, firstly, a single document regulating the use of cyber weapons and, secondly, states to conduct an independent report to a third party, such as the International Committee of the Red Cross, about successful and unsuccessful attempts creating and using cyber-weapons to make it easier to regulate in the early stages.

Keywords: cyberwarfare, international humanitarian law, drones, autonomous weapon systems, repsonsibility, international committee of the red cross

INTRODUCRTION

War - in the opinion of many philosophers is an integral part of life on Earth, because war, as it creates, and destroys. Throughout the life of our planet, there have been a number of wars caused by various factors: the economic situation of a state or empire, the existence of economic classes, political influence and various political views, a sense of power and greatness, a sense of justice and patriotism, and much more. It is no secret to anyone that there is such a thing as “the art of war”. The art of war embodies the ordering of military disciplines and the norms for the development of military affairs, without whose existence it would be difficult to wage war in view of chaos. The art of war includes various strategies, methods of warfare, determining the position of the military and civilian, choosing, creating and improving weapons and much more. Like any other field, military art cannot exist without development. Since military affairs often violates the principles of humanity and ethics and is often aggressive, the authorities of different countries and different nationalities are trying to stabilize this art and make it as humane as possible. Thanks to the leap in military affairs, other structures are developing in parallel, in particular, legal and political. Armed conflicts create the ground for the creation of new legislation, which, in turn, sets the stage for the development of the art of war. It is not possible to submit major articles, for example, of the European Convention on Human Rights (ECHR), without a prior violation of these rights. In the same way, it is impossible to imagine the current military structure without the development of human rights. Both concepts go side by side.

As a result, the development of other structures also does not stand still, especially the development of technology. In this particular study, we will focus on the development of robotic technology, which is used not only by ordinary people to simplify their life needs or personal protective equipment, but also becomes a terrible weapon with a certain use. The current type of warfare is very different from what it was a century ago. The development of technology introduces very usable facilities into the world, the regulation of which is problematic. It is easy to bring a person to retaliation, but to hold accountable is that which is not controlled or is managed mediocrely, or in general is not a person and can self-destruct - is difficult.

Cyberspace activities that affect national security issues are high on the agenda of politicians and military leaders around the world. At different levels of governments of different countries, new cybersecurity structures are being created. Cyber operations conducted in situations of armed conflict can have very serious humanitarian consequences for the civilian population.

Fortunately, until now, cyber operations, which served as means and methods of warfare during armed conflicts, did not lead to tragic consequences from a humanitarian point of view. However, despite the fact that the military potential of cyberspace has not yet been fully studied and not widely understood, cyber operations against transport infrastructure facilities, power grids, dams, chemical plants and nuclear power plants are technically possible. Such operations can entail extensive consequences, leading to a large number of civilian casualties and causing significant damage. With a greater likelihood, cyber operations and cyber weapon can be used as a means of influencing civilian infrastructure facilities, disabling them or leading to disruptions in their work - and such an impact could immediately lead to the death or injury of people.

In the first paragraph of this thesis, the author will introduce the main principles of International Humanitarian Law that apply in the field of the use of modern weapons. Thank to these principles, the reader would be more clear in what way and by what means the use of various measures of warfare is regulated. Then the author will talk about the types of modern weapons that exist and are most problematic in the legal environment, explaining why these types of weapons are controversial and which principles of international law they can violate or violate. In the next paragraph, the author will streamline the first two paragraphs, explaining the relationship between the above main legal principles and the weapon to which these principles are applied. The third part of the thesis is focused on the analysis of legal norms that may be violated and / or violated by the use of new weapons. Also, answering the main question of this work, it is important to analyze the legal responsibility of individuals or states using modernized weapons as a means of warfare. As a result of this analysis, the author will identify the weaknesses of the law and the gap within it that governs the use of modern weapons. In the last part of the thesis, the author will suggest potential solutions to problems.

The reason why the author chose this topic is relevance. The problem of the thesis that was described above is relevant in our time and, firstly, has not been fully studied by legal experts, and secondly, it has a sufficient number of gaps in the law and regulation. Thus, thesis is mainly aimed at finding **how can international humanitarian law regulate the use of cyber weapons, both by civilians and the military** by finding weak, outdated sides of the legislation that specialize specifically in resolving the aforementioned means of warfare. Also, it is worthwhile to figure out how well the legal structure regulates the use of these devices in military affairs and, if possible, put forward new or improve existing solutions. As to the research method, three methods will be used. Firstly, in the case of qualitive method author would need to delve into the

study of specific information by analyzing different sources such as books, articles and *opinio juris* of different legal representatives, hence research data. Qualitative analysis methodology, as a result it focuses on getting knowledge through open-ended and informal communication. Secondly, "black letter" method will be used. The most important point of this technique for research is to compose and depict lawful guidelines and to offer critique on the rise and hugeness of the definitive lawful sources in which such principles are considered. Specifically, case law, with the point of distinguishing a hidden framework. Eventually, author will use quantitive method because the final opinion will be based on gathering information from a survey of people who are versed in the field of the topic.

1. GENERAL LEGAL FRAMEWORK

1.1 IHL and CIHL fundamental principles

1.1.1 Definition of armed conflict

According to the ICRC, there are currently only two types of armed conflicts: an international conflict, which involves the participation of two or more states, and a non-international armed conflict, which consists of domestic government forces and non-governmental armed groups.[1]

1.1.1.1 International Armed Conflict (IAC)

According to Article 2 of the 1949 Geneva Convention, "In addition to the provisions which shall be implemented in peacetime, the present Convention shall apply to all cases of declared war or of any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them. The Convention shall also apply to all cases of partial or total occupation of the territory of a High Contracting Party, even if the said occupation meets with no armed resistance ".[2]

Despite the fact that open hostilities may not directly exist, however, particular principles and rules of international humanitarian law must be respected.

Also, according to this article, it is absolutely not necessary to formally declare the status of war, and regardless of whether the other side accepts this status, the conflict can have the status of an international armed conflict, no matter how long the conflict and open hostilities last. However, at least one of the parties must be a member of an international agreement and convention in order for its rules to take effect.[3]

[1] ICRC Opinion Paper. (2008) How is the Term "Armed Conflict" Defined in International Humanitarian Law? p 1
[2] See Article 2 of the 1949 Geneva Convention
[3] See Article 2 of the 1949 Geneva Convention

1.1.1.2 Non-international armed conflict (NIAC)

In order to distinguish between an internal armed conflict from another activity that involves the use of weapons and equipment, the situation must meet the following criteria:

1. The level of hostilities should reach a minimum intensity. Examples include cases where police action is not enough to resolve the conflict, which is why the state must intervene and take action.

2. If the state is the first batch, then the second batch should have a warring character for the first batch. This means that the second party must have sufficient forces to carry out military operations, the level of military training and the availability of military resources, as well as the second party must be under the strict supervision of the commanding structure.

Whereas in the previous case, in order to have the status of an international armed conflict, at least one party must be a member of the international agreement, in this case, if a certain state is not a party to the international agreement, then its articles cannot be used, it also disappears and non-international armed conflict status. [4]

1.1.2 Principle of humanity in IHL

The fundamental principle of international humanitarian law is the principle of humanity. It founds his concrete normative embodiment in all humanitarian international legal documents. If we turn to the texts of the Geneva Conventions for the Protection of Victims of the War of 1949, we can easily find illustrations of the principle.

Thus, Article 3 (1) of the Geneva Convention states that persons that do not directly take part in hostilities, including those who do not carry their arms openly anymore, as well as those who have ceased to participate in hostilities due to injury, detention or for any other reason, must under all possible circumstances use humane treatment.[5] To this end, the convention prohibits all forms of assault on life and physical integrity, all forms of murder, mutilation, ill-treatment and torture. Similar idea could be found in other Geneva Conventions. For example, in Article 13 of the 4th Geneva Convention requires the humane treatment of prisoners of war.[6]

[4] ICRC (2008), supra nota 2, p 2.
[5] See Article 3(1) of the 1949 Geneva Convention IV
[6] See Article 13 of the Geneva Convention IV

The content of this principle is constantly expanding. For example, the environment is already involved in its spectra as an object of possible military use, the consequences of which can catastrophically affect a person. The principle of humanity not only laid the foundations for the formation of other principles of international humanitarian law, for example, the principle of protecting civilians, but is constantly being improved, finding concrete expression in new norms, regulations and codes of law.

Also an integral part of this principle is the choice of weapons. The main criteria for the unconditional prohibition of specific types of weapons are the consequences of their use, namely: excessive suffering, the inevitable death of people incapacitated, violation of the ecological balance. It should be especially noted that to ban a particular type of weapon, it is sufficient to comply with any of the above criteria.

In addition, the principle of honesty and good faith in the choice of methods used and the course of hostilities. In accordance with it, the belligerents must show honesty and conscientiousness and not resort to treacherous, treacherous and treacherous methods. It is specified in the IV Hague Convention of 1907, which prohibits the treacherous killing or wounding of persons belonging to the population or troops of the enemy; killing or injuring an enemy who surrenders a weapon or, having no more means to defend himself.[7] In the Geneva Convention for the Protection of Victims of War of 1949, the main idea behind this principle is reflected in Art. 3 as it contains a list of prohibited actions in relation to persons who are not directly involved in hostilities, as well as in customary IHL rules, which prescribe standards of conduct in the case of, for example, *hors de combat*.[8]

1.1.3 The prohibition on the infliction of unnecessary suffering

Currently, Article 35 of Additional Protocol I stipulates that warring parties must be extremely careful in their choice of methods of warfare. The will to choose methods and types of weapons is limited. This article is one of the fundamental, since it entailed the creation of a separate convention called the Convention on Prohibitions or Restrictions on the Use of Certain

[7] See Article 23 of The Hague Convention IV 1907
[8] Article 3 Geneva Convention for the Protection of Victims of War of 1949

Conventional Weapons which may be deemed to be Excessively Injurious or to have Indiscriminate Effects 1980. [9]

Section 35 (2) prohibits the use of methods of warfare, which by nature may cause unnecessary torment. This principle mainly refers to the effect of the weapon, from which the soldier will suffer excessive suffering. States generally agree that suffering without military necessity, that is, not being a military objective, is a violation of this rule. This rule immediately includes three important principles of international humanitarian law. Firstly, the principle of military necessity, secondly, the precautionary principle and, thirdly, the principle of proportionality.[10]

Examples of weapons that cause excessive suffering or injury are lasers that are directed at the eyes of a soldier, after which the soldier is left without vision and is unable to recover him; a certain type of mine, after contact with which the soldier is not able to move independently; explosive bullets, wounds from which it is impossible to operate and the like. In general, a weapon that is inevitably fatal to a soldier violates this principle.

It is widely known, many states have not signed and ratified Additional Protocol I, however, they widely use and practice this rule within their national law.

1.1.4 The distinction between civilians and combatants.

For the first time, the principle of distinction civilians and combatants was born and described in the St. Petersburg Declaration, according to which the only legitimate goal that a State should pursue during a war is to suppress the enemy's military power. Further, the protection of civilians was described in The Hague Regulation in Article 25 [11]and in the Geneva Convention Additional Protocol 1 in Articles 48, 51 (2), 52. While the listed sources of law are Customary International Law, in many states the "attack" of a civilian should be considered as a criminal offense and is punishable at the national level. Also, despite the fact that many states did not sign the convention, the ICRC's appeal to concerning states to respect civilian lives and distinct them from the military was successful.[12]

[9] Articles 35, 35(1) of AP I
[10] Article 35 (2) of AP I
[11] Article 25 of The Hague Convention 1907
[12] Articles 48, 51(2), 52 of AP I

This principle explains who are civilians and what should be considered as a military objects and when the attack is lawful in the event of an armed conflict. The principle prohibits direct attack of such objects and persons. In case of violation of this principle, the violation should be considered as a war crime. In addition, the creation of weapons that are unable to distinguish between military and civilian persons or/and objects should be prohibited.

Also, Article 54 of Additional Protocol I prohibits, regardless of motive, the attack or transfer of such facilities that could deprive civilian resources necessary for life. Such objects can be agricultural fields where food is grown, stations with drinking water and livestock. [13]Military facilities that are located in close proximity to nuclear power plants or nuclear laboratories are of particular danger, after destruction of which the damage to the civilian population is guaranteed.

1.1.4.1 Definition of Civilian

A civilian is a person who is not a member of the armed forces and does not directly participate in hostilities, is not a volunteer or member rebel force, or does not spontaneously raise a weapon during hostilities to stop or resist the invading forces. [14]

In case if a civilian takes a direct part in hostilities, he loses civilian status and does not receive the status of combatant, which means, firstly, that a civilian could become a target for an enemy forces, and secondly, civilian may lose the opportunity as a combatant to have captive rights. Therefore, the right to be protected during an armed conflict remains on the choice of the civilian itself.[15]

Such a concept as *levée en masse* is applied only when residents of an unoccupied territory spontaneously arm themselves to resist enemy troops and fight back, respecting the norms and laws of armed conflict, not having time or possibility to organize themselves into regular armed forces. With such actions, and only, civilians have the status of Prisoners of war in case if captured. The element of spontaneity plays a key role here, because if there was time for organization, then such a group of people would bear the character of an organized resistance

[13] Article 54 of AP I
[14] ICRC Rule 5 of CIHL
[15] Ibid.

movement which is not endowed with combatant privileges and such hostilities may be considered as an act of war or war crime.[16]

1.1.4.2 Definition of Combatant.

Combatant has right to take direct part in hostilities between states. In international armed conflicts, combatants should meet the criteria of being under the command of a person responsible for subordination, have distinctive signs, emblems or uniform that could be recognized from a distance, carry weapons openly, and carry out operations in accordance with laws and agreements on war. [17]

In case if captured combatants should be treated as Prisoners of War. The rights of war hostages are described in III Geneva Convention Articles 12-16.[18]

1.1.5 Principle of proportionality.

One of the most important tasks of international humanitarian law is to preserve and protect the civilian population from attacks. Along with other principles and rules, the principle of proportionality is one of the main rules of Customary IHL[19] and is described in Article 51 (5) (b) and in Article 57 (2) (a) (iii) of Additional Protocol I [20], despite the fact that that the principle of proportionality is not explicitly stated in Additional Protocol I. The principle and rules must be observed in the lawful use of force by the state or by an individual or group of people. In the case of non-compliance with which such actions can be considered as an act of aggression, even if carried out in accordance with the rules of *jus ad bellum.* [21]The legal basis for the use of force will be described below in the course of work.

In the modern sense, the principle of proportionality consists in eliminating the act of aggression in the event of a legitimate attack, that is, with self-defense or defense of a third party, without exceeding the forces that the aggressor spends. For example, if a person is attacked without weapons, the use of knives or firearms against the attacker will be disproportionate, hence

[16] Ibid.
[17] ICRC Rule 3 of CIHL
[18] See Articles 12-16 of the Geneva Convention (III)
[19] ICRC Rule 14 of CIHL
[20] See Articles 51, 57 of AP I
[21] Casey-Maslen, S (2012) Pandora's box? Drone strikes under jus ad bellum and jus in bello, and international human rights law. International Review of the Red Cross. p 604

illegal. However, militarily, this principle has a similar meaning, but is controversial. Some consider the principle of proportionality when they create and / or use weapons, so that their effect does not cause unnecessary injuries and suffering. Others consider the principle of proportionality in the vein of events where a civilian may be randomly affected when hostilities pursue a legitimate military goal. [22]

Often, in hostilities, there is not always time to sensibly assess the situation when preparing an attack. Naturally, pursuing military objectives, civilians can suffer while in the immediate vicinity of military installations. However, the principles of international humanitarian law, in particular the principle of proportionality, seeks to minimize such cases where the civilian population suffers. These decisions should be made by the commanders with full responsibility and adequacy, using all possible sources to reduce the risk to a minimum. If this rule is not respected, in many countries, such negligence will have the status of a war crime.

1.1.6 The prohibition of discriminate attack

Article 51 of Additional Protocol I is fundamental in protecting civilians from any type of attack during hostilities. This article describes a wide range of protections, from which a large number of Customary IHL rules follow. [23]

One of these rules is Rule 12, based on Article 51 (4), which prohibits any indiscriminate attack. According to this article, an attack is indiscriminate if the attack is not aimed at a specific military target; an attack in which the methods and means used cannot be directed to achieve a specific military goal; an attack in which methods of fighting are not used in accordance with the restrictions of international humanitarian law. Also, according to paragraph 5 of this article, attacks are indiscriminate and thus prohibited if: if the attack is a bombardment, where the concentration of civilian and civilian objects is approximately equal to the share of military objects, for example, in villages or cities; an attack that could result in the accidental loss of civilian population and / or civilian objects, creating an excessive direct military advantage.[24]

This principle is fundamental because it combines the application of the principles of proportionality and distinction, prohibits the use of certain weapons, which are described in

[22] Liu, H. Categorization and legality of autonomous and remote weapons systems. International Review of the Red Cross, 2012, 94 (886). P 628
[23] See Article 51 of AP I
[24] ICRC Rule 12 of CIHL

Protocol II and Amended Protocol II to the Convention on Certain Conventional Weapons and international humanitarian law in general. The rules following from this principle are used in both international and non-international armed conflicts, the violation of which is a war crime.

2. TYPES, TOOLS AND WEAPONS OF WARFARE

2.1 Cyber and Information warfare.

Cyber-warfare is a term, which means the aggressive use or misuse of advanced digital or computer technologies leading to harm the fundamental interests of a political community. A political community is a country, state, or nation. The most fundamental interests of such are: public and private safety and security; access to necessary resources; the right to political power without domination from other States; the right to grow economic aspects; the balance between creative innovation and reliable stability. States' basic interests are to be considered as: freedom from invasion; freedom from domination; and secure possession of resources which are indispensable to survive. Cyber-warfare is often associated with following activities:

1. espionage or reconnaissance (i.e., using the Internet, malware or DDOS attacks to gather target States' secret, confidential, codified or classified information);

2. the spread of disinformation aimed to achieve political, economic, military or other goals of the strategic level, by influencing the civilian population, the authorities and/ or armed forces of the opposing side, by disseminating specially selected and prepared information, information materials, and countering such impacts on one's own side; and/or

3. sabotage or data destruction of various systems which are vital to the basic abovementioned interests of a political and States' community. Generally, such systems are: electricity, power and atomic plants; fuel and water; manufacturing facilities; transportation on land and air systems; banking and the market. [25]

As to the challenges of cyber warfare, following are to be mentioned:

1. Absence of physical boundaries. It means that the world's network, alluded by numerous individuals as "the internet" has no physical limits. The opposing side does not necessarily have to be a country; it could be a meeting of similar people connected via the Internet in the visiting

[25] Floridi. L., Taddeo. M. (2014) The Ethics of Information Warfare: Analyzing Information Warfare. Volume no. 14. London: Springer Science & Business Media

rooms to fit for a criteria of a potential enemy. The expansion of access to and through the Internet creates certain understanding of enemies.

2. Absence of front line. There is no certain combat zone of warfare. The development of technology brings the front lines home. Orders may be executed from a computer using a home Internet connection.

3. Difficult to detect and hard to track. If it is likely that the attack is organized and compiled, it cannot be tracked regardless of where it started and who is responsible for it. or at the best scenario, the detection would take exessive amount of time. One could be able to wage a hidden war, inflicting great damage on any goal of community, without being recognized and, accordingly, without being subjected to retaliation.

4. Affordability in terms of organization and price. For comparison, it is worth giving an example of the price of equipment for an average soldier, which varies from 1,400 to 17,000 US dollars, according to data collected by a survey. The average price for a personal computer that can pose a threat to cybersecurity costs about 400 US dollars. Hackers or cyber-warfare operators often use programs, apps and tools that do not require any investment. For example, some programs can decode or encrypt a secret key in under a moment. Naturally, waging war in cyber space is more profitable and easier than waging traditional warfare using weapons.

According to the survey, nowadays it is in the region of 30 countries that create, develop and use malicious computer programs. The largest developers are the leading countries, in particular, in the field of military industry: China, the USA, the Russian Federation and Israel. However, regardless of military power or the availability of certain resources, the development and status of danger in the cyber industry may appear even in a small state. [26]

2.1.1 Offensive cyber operations

2.1.1.1 Estonian DDoS attacks in 2007

In 2007 The Republic of Estonia suffered the first coordinated, large-scale cyber-attack. Both Estonian government and private systems were subject to a cyber-attack. The reason was the contradictory decision to transfer the Bronze Soldier monument from the time of World War II,

[26] 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.

set in the Soviet times, from the central part of the city to the area where the majority of the population is Russian-speaking. [27]

Such actions led to a three-week cyber siege in the form of an overload of public website servers. DDoS attacks carried a different nature. Some forms of attacks replaced the real content of websites with sites with Russian anti-fascist propaganda; another and larger form of attacks was expressed at the completion of the websites. [28]However, along with such insignificant and harmless attacks, there were also those that stifled the websites of the Prime Minister, thus disabling law enforcement, governmental, banking, media and Internet infrastructures, endangering not only the state's economy, but also internal public order and security.[29]

2.1.1.2 Georgian attacks in 2009

As a result of disputes regarding the pro-Russian autonomous region of Georgia in the region of South Ossetia, a war broke out between the Russian Federation and Georgia. During the war, not only direct military operations were carried out using bombs and weapons, but also cyber-attacks. As a result of cyber-attacks, many web servers were disabled, which led to the suspension of the communication function and caused even greater embarrassment within the state.

As in the aforementioned case, the case was related to DDoS attacks, by overloading the servers with a lot of requests. Communication between the government and citizens of Georgia was suspended, which is very difficult to imagine when military operations are taking place inside the country and communication is needed more than ever. The websites of the president's office, the Ministry of Foreign Affairs, and the Ministry of Defense were temporarily unavailable, while Russian troops were entering lands of Georgia.[30]

[27] Benatar M. (2009), 'The Use of Cyber Force: Need for Legal Justification?', 1 Goettingen Journal of International Law, pp. 375–394, p 385.
[28] Shackelford, S. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. - Berkley Journal of International Law (BJIL), 25(3), 191-250, p 205.
[29] Tikk, E. Kaska, K. Vihul, L. (2010). International Cyber Incidents, Legal Considerations, Cooperative Cyber Defense Center of Excellence, CCDCOE, 2010, 4-120, p 81.
[30] Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. - Loyola of Los Angeles International and Comparative Law Review, Winter 2010 Volume 32 (1), 303-333, p 304.

2.1.1.3 Stuxnet in 2010

In 1960, the Islamic Republic of Iran began the development of an atomic program, which for 50 years was either suspended or resumed again. Iranian leaders and politicians attributed their interest in developing the nuclear program to the fact that they wanted to invent electricity without using oil, which in turn would be exported separately, and that they wanted to develop new fuel for medical reactors.[31]

However, the US and Israeli authorities expressed skepticism towards such statements. Thus, for the purposes of an intelligence operation, a virus was created to verify the good faith intentions of the Iranian Islamic Republic.[32]

A cyber-attack was nothing more than a worm (virus), which did not intend to have actual harm, but to disable industrial control systems. The virus could monitor and scan data from systems, delivering this data to the developers of this program. As a result of this cyber operation, not only the data of the Islamic Republic of Iran, but also other countries such as Australia, India, Indonesia and Britain were affected. [33]

As it turned out later by analyzing the attack by experts from different countries, the malware was invented not to intercept any data, but specifically to destroy certain targets, such as gas centrifuges, which were enriched with uranium for nuclear industrial purposes. As in was in this case. Thus, the destruction was of a military nature, rather than recon-collective. [34]

2.1.1.4 Ukrainian attacks in 2015

A cyberattack on energy companies in Ukraine is the first registered successful cyberattack on an energy system with the failure of it. It happened on December 23, 2015. Russian attackers managed to successfully attack computer control systems of three energy supply companies in Ukraine. The next, and much less large-scale, cyber-attack occurred on the night of December 17-18, 2016. Within no more than one hour, the substation Severnaya of the "Ukrenergo" energy

[31] Richardson, J. (2011). Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. - The John Marshall Journal of Computer & International Law an International Journal on Information Technology, Fall 2011, 29(1), p 1-27, p 8.
[32] Lindsay, J. R. (2013), Stuxnet and the Limits of Cyber Warfare - Security Studies, Vol. 22, No. 3, pp 366.
[33] Richardson, J. (2011) Supra note 2. p 9.
[34] Ibid. p 11.

company was disabled, consumers without electricity remained the northern part of the right bank of Kiev and the surrounding areas of the region. The consumers of "Prikarpatyeoblenergo" suffered the most from the first cyber-attack: about 30 substations were turned off, more than 200,000 residents were temporarily without electricity.[35]

In general, the cyber-attack was complex and consisted of a minimum of the following components:

1. pre-infecting networks with fake email using social engineering methods
2. capture control ASDU with operations shutdown at substations;
3. failure of IT infrastructure elements;
4. destruction of information on servers and workstations;
5. attack on the phone numbers of call centers, with the aim of denial of service to de-energized subscribers.

Due to the fact that the nature of the cyber-attack brought destruction, this case, along with the above-mentioned, should also be considered from the point of view of International Humanitarian Law. [36]

2.2 Drones

Drones (likewise called RPAS, Remotely Piloted Aircraft Systems, or UAV, unmanned aerial vehicles) are airplane without a human pilot ready, which are guided by a remote pilot. UAV have been produced for military use however are currently progressively utilized for common purposes. [37]

Despite the fact that, on the one hand, drones are utilized for basic and common insurance, ecological assurance, law requirement and reconnaissance, news-casting, business exercises and relaxation, while it is predicted that later it would possibly be utilized for different missions, for example, farming, vitality, transport of products and freight - and even of individuals. Drones can do tasks in crisis circumstances, where human mediation is either incomprehensible or

[35] E-ISAC, SANS ICS. (2016) Analysis of the Cyber Attack on the Ukrainian Power Grid.
[36] Ibid.
[37] 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 653.

troublesome. On the other hand, drones are as a rule joined with applications, for example, cameras, camcorders counting high power zoom, facial acknowledgment, conduct profiling, development identification; number plate acknowledgment, warm sensors, night vision, radar, transparent imaging, Wi-Fi sensors, amplifiers and sound account frameworks, biometric sensors and other applications depending on a target of use. [38]

Thus, in view of the huge range of capabilities and multi-functionality, drones have a place to be in the military sphere and carry out military tasks, ranging from reconnaissance to coordinated attacks and targeted killings. [39]

The first widely known use of UAV was in 1960 in the armed conflict in Vietnam by the United States, in Bosnia and Herzegovina in 1990, and in the same year in Kosovo. Also, in 2012, drones were used in Syria to detect and track rebel forces. However, as the intentions are different, in view of which the drones became famous for their ability in terrorist operations as targeted killing weapons.[40]

Nowadays, UAVs are widely used in armaments in at least 44 countries, led by the previously mentioned USA, Israel, the Russian Federation and Canada. [41]

As to the main challenges of the UAVs:

1. As with cyber-attacks, it's difficult to identify and track a UAW. Those cars that are not bought in a regular electronics store, or made by yourself for personal purposes - may not be advanced with a GPS navigation system, which makes it difficult to detect and track;
2. similarly, to cyber-attacks, does not require large investments in relation to other military equipment;
3. it is easy to do it yourself from the means at hand;
4. can be used for various purposes: various civilian purposes; intelligence and counter-intelligence, military training or tactics (which is prohibited in many countries due to national law), espionage and harassment, active combat missions, terrorism;

[38] Smith. S. (2019) Military and Civilian Drone Use (UAV, UAS)
[39] Alston, P. (2011) "The CIA and Targeted Killings Beyond Borders". New York University Public Law and Legal Theory Working Papers. Paper 303, p 3.
[40] Casey-Maslen, S. (2012) supra nota 2, p 599.
[41] Jenks, C. (2009), supra nota 2, p 655.

5. there is no effective frontline, without difficulty it can be controlled up to 1000km away from the starting point.

The greatest example is the Reaper that is in use of U.S. military forces. Reaper is more than 10 times cheaper than modern combat aircrafts, but in terms of importance it is not inferior to them. This UAV is by and large a reconnaissance aircraft that collects data both on the battlefield and on land. Due to this, the US military was protected in its missions on the territory of Afghanistan, because they knew many important data about their opponents, in particular - their location and weapons. UAV broadcasts in real time, the battery lasts about 20 hours. [42]

In case with drones, it is a question of a single invention, which was misused. However, if it could be imagined as thousands of drones that work along to harm a certain target, facility or a state. For example, the United States has more than 10,000 drones in service. [43]Such attacks can be catastrophic. Moreover, without any breach of law and without causing direct harm, it is possible, for example, intercept or interfere with the transportation of resources, to disable certain objects (for instance, prevent medical transport from reaching the destination where wounded people should receive medical care). Hence, nuclear reactors, GPS routes, the location of various objects that have important value for the state - will be the first target for enemy defense forces. However, as in the case of a cyber-attack, important algorithms, important information about individuals or objects, can be intercepted using hacked or created drones.

In either event, such UAVs could be controlled by ordinary people without wearing the status of a military officer or officer. Anonymity in this case becomes a security vulnerability, both in the cyber industry and in the humanitarian law industry.

2.3 Autonomous weapon

Autonomous weapon system (AWS) – robotic vehicles that can attack or defend certain objects or targets without human intervention, which are able to make certain decisions on the basis of an artificial intelligence (AI) system.Autonomous weapons can become “weapons of

[42] Graham, D. The U.S. employment of unmanned aerial vehicles (UAVs): An abandonment of applicable international norms, Texas A&M law review, 2015, 2, p 678.
[43] Ibid. p 677.

intimidation", weapons that tyrants and terrorists can use against innocent people, weapons that can be hacked and made to work in undesirable ways. [44]

Initially, the first developments of artificial intelligence were in 1980 in the USA, the cause of which was the arms race between the USA and the Soviet Union, which began in 1945 due to the development of nuclear weapons.[45] Despite the fact that the race process was either stopped or resumed due to certain political reasons, the development of artificial intelligence is still an integral part of science, technological progress and politics. [46]

Nowadays, there are three types of autonomous weapon systems, evaluated by the criteria of autonomy:

1. Weapons with a system of complete autonomy. After activation, it is capable of choosing the target itself and engaging with the target completely independently of human control and management. Often equipped with a radar and electronic sensors. The goals may vary from either electronic or frequency communication tools (walkie-talkies, telephones) that an autonomous weapon could disable, or other physical objects, when detected on the radar of which the machine makes contact. This type of autonomous weapon system is the most problematic in the scope of IHL and this Thesis.
2. Controlled autonomous weapon system. This type allows human control to intervene in the system in the event of a potentially unacceptable level of damage or in the event of an autonomous weapon failure.

   As an example of this type of weapon, various protective anti-air systems for intercepting missiles can be presented. This type of weapon works independently, however, performing tasks based on how it is programmed.
3. Weapons with incomplete autonomy. When activated, it executes a given program for specific goals or groups of goals that the operator has selected. Such targets may be moving artillery or tanks that meet the characteristics specified by the program.[47]

[44] The Ethics of autonomous weapons systems, University of Pennsylvania Law School. www.law.upenn.edu/institutes/cerl/conferences/ethicsofweapons, 19 February 2020.
[45] Liu, H. (2012), supra nota 2, p 632.
[46] Leyen, U. (2019) A Union that strives for more. Political guidelines for the next European commission, 2019-2024. pp 1-22, p.13
[47] ICRC (2014) Autonomous weapon systems: Technical, military, legal and humanitarian aspects. Expert meeting, Geneva, Switzerland, 26 -28 March 2014, p. 14.

According to some reports, since the beginning of the twenty-first century, the United States has used autonomous weapons in more than 100,000 different missions in its operations in Iraq. However, the United States is not the only representative of users of AWS. More than forty other countries either bought this technology or developed similar programs for military purposes. A number of these countries include the USA, Israel, China, India, and South Korea.[48]

Why are autonomous weapons being of interest of the states?

Firstly, it is expected that the autonomous system of the armed forces would increase forces' power, expanse the battlefield, increase the radius of action of the other human-controlled vehicles, and it would increase the accuracy of reconnaissance and the acceleration of warfare actions. All this thanks to the ability to equip autonomous weapons with various sensory technologies. [49]

Secondly, in view of the fact that a machine, unlike a person, does not instinctively protect itself, for example, in case of contact with an unidentified army, where a person experiences stress and resort to extreme measures (blue on blue fire, harm to civilians), we can assume that a programmed machine is more likely to adhere to the rules of international humanitarian law than a person.[50] Thirdly, artificial intelligence lacks emotions and a psychological factor. In order to preserve the morale and mental state of the troops, a healthier option, of course, would be to use tools that military actions do not harm health, that is, autonomous weapons.[51] Fourth, the previously mentioned paragraph on content. For obvious reasons, it's cheaper to keep one multifunctional self-governing invention than the technique that is managed by a separately trained person. [52]

Sometimes, to complete one mission, more than 40 people are required (a whole group of soliders). Such use with a threat to human life seems irrational.

On the other hand, the operators of such systems are not able to give an accurate forecast on how an autonomous weapon will behave in a particular situation and when a system failure can occur.

[48] 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. 1028
[49] Ibid. p 1028
[50] Ibid. p 1029
[51] Ibid. p 1029
[52] Ibid. p 1029

Also, human panic, fear and other emotions have been studied for a long time and to predict how a person will behave in a particular situation is relatively simpler, since human psychology is based on certain models of behavior. With artificial intelligence, this is not the case. In view of the fact that artificial intelligence is a fairly new discovery, it is almost impossible to predict its behavior.[53]

In addition, the controversial issue is the recognition of the status of a fighter. New technologies, of course, see a lot and can broadcast and process, but the art of live battle does not stand still in development. For example, artificial intelligence sees the target on the radar, since the target holds an object in its hands in a silhouette resembling a weapon, and fixes it for further actions. In contrast, a person can recognize through intelligence that the target is a child who is holding a mock-up of a weapon made of plastic or other material, which does not pose any threat or potential violation of legal acts. [54]

Despite the danger to mankind this invention is, every year it improves and develops. Also, despite the fact that such inventions may be prohibited at the national legislative level in some states, it is actively developing, being used and it conducts economic turnover of these inventions.

[53] Ibid. p 1030.
[54] Ibid. p 1030.

3. LEGAL STATUS AND ANALYSIS OF ABOVE-MENTIONED TYPES, TOOLS AND WEAPONS OF WARFARE

3.1 Cyber Warfare

3.1.1 Status of cyber-attack

Nowadays, international law, which refers to armed conflict, is divided into two types: *jus ad bellum* and *jus in bello*. In the first case, armed conflicts are considered from the point of view of the state's behavior, as an instrument through which the state has the legal right to use force. This has been previously mentioned and is governed by the articles of the UN Charter. In the second case, *jus in bello* regulates by what methods and means the legal use of force should be applied. These two concepts, in other words, are International Humanitarian Law (jus in bello) and the Law of Armed Conflicts.

3.1.2 Cyber-attack and *jus ad bellum*

Jus ad bellum seeks to maintain relations between countries and therefore establishes strict rules and regulations regarding when states can exercise their right to use force, thereby going beyond diplomatic and economic relations.[55] As mentioned above, often, such actions can be used only when an act of aggression is used against the state and the state uses force as a defense and / or other states use force to protect it.

From the point of view of *jus ad bellum*, the concept of attack or the use of force, as such, has a very controversial meaning. First, article 2 (4) of the UN Charter mentions the word "use of force", however, has no defining descriptions.[56] It is likely that the law was promulgated in such a way as to have the widest possible range of applications and was flexible in terms of adapting to the new norms of aggression. Secondly, other articles of the appropriate Chapter mention "armed forces" in the literal sense, which is too narrow in understanding and excludes other

[55] Schmitt, M. (2012) "Attack" as a Term of Art in International Law: The Cyber Operations Context, IEEE. p 286
[56] See Article 2 (4) of UN Charter

possibilities of using force. [57]Thirdly, the use of force is illegal only if it is used for the political independence of another state.

Thus, in order to fall under the understanding of these articles, a cyber-attack must be sufficiently destroyed so that the state against which this attack is directed considers this an act of aggression and could defend itself in proportion to this. However, in the examples discussed above, cyber-attacks are mainly aimed at infrastructures and therefore do not bring enough destruction to use force as a self-defense or defense of a third state.

3.1.3 Cyber-attack and *jus in bello*

3.1.3.1 Distinction and Dual-use target attack.

As previously mentioned, the principle of distinction is an integral and fundamental principle in IHL. In the context of cyber warfare, this principle is rather contradictory, since the concept of a military and military object, as well as a civil and civilian object in the field of cyber space, differs from kinetic or physical.

For example, certain information inside a computer can carry a certain military significance, but an organized attack on this information cannot be classified as an attack as a whole, since many experts along with Tallinn Mannual believe that data is intangible and therefore outside of the scope of ordinary meaning of the term object. Thus, a cyber-operation aimed at destroying or manipulating data inside a computer or operating system, without prejudice to the functionality of this computer or operating system, is not an attack from the point of view of IHL and its principles.[58]

However, in any case, according to this principle, a cyber-attack should be applied only to a military object. For an object to become a military, it must in some way contribute to the military. Obviously, this notation is broad in understanding and can be interpreted in different ways. It is clear that kinetic military objects are such in nature and easy to distinguish from non-military, but there are also objects that contribute to the help of the military. In the context of cyber space, an object that supports the military or contributes to the military, for example, a factory for the production of certain operating systems for military purposes or the production of

[57] See Article 51 of UN Charter
[58] Pascucci, P.(2017) "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution". Minnesota Journal of International Law. 257, p 431.

instructions for using weapons - can also be considered as a military object and thus may be legitimate target for cyber-attack. [59]

In addition to this, it is important to understand that there are facilities that can be used for both civilian and military purposes, as well as military facilities that can be in close proximity to civilian facilities. Such objects may be the previously mentioned agricultural fields or water supply facilities, the damage of which through cyber-attacks is also possible, however, according to this principle, IHL is a war crime. Along with this, the production of atomic weapons can also be a military facility, as is the case with Stuxnet. However, assuming that a cyber-attack would not entail collecting data about the object, but would have a devastating effect, which could potentially damage the nuclear reactor, which would entail an explosion. In this case, most of the previously mentioned IHL principles would be violated, because such an attack would cause significant harm to both civilian objects and civilians, and the environment.[60]

Despite the fact that a cyber-attack is often aimed at exterminating or manipulating data, the effect of improper use of such an attack can be different and cause different consequences, which may not always be a violation of IHL and international law. In this regard, the person responsible for the cyber-attack must take into account the consequences in accordance with the principle of distinction, even if this person is a military man and makes an attack for military purposes.[61]

3.1.3.2 Principle of proportionality

It is very difficult to talk about this principle within the context of cyber war, in view of the existing gap in the law regarding data manipulation. As previously mentioned, in order for an attack to be seen as an act of violence or aggression, it must do enough harm, often this harm must be physical in nature. In view of this, a difficulty arises in determining the attack as a whole and its proportionality. The main objective of International Humanitarian Law is to preserve the life of civilians and its protection, the same principle is to limit the potential harm to civilians during military operations, through a more reasonable and prudent use of measures of warfare. However, for example, if we hypothetically compare one physical or kinetic attack, as a result of which 4 civilian and cyber-attacks were injured, as a result of which, due to data destruction, tens

[59] Ibid. p 432.
[60] Ibid. p 433
[61] Schmitt, M. (2012), supra nota 2, p 290

of thousands of medical histories of civilians disappeared without a trace, then the first is a violation of international military law and last does not constitute a violation. [62]

In the case of the kinetic vision of war, there is some understanding of which attack is proportionate and which is beyond the scope, while in the case of cyber spaces such a standard does not exist. It is obvious that the destruction of a military nuclear reactor, the explosion of which will cause enormous harm to the civilian population, or direct damage to civilian health by destroying the water supply through a cyber-attack will violate the principle of proportionality, but the expected result in obtaining military superiority will not always be potentially aimed at such objects.[63]

In addition to this, according to this principle, civilians and facilities should enjoy the protection of the armed forces of their state. Despite the fact that IHL perfectly regulates the protection of civilians from physical violence or manifestations of aggression, due to the ambiguity of the concept of "attack" as such, the principle loses its strength precisely in cyber space, since it is impossible to defend and protect others if there is no act of aggression or violence.[64]

3.2 Legal analysis of Drones and Autonomous Weapon

3.2.1 Legal basis for the Use of Force

Currently, according to UN Charter article 2 (4) "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state".[65] However, Articles 39-42 and 51 create two exceptions to the use of force. In the first case, according to article 41, the opportunity of use of force arises when there is a threat to peace, a violation of the peace, or aggression by another state. In the second case, according to article 51 of this law, it allows the use of force as: a method of individual or collective self-defense, in the case of the use of armed conflicts or actions. Thus, there are only two legitimate uses of force in armed conflicts, and both from a defense perspective. [66] In the case of the

[62] Pascucci, P.(2017), supra nota, p 432
[63] Ibid. p 433
[64] Schmitt, M. (2012), Supra nota 3, p 291
[65] See Article 2 (4) of UN Charter
[66] See Articles 39-51 of UN Charter

legitimate use of force, the principle of proportionality and the principle of necessity must be respected. [67]

Despite the fact that not all states have accepted and ratified this agreement, the member states of this agreement must behave and treat in the same manner with those states that have not ratified.

Single use of UAV may not pose any threat or violation of international law. However, if UAV and AWS are used for attack purposes, then such an attack can be interpreted as an "armed attack", after which the state that activated the UAV or AWS will be forced to justify its actions by referring to self-defense, so that the attack is not considered as an act of aggression in relation to another state. This point is controversial. Measures and criteria for the concept of self-defense apply to cases in which two separate states participate, where one behaves as an aggressor. However, what if the actions of self-defense are considered from the perspective of collective self-defense, in which case the first state intervenes, for example, in an act of terrorism by a person or organization that is a representative of a third state while in the second state. Such cases require special caution in the analysis of each individual situation, because any erroneous action can unleash a war between two states. [68]

3.2.2 Status of Combatant operating AWS or UAV.

One of the main issues regarding the problematic is the status of UAV and AWS operators. According to the distinction principle described below, combatant must have distinctive signs on the battlefield so as not to be wounded or killed by friendly troops. [69]The problem is that AWS and UAV statements are not uniform. These may be exclusively civilians involved in military operations for a short or long term. Nowadays, not every person who can be burdened with military status has a distinctive uniform and at the same time performs military tasks, also, most people with military status do not wear a uniform in non-wartime and wear it only at the time of mobilization, however, they can interact with civilians. By the way, even such people can carry the status of the goal, although the form and distinctive features are absent. In the case of AWS

[67] See ICRC Rule 14 of CIHL
[68] Casey-Maslen, S. (2012) supra nota 3, p 604
[69] See Articles 37-40 of AP I

and UAV, wearing certain outfit as a criteria of distinction are not of significant importance, since the location of such a system may be thousands of kilometers from the one who controls it.

Often, in armed conflicts, soldiers carry out orders rather than acting on the basis of their will and initiative. The drone operator is no exception. Operator - the person carrying out the order. The status of the operator depends on what order he will have to follow. If the *jus ad bellum* rules are followed by the person giving the order, then the operator controlling the weapon is a civilian who takes direct part in hostilities and has the status of a soldier with his list of rights. However, if the *jus ad bellum* rules are not followed, then such an operator may be the target for attacks at any time and not have the privileges and rights of a soldier in case of such attacks.[70]

3.2.3 The Principle of Distinction between Civilians and Combatants.

One of the most important principles of international humanitarian law is to secure in every way those who are not participating or are no longer directly involved in hostilities. [71]
According to the Interpretive Guidance from ICRC, only those who are directly involved in hostilities on a spontaneous and disorganized basis should be considered a target, but only for the actual time when they are involved in it. Those who carry out political or administrative tasks cannot be the target for an attack until they are directly involved in hostilities. Thus, civilians, operating AWS or UAV in whole or in part, may lose their status of civilian protection, as they conduct direct actions and take part in hostilities.[72] It is worth to consider the above example, where the target for the killing is one person, presumably a terrorist. In the event of an international armed conflict, there is ambiguity, since the target is civil in nature and falls under the protection of international law until the criteria of the combatant is met. However, in non-international armed conflicts, members of organized armed groups with a certain status of "continuous combat function" are the target to be constantly attacked.[73] At at the same time, the AWS operator can simply be the designer of this system and be involved in the process only at the click of a button, or activation, which is not a continuous combat function.

As mentioned earlier, weapons are equipped with sensors and are often devoid of human control. Based on the algorithms, the weapon makes a decision. However, whether there is a guarantee

[70] Lewis, M. & Crawford, E. (2013) Drones and Distinction: How IHL Encouraged the Rise of Drones, p
[71] Asaro, P. (2012) On banning autonomous weapon systems: human rights, automation, and the dehumanization of lethal decision-making. International Review of the Red Cross, 94, pp 697
[72] See ICRC Rule 6 of CIHL
[73] Liu, H. (2012), supra nota 3, p 645

that the decision made by these means will be in accordance with international humanitarian law remains an issue. It could be assumed that UAV and AWS would be capable of scanning faces thanks to high-precision sensors, however, often, speaking about soldiers, especially reconnaissance groups, such data is not available in the databases. Also, due to the fact that the personal data of each person is protected by national law, in order to obtain such data about a person in another state, there would be a need to penetrate or hack into the database of the government of another state, which is a priori a violation of the law and could be counted as an act of aggression against to the state.

Recently, most of armed conflicts are not-international, often there is no clear front line and military facilities may be in close proximity to civilian facilities. Along with this, participants in hostilities often cannot always adequately assess who is the enemy or civilian in a given situation. Due to the fact that it is still not completely clear how well recognition systems work with remote armed systems, in particular AWS and UAV, the level of civilian protection is weakening. [74]

3.2.4 *Hors de combat* and perfidy

According to Article 41 of Additional Protocol 1 (Customary IHL rule 47), it is forbidden to attack a person of an enemy party who expresses a desire to surrender; disarmed or wounded and has no ability to continue to fight. [75]This principle is fundamental in international humanitarian law.

The Challenge of the *hors de combat* is whether the UAV or AWS can recognize the surrendering enemy and act along with the principle of humanity.[76]

As already discussed earlier, recognition systems are far from being ideal and are themselves not trustworthy in the subject of military affairs. If such systems could distinguish a military object from a civilian object, then there is no certain guarantee that the systems would also be able to distinguish between military objects that have lost their combatant status by, for example, being injured. Also, despite the fact that Article 37 of Additional Protocol 1 prohibits perfidy, there is no guarantee that, firstly, the opponent would strictly follow and stick to the guidelines of

[74] Casey-Maslen, S. (2012), supra nota 4, p 609
[75] See Article 41 of AP I
[76] Liu, H. (2012), supra nota 3, p 643

International Humanitarian Law, and secondly, AWS and UAV would be able to recognize and / or prevent such war crimes.[77]

3.2.5 The principle of proportionality.

The principle of proportionality in the use of force for attack is one of the main principles of *jus in bello*, it is also the rule number 14 of customary IHL, which is described in 51 (5) (b) of Additional Protocol I. It prohibits launching an attack that may incidentally entail death of a civilian, causing damage to a civilian or civilian object, or a combination that would lead to excessive military advantage.[78]

The principle of proportionality is a balance between military advantage and civilian harm. The attack is proportionate if the attacker correctly assessed the military advantage and the expected damage to the civilian, where the damage did not exceed expectations. To this day, disputes are ongoing regarding the proportionately used weapons, both in the case of *jus ad bellum* and *in jus in bello*. Often, this issue requires human judgment and decision-making for each individual case. It is hard to imagine that AWS or UAV are capable of making judgment and consequently make the right decision.[79]

For example, on the basis the previously mentioned scenario, where the target is a civilian person or group who is aimed to do terrorist acts. Alleged terrorist groups or individuals are often located in civilian facilities and mixed within the civilian population. There is a risk that, due to their illegibility in choosing a goal, civilians may suffer. Looking from this perspective, the legality of the use of remotely controlled weapons is in doubt, because the principle of proportionality is not fulfilled. In this particular case, it would be proportional to use a specially trained group of people in order to neutralize a potential terrorist target. [80]

Also, certain types of AWS and UAV are programmed to destroy specific objects, such as trucks that transport resources or other objects and property. In this matter, the inside of the truck container may become a target, however, destroying the given object may damage civilians who transport this cargo. [81]

[77] See Article 37 of AP I
[78] ICRC Rule 14 of CIHL
[79] Casey-Maslen, S. (2012), supra nota 5, p 612
[80] Ibid. p 612
[81] Ibid. p 613

4. STATE AND INDIVIDUAL RESPONSIBILITY

In international law, states are responsible for actions that people or organizations have committed on behalf of the state or with the approval of the state. These individuals or organizations include not only government agencies, such as the police or the army, but also private military companies or people who maintain order, being on a contract from private firms. In the case of armed conflicts, regardless of where the operations take place and where the consequences of these operations appear, the state is responsible. In addition to this, assistance to other states in operations that violate the principles of international humanitarian law and the principles of human rights also holds the assisting state accountable. For example, if a state intends to carry out an attack using a drone, and it is known that the consequences of this attack would entail a violation of international agreements, military assistance to that state, for example, intelligence or logistics, would also be considered as a violation of international law and a state that helps committing a war crime would be held accountable. In the case of serious violations of law, such military support could bring not only the assisting state to justice, but also individual criminal responsibility. [82]

Speaking about responsibility for using drones, the most important issue remains the controversial status of the operator. If you look at this issue from the angle of International Humanitarian Law, in particular the Hague Regulation 1907[83] and the Geneva Convention III[84], the operator's status will hardly be given combatant status. According to the IHL and CIHL, the status of a combatant is given to persons who are under command, or follow the orders of the commander; have a specific distinguishing mark or emblem or wear the uniform; carry arms openly and fight in accordance to the rules of war. These criteria apply not only to the armed forces of a state member of the conventions, but also to volunteer or rebel movements. In order for the observance of the criteria to be significantly important, this should be applied only to the kinetic method of warfare, otherwise the question of responsibility is very controversial. Despite the fact that the drone operators do not wear uniforms or other recognizable signs and are not always on the battlefield, they control the weapon in one way or another (if the drone has the ability of targeted killing), while fulfilling the command of the person responsible for the order. As mentioned earlier, the drone operator must in one way or another take into account the

[82] Melzer, N. (2013) Human rights implications of the usage of drones and unmanned robots in warfare p38.
[83] Article 1 of Hague Regulation 1907
[84] Article 4 of Geneva Convention III

fundamental principles of International Humanitarian Law, such as the principle of Proportionality and Caution in Attack and the principle of distinguishing the military from the civilian. Thus, persons controlling drones are no different from those who operate any other air vehicle while performing military tasks. For example, helicopters are often equipped with machine gun and missile calculations, which requires the opeator to use this weapon in accordance with the rules of international humanitarian law. It follows that the person managing the drone, like the command post, is responsible for violations created by the use of drones. [85]

In addition to this, the complexity of complying with international military standards is created by intelligence and intelligence operations. The difficulty is that the responsibility for using drones remains unclear when UAVs are used by intelligence. The ambiguity is created by the fact that, for example, in the USA, firstly, intelligence can use tools and programs that are neither of military purposes nor used by the US armed forces. Secondly, intelligence does not wear a distinctive uniform and does not carry weapons openly. Thirdly, despite the fact that intelligence carries out certain orders and is under command, the command post is not always military in nature. According to the IHL, intelligence does not fall under the status of a regular combatant. This type of person is explained in the IHL as an "Illegal Combatant" or „unprivileged belligerent" whose status is still controversial. Some believe that this type of fighter bears the status of a combatant only when they take part in hostilities, but if captured, they have protection with civilian status under the IHL. Others believe that these fighters are not entitled to protection by the IHL and may be the target at any time, regardless of whether they are executing orders from a military command post or straining from the state. However, regardless of the status of persons of this type, the ICRC has a clear definition of the responsibility of a person or group that has "a continuous combat function." In the case of a prolonged combat function, a person can be the target of attacks at any time and in any place where they can be found.[86]

When states and their amed forces use autonomous weapons systems, the issue of human responsibility is in great doubt. Any offense consists of two parts: a criminal act and its mental state.[87] Crimes committed by humans often have both of these parts. Speaking of autonomous weapons, he does not have a living mind, and therefore there is no mental position. As discussed earlier, autonomous weapons may have a system malfunction, which could pose a threat to civilians or the environment. In addition to this, weapons that are beyond human control can

[85] Sehrawat, V. (2017), Legal Status of Drones Under LOAC and International Law, 5 PENN. ST. J.L. & INT'L AFF. 164. p. 202.
[86] Ibid. p. 203.
[87] See Rome Statute Article 30.

commit crimes based on their algorithms and independent decisions based on programming. Could such a machine be responsible for the violation, or could there be liability for such weapons in the form of punishment? The answer is obvious, if the weapon does not satisfy the requirements of the offense, then such a weapon cannot be held responsible for its illegal actions.

Thus, three types of persons can be responsible for violating international law: manufacturers, IT specialists or programmers and states that use autonomous weapons or commanders who act on behalf of states in their operations. [88]

Firstly, it is worth dealing with manufacturers. The manufacturer is responsible for his product and for the potential harm or damage that this product may cause. What is the difficulty? First of all, the jurisdiction of the court in relation to the manufacturer. Since this case is related to the use of the civil code, in some proceedings the civil courts of some states do not have jurisdiction over violations created in other states or to persons located in other states. Thus, it is difficult to sue the manufacturer of one state that supplied autonomous weapons to another state when damage occurred during the operation in the third state. The financial component, among other things, creates the complexity of such a court case. Since damage can occur in countries with weak economies, initiating such cases against economically developed countries is financially disproportionate. [89]

Secondly, the responsibility of the person who programs or activates this type of weapon is also in doubt. The catch is that after activation, an autonomous weapon acts independently, without human intervention and no matter what commands it should carry out. Suppose a weapon is programmed to undermine a specific military object, but at a certain time near this object there is a high probability of a threat to the civilian population or objects. The command post command was given to eliminate enemy forces and destroy an important enemy object, but the action by autonomous weapons may be different. It is controversial to argue that the person who gave the command to destroy the military facility is responsible for the independent decision of the autonomous weapon to endanger or for causing harm to civilians. The difficulty lies in finding the person clearly responsible for the crime, since most people are involved in the development and use. Some do programming, others test and still others activate or partially control. It is also difficult to prove the involvement of one particular person for a specific violation. A large number of people are involved in the programming process, where everyone is responsible for a

[88] Cass, K. Supra note 2, p. 1049
[89] Ibid. p. 1050.

small part of the whole work. Thus, it can be argued that in reality a person activating an autonomous weapon is only responsible for his actions when he directly intends to commit a crime, for example, to harm the civilian population. In the case of the programmer, it is difficult to identify whose "piece of work" entailed the offense. [90]

Thirdly, in international criminal law, there is also the concept of command responsibility. The main idea of this responsibility is that the person who issues the order is responsible for the violation if it could not prevent or punish the person committing the crime. If we consider an autonomous weapon as an object executing orders, in the absence of *actus reus* and *mens rea* [91] there is also no existence of the crime in general. Thus, a crime committed by an autonomous weapon cannot be a crime for which a command post would be held accountable. In addition to this, the command post should be aware of the actions of its subordinates in order to know whether all orders are executed in the correct order.[92] When a fully autonomous weapon is used, the command post cannot always assume and certainly know with certainty what actions it will take. A risk assessment by the command post may also not be adequate. For example, when the subordinates of a particular command post had previously committed a crime, then the command post is aware and in similar situations can foresee one or another denouement of the scenario, while in the case of autonomous weapons it is impossible to predict behavior due to the lack of a mental component. Thus, it is impossible to say with accuracy that the previous crimes of one particular robot are a mistake in the development of one particular robot or an entire manufacturing batch. Also, it is impossible to determine whether autonomous weapons, which in the past put civilians at risk, cannot do this in the future. Depending on what information the command post possesses, it can and should take certain measures to prevent crime, but this is not possible in the case of using autonomous weapons. Thus, if the command point possesses such information, then the principle of punishment or prevention is not possible, since prevention is a controversial point, and punishment, as previously discussed, is impossible. From which it follows that any crime committed by a fully autonomous weapon, where the command post does not have control, in case of information or control weapons, the command post is not liable.[93] On the other hand, according to article 28 (a) (i) of Rome Statute, if the commander or command post knew about a potential violation or could have known about the violation and did not take

[90] Ibid. p. 1052.
[91] See Article 30 Rome Statute.
[92] Human Right Watch (2015) Mind the Gap. The Lack of Accountability for Killer Robots. Accessible at: https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots#695b43. 7 May 2020
[93] Ibid.

any possible preventive measures, then the commander who issued such an order is responsible for the crime.[94]

Speaking of cyber warfare, cyber space is often built around anonymity. According to ICRC, identifying a person who is responsible for a cyber-attack is either very difficult or impossible in some cases, so the suitability of IHL in such operations is questionable. Despite this, in cases where the damage and damage resulting from a cyber-attack is obvious and clear, the aforementioned liability analysis can also be applied in accordance with IHL.

However, despite the fact that in some cases it is not possible to establish individual liability for the offense the state is in any case liable for such offenses. In the event of force majeure, states must also reckon with the norms and principles of international law.[95]

There are different types of bodies that provide investigations and detect criminals of international law and international humanitarian law, including. First of all, there are national courts, since states must provide penalties for individual criminal responsibility. Also, there are international tribunals that also deal with criminals. The last and the newest instance is the International Criminal Court, which helps states dealing with criminals in cases where the states do not have such ability to deal with itself. [96]

[94] Ibid.
[95] Melzer, N. (2013) Supra note 2. p.39
[96] Henckaerts, J-M (2005). et al. Customary international law, volume I, Rules. Cambridge, Cambridge University Press. p.610

5. Proposals to the legal problems

Speaking about how the analyzed methods of warfare are regulated by law now and should be resolved in the future, it is impossible to come to an unequivocal opinion. Many experts around the world, solving this issue, arrange debates about how and why this or that aspect should be settled when using the above methods of warfare, and in the end do not come to one unanimous opinion.

Speaking about the use of drones, the picture and idea of how this issue is regulated is quite clear, although it has its weaknesses. The main issues and problematic areas of use of this weapon are effectively covered by the norms of International Humanitarian Law and by rules of Customary IHL, such as "indiscriminate attack", "principle of proportionality in attack", "principle of distinction" and others. D.R. Brunstetter and A. Jimenez-Bacardi, in their study, believe that using fewer drones as weapons will not lead to a significant improvement in human rights. While the solution to this problem, experts see that if a decision were made to change the regulatory framework in addition to the idea of the right to life, to embrace a life free from fear of an unmanned "strike from nowhere", this could initiate a shift in international law, which would mitigate some, though not all, of the dangers that drones pose to human rights during acts of aggression and terrorism. [97]At the same time, other experts are generally worried by the policy of article 36 of Additional Protocol I on the creation of a new weapon, which in the interpretation of many may become "less lethal" in the context of warfare, since the words "it is better to be wounded than killed" are hidden in many international discussions. [98]

In addition, the legal status of the UAV operator as a combatant remains the biggest problem, since the interpretation of Article 4 (A) (2) of Geneva Convention III, Article 1 of The Hague Regulation 1907 and other Regulations and National Law Manuals (Practice Relating to Rule 4. Definition of Armed Forces), does not give a clear definition as to which criteria must be met by the person or group of people who control the drone. It is in view of this ambiguity that states begin to interpret legislation in their own way or use it in their own interests and for their own benefit, observing the minimum requirements. An example of such behavior in its covert intelligence operations can be the United States, where undocumented actions raise doubts and

[97] Brunstetter, D. R., Jimenez-Bacardi, A. (2015) Clashing over drones: the legal and normative gap between the United States and the human rights community The International Journal of Human Rights, 2015 Vol. 19, No. 2, 176–198, p. 198

[98] Jacobsson, M. (2016) Modern Weaponry and Warfare: The Application of Article 36 of Additional Protocol I by Governments. International Law Studies, Volume 82. p 189

distrust of other countries.[99] Thus, the author believes that despite the fact that International Humanitarian Law answers quite clearly the questions of the legality of using drones as methods of warfare, some aspects, such as the status of an operator, should be studied from an angle of modern time with a wider number of people and specialists in various fields, for example, scientists, programmers, production specialists and other irreplaceable specialists in the field of regulation. In addition to this, it is important to ensure the education of drone manufacturers for military purposes at an appropriate level so that international law can be observed by persons using drones, both at the individual level and at the level of those who give orders to use. Also, you should specifically train people who directly control drones, since even the slightest mistake or oversight in pressing the "wrong button" can be considered an act of aggression, which subsequently can lead the state to responsibility to pay compensation at minimum, and at maximum to be considered as an act of aggression which could lead to a war between countries.

Moving on to the next subject, it is important to say that there are much more disputes and debates regarding legalization or the ban on the use of autonomous weapons. In view of the fact that autonomous systems affect a huge part of the legal structure, ranging from human rights, legal and military ethics, international law, principles of humanity in law, criminal law and much more, it seems impossible for an author to come to one clear opinion unanimously for all countries. Despite the fact that the most common belief among experts is that autonomous weapons should be prohibited by law, some believe that the ban is meaningless and ethically controversial, since they consider autonomous weapons to be part of technology development that cannot be influenced by a conventional ban, then how it is the other way around to direct forces to make this weapon the most acceptable to use. Also, experts advocating the legalization of autonomous weapons firmly believe that autonomous weapons have humanitarian superiority in view of their accuracy. Despite possible violations when using this weapon, it is not mentioned that this development needs to be used, however, it can be developed. Therefore, a ban does not make sense. [100] In addition to this, one cannot deny the fact that from the point of view of the public ban does not make sense at present. Often, weapons were criticized by the public only after their use. Due to the fact that autonomous weapon systems have been used extremely rarely at the moment, relative to classical weapons, it is impossible to conduct a clear analysis of autonomous weapons from the point of view of humanity. The fact of what effect this weapon can cause is still unknown. Also, there is no guarantee that after the ban states will not

[99] Graham, D. Supra note 2, p. 679
[100] Asaro P. Citing K. Anderson and M. C. Waxman.

continue to develop this technology in secret from others. Naturally, only the states that used it will know about the effect and the real possibilities of autonomous weapons, autonomous or semi-autonomous.[101] Asaro, in his turn, is quite conservative in his favor of banning AWS, because, with given the characteristics and potential of autonomous weapons abovementioned in this paper, they are not able to satisfy the requirements of International Humanitarian Law, such as the principle of proportionality and the principle of distinction, thus autonomous systems cannot be used as weapons.[102]

Despite the differences, experts believe that the only thing that needs to be focused on in this matter is the establishment of rules that would govern both the development and use of autonomous systems. An important part of regulating this issue is the desire for research and practice on the part of states, which will help establish a limit on what is legal in use and what is not. Thanks to this, states will better understand the nature of what is allowed. In addition to this, the settlement of this issue will help put the state on one level before the law. Such legal challenges encourage states to negotiate, which help to avoid ambiguities in the interpretation of the law and help to bridge those gaps in the law that remain unclear. As ordering, there may be amendments to this law (Certain Conventional Weapons) or separate independent agreements, similar to the Chemical Weapon Convention. In addition to this, states couldn, through negotiation or the creation of nonbinding declarations, create informal laws or guidelines on how to produce, how and who should be trained, how to use and what should be taken into account.[103] Cass is of the similar opinion on a question how should AWS be regulated. Such an approach, according to the author, will help states better study the nature of autonomous systems before it is widely used on the battlefield, which could potentially lead to the general opinion that this system should not be available for use. The author also believes that existing autonomous weapons systems that are protective in nature are a great example of how such systems should be used in a useful sense.

Analyzing cyber-attacks, according to Schmitt, the main legal ambiguity is the interpretation of an “attack” and “armed forces”. Without a clear presentation of such definitions, the use of IHL in the field of cyber war is in doubt. Also, since kinetic attacks have a clear effect where civilians can suffer, receive damage, or be killed, according to IHL, civilians are protected. Whereas, in comparison with a kinetic attack, a cyber-attack may not really be considered an attack in

[101] Crootof, R. (2014) The killer robots are here: legal and policy implications Midyear Meeting p.1891
[102] Asaro, P. Supra note 2, p. 787
[103] Crootof, R. Supra note 2. p. 1901

general, civilians may be at risk. Also, humanitarian law and the civilian population may be threatened due to the controversial status of a combatant, where there is non-compliance with strict rules on the participation of civilians in hostilities.[104] In addition, according to the Oxford Internet Institute, sources of law such as the UN Charter, NATO Treaty, Geneva Conventions and Additional Protocols, Certain Conventional Weapon Treaty are a significant source for regulating cyber-attacks, but all of these sources are lacking. one document in which all these main principles and articles could work together for one purpose. The problem lies precisely in an unclear interpretation, which, as discussed above, states can use to their advantage.[105]

Some analysts believe that even assuming that there is a single document or treaty that controls the use of cyber-attacks as a weapon, states will still use them for several reasons: attributing responsibility for cyber-attacks is difficult; cyber warfare regulations cannot at all times be enforced; most of cyber-attacks are unreported; the costs of cyber warfare is minimal; cyber warfare can be used to coerce superior military forces into asymmetric warfare and finally attacking a states 'critical infrastructures destroys the victim states' internal operational viability. Thus, if it was now the assumption that there is a separate agreement, in reality, because of the points set forth above, not every state would want to sign such an agreement, since its absence can give a great advantage over the enemy state.[106]

Thus, some experts believe that in order to strengthen the law and fill in the gaps in the legislation, the following states should expand the scope of domestic law. Domestic criminal law cannot independently regulate cyber-attacks, because not all cyber-attacks are defined as cyber-crimes. But many cyber-attacks, including those involving non-state actors, are also cyber-crimes that fall within the scope of domestic criminal law. Further, states should begin developing policies that define the types of countermeasures that are legally and strategically appropriate for cyber-attacks.[107] Therefore, it would be worthwhile for states, through negotiations, to adopt clear and adequate definitions of "cyber-attacks" and "cyber-crimes" in order to know exactly when such an "attack" could be considered in terms of a sufficient attack for the right to self-defense and to know when a cyber-attack falls under the section of International Humanitarian

[104] Schmitt N.M (2002). Wired warfare: Computer network attack and jus in bello. Vol. 84 No 846, p. 396.
[105] Oxford Internet Institute (2015) Should we use old or new rules to regulate warfare in the information age? Accessible at: https://www.oii.ox.ac.uk/blog/should-we-use-old-or-new-rules-to-regulate-warfare-in-the-information-age/. 9 May 2020
[106] Garrie, D. B. (2012) Cyber Warfare, What Are The Rules? Journal of Law & Cyber Warfare. Volume 1. p. 150.
[107] Ibid. p. 151.

Law. For this, states require cooperation in the field and negotiations.[108] As a model example, in the understanding of the author, the document that states should adhere to on the issue of cyber war is Tallinn Manual, which describes the application of IHL standards and explains key ambiguities of international agreements.

In conclusion, the author believes that states, in order to avoid ambiguities in the law, should contact the competent international authorities whose answers would have a binding effect for all other states. Also, when considering the issue of new weapons, the development of which is not prohibited, such a body as the ICRC, for example, could keep documented statistics consisting of mandatory reports from other states that would be public and possible to read and guide other states. Thus, without any need for constant and continuous negotiations, states could independently develop in view of their capabilities and help other states in the same way if they have a desire to receive help in the form of leadership. In described case, all states have equal responsibility before the law and the competent authorities, as well as equal opportunities, and not equality of results.

[108] Hathaway, O. A., Crootof, R (2012) The Law of Cyber-Attack. California Law Review. Vol. 100:817 pp. 819-884. p. 880

CONCLUSION

Since the aim of this work was to study cyber weapons and how international law, in particular humanitarian law, can regulate various aspects of its creation and use, the author was able to find relatively outdated norms in which there are a large number of gaps and ambiguities. In general, international law partially covers the field of cyber weapons, and the example of Tallinn Manual shows how it can be applied. The current norms of International Humanitarian Law are naturally more focused on the settlement of the kinetic method of warfare, however, despite the fact that the cyber weapons studied above are not kinetic, therefore, the classical method of warfare, the interpretation of the IHL may also include a non-kinetic method. Thanks to the analysis, the author was able to answer the main research question

Drones have a huge number of advantages. UAVs have their advantages in civilian use, in military affairs and also by law. For the military, the use of drones reduces the cost of weapons and increases the functionality of the armed forces of different states. Also, since drones are used remotely, the risk that troops will fire on their own is reduced. In addition, equipping drones with various equipment partially replaces the need to use a human resource, as in the case of reconnaissance, where it is more expedient to collect the necessary data by remotely controlling such a tool, observing the desired picture through sensors and cameras. Due to such properties, as you know, cameras of our time allow us to see objects in phenomenal quality, the risk of targeting wrong or dangerous object that by its nature are civilian objects is also reduced. Speaking of drones from a legal point of view, the principle of distinction and proportionality, same as indiscriminate attack principle of IHL, can be achieved if a person using the drone for military purposes is well trained in this industry. As analysis and practice have shown, along with public opinion, the non-lethal use of drones is, firstly, regulated both at the level of national law and international law, and secondly, does not violate the basic principles of IHL. Despite the fact that lethal use of drones is also possible and not prohibited by law, as is the case with targeted killing, the fundamental principles must be taken into account. Speaking about how states can or will use this development, it is also important to mention that any ambiguity or a gap in legal norms can be used by the state for their own benefit. Using the example of how The Hague Regulation 1907 in Article 1 describes the criteria for the status of a combatant, which was later adopted by the CIHL and Geneva Convention 3, one may see what states can interpret in their own way until this ambiguity is corrected. The author believes that in order for the status of the combatant to become clearer, the criteria should be updated, since they are excellent, but

more likely, suitable for the kinetic methods of warfare. In addition, states should clearly describe the provisions of the contract when hiring workers for UAV operator positions. Presumably, drone operators should also wear uniforms or identification marks and work from military headquarters and buildings, carrying out military orders at the command post, as the signalmen do.

According to the author, the biggest challenge for international law is the regulation of autonomous weapons. Naturally, as in the case of drones, the use of this type of weapon for military purposes is a huge technological breakthrough and has a large number of advantages. In those moments when human resources can usually be depleted, robotic equipment does not get tired on the battlefield and can function much longer, while consuming much less energy and economic resources. Also, thanks to sensors, autonomous weapons on their own can very quickly make decisions, the potential fidelity of which to this day is a mystery and the subject of numerous disputes. However, from a legal point of view, it is doubtful that weapons with an unclear probability can act in accordance with the law and fundamental principles of warfare. In addition, if in the case of drones, it is relatively easy to establish the person responsible for the offending order or action, then in the case of an autonomous weapon system, in many cases this may simply be impossible. Despite the fact that Article 36 of Additional Protocol I allows states to invent and use new weapons under the law and there is no other agreement or decree that would regulate the use of specifically autonomous weapons, states should test and improve this type of development as long as it is likely successful use will not be close to existing weapons that are already permitted. As analysis has shown, a ban on this development may have a dubious effect or not have it at all. Consequently, it is in the common interest of states, and rather in a forced manner, it is reasonable to have a third-party documented database describing successful and unsuccessful attempts and stages of development and use of autonomous weapons. Such a thorough study of such a new weapon would allow the law to develop and limit the specific sector of the use of this weapon, instead of its complete ban, since its useful properties cannot be denied.

The use of the Internet in our days is an integral part of life and an area without which life could not be imagined. Talking about the advantages of using the Internet for civilian and peaceful purposes does not make sense. From the point of view of military affairs, Internet operations are also gradually being introduced into the military structure and, as shown by the analysis, they can be used in good intentions, for example, in the case of cyber intelligence operations, to detect potential offenses of certain states or organizations. Naturally, any military interest in the

development poses a potential risk to the threat to civilians, which is why there is international humanitarian law. Using the example of Tallinn Manual, we can say that the cyber structure in military cyber operations is well covered by the principles of International Humanitarian Law. However, this manual is not legally binding and, as analysis of this work has shown, not all states have a desire to apply these principles in their national law. The author believes that the creation of one universal document, which would be created by the appropriate number of specialists of different structures, would help to regulate the Internet as a weapon. Such a document could contain information unclear today and the conditions under which an "attack" in a cyber-context would constitute a violation of military law; information when states can legally use a cyber-attack in means of use of force; information on criminal liability, both of individuals and states, and what measures states can take against whom the attack was committed in the context of a cyber-war.

Thus, now is the best time to review, take into account the debates of various specialists, and update outdated legislation. Despite the fact that laws were still written after the effect of their use, which was further widely criticized by public opinion, in order to ensure universal security, it is worth thinking about many things in advance, including the settlement of new types of weapons in order to avoid possible catastrophic consequences for humanity as it is "better to be safe than sorry".

LIST OF REFERENCES

Books:

1. Schmitt, M., (2013), Tallinn Manual on The International Law Applicable to Cyber Warfare. Cambridge University Press

2. Schmitt, M., (2017), Tallinn Manual 2.0 on The International Law Applicable to Cyber Warfare. Cambridge University Press

Articles:

3. Alston, P. (2011) "The CIA and Targeted Killings Beyond Borders". New York University Public Law and Legal Theory Working Papers. Paper 303. pp. 1-117.

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

5. Benatar M. (2009), 'The Use of Cyber Force: Need for Legal Justification?', 1 Goettingen Journal of International Law, pp. 375–394.

6. Brunstetter, D. R., Jimenez-Bacardi, A. (2015) Clashing over drones: the legal and normative gap between the United States and the human rights community The International Journal of Human Rights, 2015 Vol. 19, No. 2, pp. 176–198.

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

8. 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.

9. Crootof, R. (2014) The killer robots are here: legal and policy implications Midyear Meeting. pp 1843-1915 Liu, H. Categorization and legality of autonomous and remote weapons systems. International Review of the Red Cross, 2012, 94 (886). pp 627-652.

10. Floridi. L., Taddeo. M. (2014) The Ethics of Information Warfare: Analyzing Information Warfare. Volume no. 14. London: Springer Science & Business Media. pp. 1-12.

11. Garrie, D. B. (2012) Cyber Warfare, What Are The Rules? Journal of Law & Cyber Warfare. Volume 1. pp. 1-216.

12. 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 677-693.

13. Hathaway, O. A., Crootof, R (2012) The Law of Cyber-Attack. California Law Review. Vol. 100:817 pp. 819-884.

14. Henckaerts, J-M (2005). et al. Customary international law, volume I, Rules. Cambridge, Cambridge University Press. p.610-623.

15. ICRC (2014) Autonomous weapon systems: Technical, military, legal and humanitarian aspects. Expert meeting, Geneva, Switzerland, 26 -28 March 2014, pp 1-28

16. Jacobsson, M. (2016) Modern Weaponry and Warfare: The Application of Article 36 of Additional Protocol I by Governments. International Law Studies, Volume 82. p 184-191.

17. 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 652-670.

18. Lewis, M. & Crawford, E. (2013) Drones and Distinction: How IHL Encouraged the Rise of Drones, p 1-47.

19. Leyen, U. (2019) A Union that strives for more. Political guidelines for the next European commission, 2019-2024. pp 1-22.

20. Lindsay, J. R. (2013), Stuxnet and the Limits of Cyber Warfare - Security Studies, Vol. 22, No. 3, pp 360-381.

21. Melzer, N. (2013) Human rights implications of the usage of drones and unmanned robots in warfare pp 1-55.

22. Pascucci, P. (2017) "Distinction and Proportionality in Cyber War: Virtual Problems with a Real Solution". Minnesota Journal of International Law. 257, pp 419-460.

23. Richardson, J. (2011). Stuxnet as Cyberwarfare: Applying the Law of War to the Virtual Battlefield. - The John Marshall Journal of Computer & International Law an International Journal on Information Technology, Fall 2011, 29(1), p 1-27.

24. Schmitt, M. (2002). Wired warfare: Computer network attack and jus in bello. Vol. 84 No 846, p. 365-399

25. Schmitt, M. (2011) Cyber Operations and the Jud Ad Bellum Revisited, 56 Vill. L. Rev. 569. pp. 570-606.

26. Schmitt, M. (2012) "Attack" as a Term of Art in International Law: The Cyber Operations Context, IEEE. p 283-293.

27. Sehrawat, V. (2017), Legal Status of Drones Under LOAC and International Law, 5 PENN. ST. J.L. & INT'L AFF. 164. pp 1-44

28. Shackelford, S. (2009). From Nuclear War to Net War: Analogizing Cyber Attacks in International Law. - Berkley Journal of International Law (BJIL), 25(3), 191-250.

29. 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.

30. Swanson, L. (2010). The Era of Cyber Warfare: Applying International Humanitarian Law to the 2008 Russian-Georgian Cyber Conflict. - Loyola of Los Angeles International and Comparative Law Review, Winter 2010 Volume 32 (1), 303-333.

31. Tikk, E. Kaska, K. Vihul, L. (2010). International Cyber Incidents, Legal Considerations, Cooperative Cyber Defense Center of Excellence, CCDCOE, 2010, pp. 4-120.

Legislative sources

32.Charter of the United Nations

33. Customary International Humanitarian Law Rules

34. Hague Regulation 1907

35. Geneva Convention Additional Protocol I 1977

36. Geneva Convention III 1929

37. Geneva Convention IV 1949

38. Rome Statute of the International Criminal Court

Electronic sources:

39. Beyond Skynet: reconciling increased autonomy in computer-based weapons systems with the laws of war. Accessible at: https://www.thefreelibrary.com/Beyond+Skynet%3a+reconciling+increased+autonomy+in+computer-based...-a0385654623. 7 May 2020

40. Human Right Watch (2015) Mind the Gap. The Lack of Accountability for Killer Robots. Accessible at: https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots#695b43. 7 May 2020

41. Oxford Internet Institute (2015) Should we use old or new rules to regulate warfare in the information age? Accessible at: https://www.oii.ox.ac.uk/blog/should-we-use-old-or-new-rules-to-regulate-warfare-in-the-information-age/. 9 May 2020

42. Smith. S. (2019) Military and Civilian Drone Use (UAV, UAS). Accessible at: https://www.thebalancecareers.com/military-and-civilian-drone-use-4121099, 18 February 2020

Appendix 1. Non-exclusive license

Non-exclusive licence for reproduction and for granting public access to the graduation thesis[1]

I _____Igor Tsverkunov_____ (author's name)

1.Give Tallinn University of Technology a permission (non-exclusive license) to use free of charge my creation

IMPLICATION OF INTERNATIONAL HUMANITARIAN LAW IN FIELD OF CYBERSPACE WARFARE,
(title of the graduation thesis)

supervised by _____Evhen Tsybulenko_____ ,
(supervisor's name)

1.1. to reproduce with the purpose of keeping and publishing electronically, including for the purpose of supplementing the digital collection of TalTech library until the copyright expires;

1.2. to make available to the public through the web environment of Tallinn University of Technology, including through the digital collection of TalTech library until the copyright expires.

2. I am aware that the author also retains the rights provided in Section 1.

3. I confirm that by granting the non-exclusive license no infringement is committed to the third persons' intellectual property rights or to the rights arising from the personal data protection act and other legislation.

[1] *The non-exclusive license is not valid during the access restriction period with the exception of the right of the university to reproduce the graduation thesis only for the purposes of preservation.*