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

Ivanna Tetera

CHALLENGES IN THE APPLICATION OF THE LAW OF ARMED CONFLICT TOWARDS MODERN INFORMATION WARFARE

Bachelor's Thesis

Programme HAJB, Specialisation in European Union and International Law

Supervisor: Evhen Tsybulenko

Tallinn 2022

I hereby declare that I have compiled the thesis 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 11547 words from the introduction to the end of conclusion.

Ivanna Tetera ……
(signature, date)
Student code: 194428HAJB
Student e-mail address: ivtete@ttu.ee

Supervisor: Evhen Tsybulenko, PhD:
The paper conforms to requirements in force

……
(signature, date)

Co-supervisor:
The paper conforms to requirements in force
……
(signature, date)

Chairman of the Defence Committee:
Permitted to the defence
……
(name, signature, date)

TABLE OF CONTENTS

ABSTRACT 4
LIST OF ABBREVIATIONS 5
INTRODUCTION 6
1. DEFINING INFORMATION OPERATIONS IN ARMED CONFLICTS WITH THE HELP OF ITS RAMIFICATION 9
1.1. Offensive operations. Dominance over the enemy's information 9
1.1.1. The physical domain of offensive IO 10
1.1.2. The symbolic domain of offensive IO 11
1.1.3. The cognitive domain of offensive IO 12
1.2. Defensive operations. Protection of information and information systems 14
1.2.1. The physical domain of defensive IO 14
1.2.2. The symbolic domain of defensive IO 15
1.2.3. The cognitive domain of defensive IO 16
2. APPLICATION OF INTERNATIONAL HUMANITARIAN LAW TO INFORMATION WARFARE 18
2.1. Principle of distinction 20
2.1.1. Distinguishing a combatant 21
2.1.2. Distinguishing a military objective 22
2.2. Principle of proportionality 25
2.3. Principle of military necessity 26
3. CONCEPTUAL ISSUES IN THE REGULATION OF INFORMATION WARFARE UNDER THE INTERNATIONAL HUMANITARIAN LAW 28
3.1. Defining 'attack' 28
3.2. Defining 'severe suffering' 30
3.3. Defining 'spread of terror' 31
4. SOLUTIONS FOR THE EFFECTIVE REGULATION OF INFORMATION WARFARE 33
CONCLUSION 37
LIST OF REFERENCES 39
APPENDICES 44
Appendix 1. Non-exclusive licence 44

ABSTRACT

Nowadays, due to technological development and globalisation, the nature of armed conflicts gradually changes towards the use of non-kinetic defensive and offensive actions. Considering the development of the means of communication in the 21st century, this thesis gives a short overview of the Information warfare doctrine, which includes the prominent ways of the non-kinetic environment used in times of armed conflicts, and the applicability of the law of armed conflict towards Information warfare.

The present research hypothesis constitutes that there are conceptual factors that preclude the application of the Law of Armed Conflict to the doctrine of Information Operations in times of military hostilities. In the sequence of the research discussions, the issue of the weaknesses in the interpretation of the main International Humanitarian Law concepts in its application to Information warfare was enclosed. Hence, the author presented a potential solution for several issues, one of which is the effective interpretation of the main disputed concepts of the Law of Armed Conflict in the context of Information Operations, in order to achieve the compelling application of the humanitarian law towards this field of informational non-kinetic environment use.

Keywords: Information warfare; information operations; IHL.

LIST OF ABBREVIATIONS

AP	Protocol Additional to the Geneva Conventions of 12 August 1949
CND	Computer Network Defense
CNA	Computer Network Attack
DoD	Department of Defense
ICJ	International Court of Justice
IHL	International Humanitarian Law
IO	Information Operations
MISO	Military Information Support Operations
Tallinn Manual 2.0	Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations
UN	United Nations

INTRODUCTION

The processes of technological development and globalisation became the influential factors for the shift from the traditional physical battlefield with the classical military equipment of tanks and air superiority fighters towards the multidimensional hybrid armed conflicts led in a variety of dimensions, including those like cyber-attacks that are of a virtual matter with the bare link to the tangible objects. Hence, the nature of armed conflicts gradually changes towards more often use of non-kinetic defensive and offensive actions.

Considering the process of development of the means of communication and global information environments in the 21st century, advanced use of operations in connection to information became a new doctrine that includes the prominent ways of the non-kinetic environment usage in times of armed conflicts. As a result, contemporary multi-modal so-called 'hybrid armed conflicts' exploit non-physical battle spaces for Information warfare in combination with cyberwarfare, psychological warfare, and electronic warfare, also jointly with the traditional physical dimension of battlefields.[1]

Despite the fact that Information warfare has negligible consideration in the eyes of contemporary scholars if compared with the frequent discussions on the topic of cyberwarfare, Information warfare nowadays gains momentum with the interconnection of communication and rapid spread of information as a weapon to affect the adversary in the armed conflicts.

Although some aspects of Information warfare are not neoteric for armed conflicts, the topical disputes about the effectiveness and issues in the application of International Humanitarian Law to the information operations in times of armed conflicts emerged due to the rapid progress in the field of Information and Communications means and the current events of the Russian

[1] Hoffman, F.G. (2009). Hybrid Warfare and Challenges. *Joint Forces Quarterly. NDU Press*, 52.Washington. 36-37.; Araźna, M. (2015). Conflicts of the 21st century based on multidimensional warfare – "hybrid warfare", disinformation and manipulation. *Security and Defence Quarterly*, 8 (3), 116.

Federation using information operations in the field of media and cyberspace against Ukraine in the process of the ongoing full-scale invasion of Ukrainian territory by Russian troops.[2]

The author, in the development of this research, focuses on the current Information warfare doctrine of the United States of America Department of Defence (DoD), which specifies Information warfare to comprise information operations. Besides, according to the aforementioned doctrine, information operations should be regarded as a separate dogma that is concerned with the information-connected abilities in times of military operations in order to alter the decision-making of the opponent party and to protect one's own interests. Such doctrine stipulates that information operations can use the means of cyberspace as well as capabilities of the physical realm to accomplish the information supply action.[3]

Consequently, the following research will aspire to deduce the existence of conceptual factors that preclude the application of the Law of Armed Conflict to the doctrine of information operations in times of hostilities. The above-mentioned hypothesis of this paper will be explored through the sequence of the following research questions:

- What are the possible difficulties in the application of IHL principles to Information warfare?
- What are the major problems with the interpretation of the humanitarian law concepts in the context of Information warfare, also with the focus of the existing law of armed conflicts on the direct physical disruption of military objectives and personnel, which could be easily avoided in the information operations?
- What are the potential legal solutions for the enhancement of the International Humanitarian Law application to Information warfare?

In the course of discussions, the recent study intends to reveal the weaknesses of International Humanitarian Law which hinder regulation of Information warfare and to propose possible solutions for several issues, one of which is the effective interpretation of the main disputed concepts of the Law of Armed Conflict in the context of information operations in order to

[2] Institute for the Study of War. (2022). Ukraine: CONFLICT UPDATE 19. *Institute for the Study of War. Critical Threats Project*, AEI. 19, 3.
[3] Theohary, C. A. (2021). Defense Primer: Cyberspace Operations. *Washington, D.C: Congressional Research Service. CRS In Focus.* IF10537, 1-3.

achieve the compelling application of the humanitarian law towards this field of non-kinetic environment use.

Regarding the qualitative research methods of this study, the multifaceted approach will be used, in particular, the first part of the research will focus on the descriptive analyses for further definition and classification of the information operations in armed conflicts, which will be prepared with the help of the process tracing. The discourse analysis, which is based on the literature review, will be used to determine the application of the fundamental concepts and principles of International Humanitarian Law to Information warfare in the second chapter. The third part of this research constitutes the discussion of the previously collected and analyzed information in order to infer and discuss the effectiveness of Information warfare regulation under the Law of Armed Conflicts fundamental principles and customary norms in the translation of the conventional concepts to the area of modern information operations. The fourth chapter of the study consists of the propositions and potential solutions for increasing the effectiveness of the International Humanitarian Law approach towards information operations in times of hostilities.

1. DEFINING INFORMATION OPERATIONS IN ARMED CONFLICTS WITH THE HELP OF ITS RAMIFICATION

Information operations (IO) in times of armed conflicts imply the use of modern technology to transmit determinative information of persuasive matter in an effort to shape specific approaches to dominate common views, influence decisions of military personnel and administer civil population conducts.[4] Contemporary IO uses cyberspace and physical dimensions but also has interlinks with traditional psychological operations (MISO)[5], which became the reason for several scholars to characterise information operations as the domain of influence operations. Besides, the common classification of IO by the categorisation of actions is as follows: defensive, offensive information operations and its supporting elements.

1.1. Offensive operations. Dominance over the enemy's information

In accordance with the common theory about the military strategy, the concept of the offensive operation is defined by the employment of the incessant belligerent activities of combined arms with the aim to obstruct the defender's military units, political control and will to confront the opponent's armed forces.[6] In military circles, the strategic offence is contended to be critical for the attainment of several political ambitions and battle aims. The targeted objectives of paramount importance, which are obtainable exceptionally through the offensive operations, are the territory takeover, power manifestation and disruption of the adversary's ability to counteract and take an act of revenge.[7]

Regarding the traditional military strategy, the offensive information operations ostensibly pursue the aim of deterioration and elimination of the enemy's armed forces' effectiveness on the

[4] Armistead, L. (Ed.) (2011). *Information operations: Warfare and the hard reality of Soft Power* (1st ed.). Joint Forces Staff College (U.S.), National Security Agency/Central Security Service. Washington DC, USA: Potomac Books, Inc.17, 16-18.
[5] *Ibid.*
[6] Agrell, W. (1987) Offensive Versus Defensive: Military Strategy and Alternative Defence. *Journal of Peace Research*. 24 (1). 77.
[7] *Ibid*., 78.

battlefield with the assistance of the influence of the enemy's managerial abilities such as decision-making in order to provide an advantage to one's loyal forces.[8]

The managerial capabilities of the opponent's party could be influenced by the seizure or demolition of the vital strategic supplies upon which the enemy's armed forces rely. The elements of the strategic resources in the information operations dimension are, in specific, information as the data in the context of the transmissible message, human resources that exploit and control the information; and information systems in the meaning of any institution or unit which is committed to arrangement, dissemination, or conversion of information into functional intelligence, also any entity that carries the responsibility for storage and manipulation of data.[9]

The division of the primary offensive objectives is influenced by the aforementioned list of strategic resources in the realm of information operations and, thus, according to the above-mentioned list of objectives, the following generalised four categories are attacks on the opponent's information, data-related processes, systems and personnel.

Several scholars also emphasise that the achievement of desired objectives (destruction of the opponent's resources) in information operations should be considered through the prism of three major domains.[10]

1.1.1. The physical domain of offensive IO

According to Edward Waltz's theory, the physical domain for offensive information operations consists of several physical objects such as communication lines, facilities of armed forces and, in particular, military personnel of the adversary party.[11] Hence, the military targeting of the adversary's resources in the physical (or so-called material) domain comprises of substantial information systems and its supportive elements in the form of administrative personnel, who are

[8] Doyle, M. P., Deckro, R. F., Kloeber, J. M., Jackson, J. A. (2000). Measures of Merit For Offensive Information Operations Courses of Action. *Military Operations Research*, 5 (2), 5.
[9] *Ibid*., 5-6.
[10] *Ibid*.
[11] Waltz, E. (1998). *Information warfare: Principles and operations*. Boston, USA: Artech House. 148-152.; Waltz, D., (1998). The Critical Role of Cognitive Models in Next-Generation Intelligence Architectures, in Proc. of 8th Annual AIPA Symp., Washington DC, 23-24.

in control of information, and electrical power stations, that supply the technological units for the data transmission, etc.[12]

Consequently, the components of the offensive informational operations consist of the physical methods of the enemy's material-related information resources destruction, for instance, air striking the personnel of the command unit or using a powerful ground-based laser against the adversary's communication satellite.[13]

1.1.2. The symbolic domain of offensive IO

The symbolic domain contains information, which is one of the above-discussed elements of strategic resources, and can be defined by the words, graphs and numbers that compose the fundamental part of data. Besides, the symbolic domain includes data-related processes (one more strategic resource) in the form of several manipulations of data, for instance, storage and transmission of data in separate electronic formats such as television signals, radio signals, computer networks, Internet, newsprints, etc.[14] In this order, the military objective in the symbolic domain is the detection, tracking and targeting of the opponent's networks, attacking information sources, information-related processes and elimination of the enemy's servers for data storage.[15]

However, since the symbolic domain is firmly connected to electronics and contemporary progress in technology, consequently, it has an immense effect on the expansion of its domain towards cyberspace. The aforementioned domain, with the help of technological advancement, has been developed into a tool with the assistance of which modern society creates its world-view.[16]

It is significant to acknowledge that the offensive operations components, which help to achieve military objectives in the symbolic domain, extend to the realms of cyber warfare and electronic warfare. In particular, the Computer Network Attack (CNA), which is one of the cyberwarfare's

[12] Waltz, E. (2001, January 1). Data Fusion in offensive and defensive information operations. *Defense Technical Information Center*. ADA400192, 6-7.
[13] Nichiporuk, B., Marshall, A. W. (1999). U.S. Military Opportunities: Information-Warfare Concepts of Operation. In Z. M. Khalilzad, J. P. White (Eds.), *Strategic Appraisal: The Changing Role of Information in Warfare* (1st ed., 179–216). RAND Corporation, 181.
[14] Waltz, E. (1998), *supra nota* 1,148-152.
[15] Waltz, E. (2001, January 1), *supra nota* 1, 6.
[16] Waltz, E. (1998), *supra nota* 2, 149.

parts[17], is exploited in the symbolic domain to destroy the opponent's communication and databases, where the information is stored, or to use the information of the adversary party for one's own military benefit. The attacks in the CNA are divided into scanning attacks (an effort to obtain the information about the network traffic types which are allowed by the firewalls etc.), penetration attacks (an effort to access the system and its resources) and denial of services (an effort to deplete the system's resources).[18]

Furthermore, with the assistance of the electronic warfare realm, specifically, electronic countermeasures, there is a possibility to block the electromagnetic spectrum[19], thus to prevent the opponent from information dissemination via radio, telecommunication means and the internet.

Besides, military deception is one of the components of the symbolic domain, which handles the falsification or manipulation of the enemy's information in order to make him take a decision that is destructive to his initial military interests. One should also note that military deception is customarily applied with the support of electronic warfare and psychological warfare.[20] The events of the Crimean Peninsula annexation by the Russian Federation, when Ukrainian soldiers received messages with the text that their commanders surrendered and abandoned them (which later was constituted to be Russian propaganda), illustrate the way the military deception could be used.[21]

1.1.3. The cognitive domain of offensive IO

The cognitive domain is commonly regarded as the collective apprehension of information. Consequently, separate individual or collective thoughts of the authority group and state population constitute the above-mentioned domain.[22]

---

[17] Bakshi, B. (2018). Information Warfare: Concepts and Components. *International Journal of Research and Analytical Reviews*, 5 (4), 184.
[18] Deka, R. K., Kalita, K. P., Bhattacharya, D., Kalita, J. K. (2015). Network defense: Approaches, methods and Techniques. *Journal of Network and Computer Applications*, 57, 73.
[19] van Niekerk, B., Maharaj, M. (2009). The Future Roles of Electronic Warfare in the Information Warfare Spectru. *Journal of Information Warfare*, 8 (3), 2.
[20] Carter, R. M. (1998). The Information Operations Coordination Cell-Necessary for Division Offensive Actions? *School Of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth*, (98-99), 9-10.
[21] Ghia, U. (2018, December 17). *International humanitarian law in a Post-Truth World*. Cambridge International Law Journal. Retrieved from http://cilj.co.uk/2018/12/17/international-humanitarian-law-in-a-post-truth-world/, 11 March 2022.
[22] Roche, J. (2010). Offensive information operations: a key enabler for the land force. *Australian Army Journal*, 7 (3), 169–182.

In the cognitive domain, perception and rationale manoeuvres are attained by influencing or altering the interrelated beliefs, moral principles and common values' culture of separate individuums and even specific population groups. Hence, the objectives of the offensive information operations in the cognitive domain are the detection and targeting of the perceptions and psychological states of the military personnel who is responsible for the decision-making.[23]

It is significant to comprehend that an adversary has more capabilities to target government and military authority decision-makers through the direct informational influence of the common personnel of armed forces and also the civil population. The component for the achievement of the objectives in the cognitive domain of the offensive operations is the combined use of cyber warfare, as a tool for information dissemination[24], and Military Information Support Operations (MISO). DoD uses the concept of MISO in the cognitive domain for the previously known functions of psychological warfare.[25] Moreover, MISO has a major impact in the sphere of public information and public diplomacy by conveying a specifically chosen message to a foreign audience in order to influence the behaviour and attitudes of foreign governments, groups of people and also internationally known organisations. Such actions aim to alter the decision-making of the adversary party under the influence of the international community.[26]

The prominent use of the MISO operations was the Russian state media rhetoric about the need for Russia to protect the Russian-speaking population, as the Ukrainian government is formed of 'fascists' and 'neo-Nazis' that aimed to commit the slaughter of ethnic Russians in Ukraine. In particular, the Russian Foreign Minister in his interview for RT stated that the government of Ukraine urges the Ukrainian population to kill all Russians.[27] Such media narrative was intentionally and carefully prepared to justify the annexation of Crimea and further invasion of Ukraine in front of the Russian national audience and international society.

---

[23] Waltz, E. (2001, January 1), *supra nota* 2, 4-6.
[24] Bakshi, B. (2018). Information Warfare: Concepts and Components. *International Journal of Research and Analytical Reviews*, 5 (4), 179-184.
[25] Marcellino, W., Smith, M. L., Paul, C., Skrabala, L. (2017, January 1*). Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in support of information operations*. Rand National Defense Research Inst Santa Monica Ca. Santa Monica, USA: Rand Corporation, 10.
[26] Carter, R. M. (1998*), supra nota* 1, 10-11.
[27] Tsybulenko E., Kajander A. (2021) The Hybrid Arsenal of Russia's War Against the Democratic World. In: H. Mölder, V. Sazonov, A. Chochia, T. Kerikmäe (eds) *The Russian Federation in Global Knowledge Warfare.* (173-194). Contributions to International Relations. Cham, Switzerland: Springer, 174-175.

1.2. Defensive operations. Protection of information and information systems

Considering a classical comprehension of the defensive military operations, one could remark that the defensive military operations aim to deter the opponent from commencing the attack. A general military strategy differentiates between forward defence, as the way of blocking the adversary's attack beforehand, deep defence, in means delaying and gradually reducing the effectiveness and strength of the enemy, and irregular defence, which delays and hinders the opponent's attacks.[28]

Defensive information operations in times of Information warfare consist of the number of actions taken in order to prevent the attacks and annihilation of the strategic resources specific to the information operations dimension or counterattack in order to receive back those strategic resources that were previously conquered by adversary powers. Consequentially, the objectives of the defensive information operations are connected to the acts of protection of the strategic information sources, in particular, of information (data, transmissible message), data-related processes (storage and any manipulations with data), systems (any institutions or units responsible for the data processing) and personnel.[29]

In the following sub-chapters, the attainment of the defence information operations' objectives in the physical, symbolic and cognitive domains will be considered.

1.2.1. The physical domain of defensive IO

Having regard to the fact that the physical domain for the information operations consists of material objects, one could note that the main military aim in defensive information operations includes the physical protection of the strategic sources in the realm of Information warfare, which, as was previously mentioned, are information technologies, telecommunication lines, facilities and assets of armed forces and military personnel which performs the data operations, processes and decision-making. Therefore, the objectives of the defensive information operations in the physical domain are classical detection and pursuit of physical ammunition that belongs to an adversary and threatens the information systems of the party and its allies who deploy the defensive information operations [30]

[28] Agrell, W. (1987), *supra nota* 1, 76–78.
[29] Alberts, D. S. (1996). *Defensive information warfare*. Defense Technical Information Center. National Defense University Washington DC, USA: NDU Press Book.
[30] Waltz, E. (2001, January 1), *supra nota* 3, 6-7.

The components of the defensive information operations involve the usage of the traditional physical means and methods for the defence of the army's strategic resources in the physical domain.[31] It is significant to note that the means and methods for the attainment of the objectives in the physical domain are similar for both defensive and offensive information operations. Consequently, the initial military function is to conduct a multitude of complex tasks to prevent the enemy's attack on the physical resources and infrastructure related to the field of information warfare with the help of withholding the adversary's forces or even overtaking manoeuvres for the destruction of the enemy's weapon and troops which threaten the technology, systems and personnel of the information field.[32]

1.2.2. The symbolic domain of defensive IO

In regards to the above-mentioned discussion on offensive information operations, it should be noted that the symbolic domain contains strategic resources in the form of symbolically coded information (words and numbers) and information-connected processes, which include the traditional processes of data storage and data delivering via telecommunication signals, computer networks and internet in order to target previously selected population group.[33]

Hence, the objectives of the defensive information operations in the symbolic domain are the protection of the information and data-related processes in the form of tracking the computer network attacks and the flows from the information objects back to their initial sources.[34] As was previously mentioned, the components of the information operations for the attainment of the military objectives are connected to cyber warfare and electronic warfare. Consequentially, the Computer Network Defence (CND) as an element of cyber warfare is also a component of Information warfare. In specific, this element is used in the defence information operations opposing CNA (a component of the aforementioned offensive information operations). The CND contains a variety of approaches to network attack prevention, for instance, intrusion detection systems (monitoring of the network for malware activities), intrusion response systems and intrusion prevention systems (alarming about the malware and blocking offensive trafficking).[35]

---

[31] *Ibid*.
[32] Hutchinson, W. K., Warren, M. (2017). Attack and defence. In *Information warfare: Corporate attack and Defence in Digital World* (1st ed., 82-89). London; New York: Routledge, 82-89.
[33] Waltz, E. (1998), *supra nota* 3, 148-152.
[34] Waltz, E. (2001, January 1), *supra nota* 4, 6-7.
[35] Deka, R. K., Kalita, K. P., Bhattacharya, D., Kalita, J. K. (2015). Network defense: Approaches, methods and Techniques. *Journal of Network and Computer Applications*, 57, 73-74.

Moreover, several elements of electronic warfare are commonly regarded as the components of information warfare, in this order, the electronic countermeasures are utilized in both offensive and defensive information operations. Electronic countermeasures are used to obstruct the electromagnetic spectrum[36] for the purpose of preventing the opponent from information dissemination via telecommunication means and the internet.

Another component to the symbolic domain of the defensive information operations is the military deception, which may entrap the capabilities of the adversary to coordinate its forces and facilities, this could have significant effects on the opponent's decisions (in the meaning of the decisions which are destructive for the primary military interests).[37] In this order, with the assistance of military deception, one has the ability to prevent deleterious attacks on his strategic information resources.

1.2.3. The cognitive domain of defensive IO

The cognitive domain of information warfare could be related to the knowledge received with the help of the senses, which consequentially results in the sensations and perception of the cognitive information (that one which is received through senses, for instance, visual senses). Furthermore, the cognitive domain is commonly regarded as the realm of intangibles, where the perception affects the morale and public opinion of a specific group of individuals.[38] Therefore, the main objective of the defensive information operations in the cognitive realm is the protection of the government, military decision-makers, common personnel of the armed forces and the civil population from the informational attacks launched in the form of propaganda, misinformation and disinformation. Thus, this means that the primary purpose of defensive information operations is the detection of denial and deception attacks on military decision-makers.[39]

The primary component for the achievement of the objectives in the cognitive domain of defensive operations is the combination of MISO with cyber warfare (used as a tool for

[36] van Niekerk, B., Maharaj, M. (2009), *supra nota* 1, 2.
[37] Waters, G., Ball, D., Dudgeon, I. (2008). Information Warfare: Attack and Defence. In *Australia and Cyber-warfare* (33–58). ANU Press, 20-21.
[38] Brazzoli, M. S. (2007). Future prospects of information warfare and particularly psychological operations. In L. L. Roux (Author), *South African Army Vision 2020: Security challenges shaping the future South African Army* (217-235). Pretoria/Tshwane, South Africa: Institute for Security Studies, 220.
[39] Waltz, E. (2001, January 1), *supra nota* 4, 6-7.

information alteration and dissemination).[40] Psychological operations of MISO influence the sphere of public information and public diplomacy, consequently, there is a paramount importance to take actions of the counter-information and protection of the foreign audience from the adversary's impact, in order not to let affect one's own government and military decision-makers via foreign governments, groups of people and also internationally known organisations. .[41]

[40] Bakshi, B. (2018). Information Warfare: Concepts and Components. *International Journal of Research and Analytical Reviews*, 5 (4), 179-184.
[41] Carter, R. M. (1998), *supra nota* 2, 10-11.

2. APPLICATION OF INTERNATIONAL HUMANITARIAN LAW TO INFORMATION WARFARE

Traditional warfare is governed by a dualistic conception which indicates that the law regulating the resort for the armed force to be permissible is *jus ad bellum* and the law governing the conduct of hostilities in times of armed conflict is *jus in bello*.[42] It is significant to note that the use of armed forces against any state is strictly prohibited under Article 2(4) of the United Nations (UN) Charter[43], however, there are only two exceptions. It is permitted for the states to recourse to armed forces in an action for the individual or collective self-defence under Article 51 of the UN Charter.[44] Also, with the exception under Articles 39-42 of the UN Charter, the recourse to the use of force is allowed if it is authorized by the UN Security Council.[45]

The common modern name for the law regulating the conduct of warfare under *jus in bello* is International Humanitarian Law (IHL) or Law of Armed Conflict (such name has broader applicability to the armed conflicts of international and non-international nature). The main purpose of IHL is the mitigation of conflict influence, elimination of excessive suffering, securing fundamental human rights, and preventing conflict deterioration toward fatal savagery and spread of terror. Moreover, actions taken in conformity with the law of armed conflicts have the tendency to decrease the disruptions in the military discipline, thus, also retaining the resources and evading global-wide violence.[46]

Considering the fundamental sources of law for armed conflicts, one could divide such sources into customs, norms of IHL and also two main categories. Namely, the first category is so-called the Geneva Law, which consists of four conventions and additional protocols that grant protection to combatants and non-combatants in times of warfare. The Geneva conventions of 1949 are the customary law and protect their subjects according to their names: Wounded and

[42] Stahn, C.(2006) 'Jus ad bellum', 'jus in bello' . . . 'jus post bellum'? –Rethinking the Conception of the Law of Armed Force. *European Journal of International Law*, 17 (5), 925.
[43] Charter of the United Nations, Article 2(4).
[44] *Ibid.,* Article 51.
[45] *Ibid.,* Article 39-42.
[46] Vadnais, D. M. (2012). *Law of armed conflict and information warfare-how does the rule regarding reprisals apply to an information warfare attack?* United States: BiblioScholar, 97 (3), 6.

Sick; Wounded, Sick and Shipwrecked; Prisoners of War; and Civilians. The second category is Hague Law, which regulates the means and methods used in armed conflicts (Hague Conventions are also widely recognised as the customary law).[47] It should be remembered that the IHL applies only to international and non-international armed conflicts, meaning that the IHL does not cover inter-state disturbances and tensions such as revolutions.[48]

The IHL's common set of rules endeavours to restrain the humanitarian consequences of military conflicts by the above-mentioned restrictions of the means and methods used during the armed conflicts and safeguarding the humane treatment of civilians and *hors de combat* (prisoners of war and injured military personnel), who do not take part in the fighting.[49] In order to provide protection to the aforementioned group of people, the rules of targeting in the armed attacks are established upon three main IHL principles (which are customary norms): the principle of distinction, the principle of proportionality and military necessity.

Once the military action is characterised as an armed attack, the principle of distinction necessitates combats to conduct their attacks against the military objectives of the adversary party; thus, the principle prohibits attacking the civilian population[50] (in the status of persons who do not participate in the hostilities) and civilian objects.[51] The principle of proportionality forbids combatants to conduct indiscriminate attacks, where such attacks could result in collateral damage to civilians and civilian objects and would be excessive in regards to the military advantage which was anticipated in the conduct of the attack.[52] Lastly, the principle of necessity requires the use of measures that are permitted under the IHL and are needed for the attainment of the legitimate military aim.

With the rapid development of telecommunication technology, it is visible that the law of armed conflicts is several steps behind the objectives of the contemporary world, and this requires immediate regulation. Considering Information warfare in the context of the IHL, the application

---

[47] Fleck, D. (Ed.). (2021). *The Handbook of International Humanitarian Law* (4th ed.). Oxford, United Kingdom: Oxford University Press, 30-35.
[48] *What is International Humanitarian Law?* (2004). Advisory Service on International Humanitarian Law, ICRC. Retrieved from https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf, 11 March 2020.
[49] Melzer, N. (2016). *International humanitarian law: A comprehensive introduction.* Geneva, Swizerland: International Review of the Red Cross, ICRC, 17.
[50] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 18 June 1977. (AP I), Article 49.
[51] AP I, *supra nota* 1, Article 48.
[52] AP I, *supra note* 2, Article 51(5)(b).

of the IHL and its principles to IO is inexplicit and quite obscured due to the difficulty in defining the contemporary information attacks, especially, those that have no connection to the tangible world. The conventional attack, as the conduct that qualifies for the act of warfare, will be discussed in the sections below.

The appliance of IHL to Information warfare is abundant through the inability to regulate several topical questions, in particular, identification of the parties to the conflict (when an individual becomes a combatant), also growing interconnectivity between the military and civilian information resources (use of social media for the military purposes). As a result, there is a definite need to reconsider the main understanding of whether the IHL can apply to the situations of the warfares with the dominant non-lethal nature, such as Information warfare.[53]

It is also important to note that the difficulty of the IHL application to Information Operations is connected to the ultimate focus of the law of armed conflicts on the objective of direct physical destructions, thus, in the following subchapters, the discussion on the applicability of the general IHL principles to the Information warfare domains will be presented.

2.1. Principle of distinction

The keystone of the International Humanitarian Law is the principle of distinction, which is established on the perception that the main and the only legitimate aim for the party to the armed conflict to achieve is to weaken the armed forces of the adversary party[54], meanwhile, the civilian population and *hors de combat* should be able to enjoy general protection against the perils of the hostilities.[55] The significance of the principle of distinction was emphasised in the Advisory Opinion to the *Nuclear Weapons* case, where the mentioned principle was characterised as 'intransgressible'[56]; thus, it could be argued that the International Court of Justice (ICJ) meant to characterise the principle of distinction as the one under the status of *jus cogens*, according to which the aforementioned principle is unchangeable.[57] Consequently, in order to

[53] Vadnais, D. M. (2012), *supra nota* 1, 3.
[54] Melzer, N. (2016), *supra nota* 1, 18.
[55] AP I, *supra nota* 3, Article 51(1).
[56] *Legality of the Threat or Use of Nuclear Weapons*, Advisory Opinion, 1996 July 8, ICJ, para.78-79. Retrieved from https://www.icj-cij.org/files/case-related/95/7497.pdf, 17 March 2022.
[57] Quénivet, N. (2010). The "War on Terror" and the Principle of Distinction in International Humanitarian Law. *ACDI Anuario Colombiano De Derecho Internacional*, 3, 161.

launch an attack, it is mandatory for the combatants to distinguish between the combatants of the enemy's armed forces and civilians. Also, there is a strict requirement to differentiate between civilian objects and the enemy's military objects, so to conduct an attack only against the military objectives.[58]

2.1.1. Distinguishing a combatant

The concept of combatant covers all members of the armed forces of the party to hostilities, apart from medical and religious personnel if those are carrying solely humanitarian activity on the battlefield.[59] Besides, the complexity of the concept of a member of the armed forces is governed by the Hague Regulations, which stipulate that the laws, rights and duties in times of armed conflict should apply not only to usual conventional regular armed forces but also to irregular forces, including volunteer corps. The irregular armed forces should satisfy four primary conditions which help to distinguishably equate them to the regular armed forces of the state. Consequentially, the conditions indicate that persons of such irregular armed forces should be commanded by an individual who takes the responsibility for the subordinates; they should have a fixed emblem that could be recognized at a distance; they are supposed to carry their arms openly; also, they should fight according to the laws and customs of war.[60]

In regards to the multidimensional nature of Informational warfare, one can argue for the existence of the conventionally defined combatants in the physical domain of the offensive and defensive information operations. Indeed, if the administrative personnel in control of information, electrical power stations (that supply the technological units for the data transmission) and military decision-makers are members of regular armed forces or irregular armed forces, which comply with the four above-mentioned criteria, such persons could be considered as the combatants. However, the symbolic domain of Information warfare includes the use of CNA (in offensive IO) and CND (in defensive IO) which are commonly led by separate cyber knowledgeable individuals or a group of cyber-activists.[61] Hence, it is enormously difficult to distinguish if the civilian or the combatant of the state official cyber security office was behind the launched cyberattack of non-physically destructing nature.

[58] AP I, *supra nota* 4, Article. 48.
[59] AP I, *supra nota* 5, Article 43(2).
[60] Melzer, N. (2016), *supra nota* 2, 81.; Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, The Hague, 18 October 1907, Article 1.
[61] Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in Bello. *Revue Internationale De La Croix-Rouge/International Review of the Red Cross*, 84 (846), 377.

In the cognitive domain, the attack (if it could be defined so, according to the existence of its physically destructive consequences) of disinformation or propaganda dissemination is usually led by the state information centres and press; thus, it creates a problem in the defining of the combatants for the cognitive domain, as journalists and ordinary citizens disseminate information among the population with the help of common communication means.

On this ground, in accordance with the recent events of the armed conflict, citizens in Ukraine participate in the IO of the cognitive domain while sharing videos and stories of how civilians stand up against the Russian occupation forces to an international audience in order to make the national fight known worldwide. This situation indicates a high level of computer literacy and a phenomenon of modern conflicts, where civilians also take part in Information warfare.[62] In regards to journalists, Article 79 of Additional Protocol I (AP) constitutes that status of civilians is provided to the journalists, however, the scope of the protection is provided only to individual journalists[63] but not to the products of their journalistic work, for instance, articles published on websites.

2.1.2. Distinguishing a military objective

According to AP I, military objectives could be defined as 'those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralisation, in the circumstances ruling at the time, offers a definite military advantage'.[64] Considering the above-mentioned definition, it is clear that the regular objects of the physical domain (electronic means and equipment) which are used exceptionally or predominantly by the armed forces should be undoubtedly considered as the military objectives.

Nonetheless, questions arise while defining the military objectives in the symbolic and cognitive domains of offensive and defensive information operations. As was already mentioned, the symbolic domain of Information warfare is connected to the cyberwarfare realm. Thus, one could struggle with the allocation of cyberspace elements toward the military objective or civil object categories. An objective of cyberspace, which includes telecommunication networks and

[62] Henkhaus, L. (2022, April 15). *The role of the internet in Ukraine's Information War*. Texas A&M Today. Retrieved from https://today.tamu.edu/2022/03/14/the-role-of-the-internet-in-ukraines-information-war/, 16 April 2022.
[63] AP I, *supra nota 6*, Article 79
[64] AP I, *supra nota 7*, Article 52(2).

the Internet, usually carries a dual function and is used for military and civil purposes, for instance, governmental sites where the information is publicly displayed could become a target for warfare in order to be used as a space for the information dissemination of the adversary party.

A prominent example of cyber warfare use in connection to Information warfare is when, in 2008, during the armed conflict in Georgia, Russia made an effort to establish control over traditional media and social narrative elements of the Georgian state in cyberspace with the support of demonstrative CNA.[65]

The cognitive domain of Information warfare is also closely connected to cyberspace; therefore, the dissemination of information could target government and military authority decision-makers through the direct informational influence of the military personnel and usual civilian population via threatening messages with the terrorising content. Moreover, MISO operations in the cognitive domain of Information warfare have a major impact on the sphere of public information in order to influence the behaviour and attitudes of foreign governments and international audiences. Such actions aim to alter, disrupt or corrupt, the decision-making of the adversary party under the influence of the international community.[66] Such informational influence is conducted with the help of social media, which is in common use among civilians and individuals of the armed forces, however, exactly individual users make a significant contribution to social media data via their public posting. Consequently, social media create a database of information on public demographics, activities, size, geographic spread (geotags of the posts) and the network of the reached audience[67], which could not be clearly defined as the civilian object or military objective. The aforementioned elements of data provide a potential for the operations to disseminate message disinformation or the counter spread of ideas and info among the particular audience or social group with a specific aim of discrediting the adversary party in the local or international community. As an apparent result of Information warfare in the cyberspace of social media, the civilian population worldwide and military personnel could be affected by the influential informational content of various kinds via the information spread on the common social media platforms of Facebook, Twitter, YouTube, Snapchat, Instagram, etc.[68]

[65] Roche, J. (2010), *supra nota* 1, 173.
[66] Carter, R. M. (1998*), supra nota* 1, 10-11.
[67] Marcellino, W., Smith, M. L., Paul, C., Skrabala, L. (2017, January 1), *supra nota* 1,7.
[68] *Ibid*., 7-8.

For the illustration of the scale of the social media usage for the dissemination of the terrific disinformation under MISO conducts during the armed conflict, one could consider the most scandalous reportage of the Russian national Channel One of 2014[69], which is gaining momentum nowadays due to Russian-paid internet employees of information warfare which are sharing pro-governmental content and comment news articles worldwide.[70] The above-mentioned reportage was displaying a refugee woman from the Ukrainian town of Slovyansk, who claimed to be an eyewitness of the event when the Ukrainian soldiers assembled local people on Lenin Square and nailed a three-year-old boy on a notice board, leaving him to die there meanwhile his mother was watching the scene and then she was tied to a Ukrainian tank and carried around until that poor woman died. The reportage had a specific aim to influence the emotions and objective reasoning of foreign audiences and, eventually, the acts of foreign governments toward Ukrainian authorities and people. However, the story was debunked with the single fact that there is no Lenin Square in Slovyansk, where supposedly the public execution happened.[71]

Besides, to understand the extended scale of the problem, one should note that opposing Russian paid internet employees, the Russian authorities regard negative comments spread on the social media about the occupation and actions of the Russian government in Crimea and illegally occupied parts of Ukraine as the acts of separatism which amount to the criminal penalty of up to two years of imprisonment.[72] Such actions of the Russian government are evident examples of the opposition media influence limitation in times of the armed conflict and occupation in order to control the media narrative.

Considering the above-mentioned discussions, one can infer that for distinguishing the combatants and military objectives in Information warfare, it is not enough to have the usual conventional criteria. Moreover, there is a significant difficulty in defining the concept of attack, for the principle of distinction to apply in combination with other principles and norms of IHL.

[69] Khaldarova, I., Pantti, M. (2016). Fake News. The narrative battle over the Ukrainian conflict. *Journalism Practice*, 10 (7), 894.
[70] Marcellino, W., Smith, M. L., Paul, C., Skrabala, L. (2017, January 1). *supra nota* 2, 15.
[71] Khaldarova, I., Pantti, M. (2016), *supra nota* 1, 896.
[72] Tsybulenko, E., Platonova, A. (2019). Violations of Freedom of Expression and Freedom of Religion by the Russian Federation as the Occupying Power in Crimea. *Baltic Journal of European Studies*, 9 (3 (28)),134−147; Tsybulenko E., Tetera, I. (2021) Occupation of Crimea and military invasion of Donbas: International law and responsibility of the Russian Federation. In: Lodyn, P. (ed) *Surviving near the empire: Price of the modern Kremlin's aggression.* (152-182), Ivano-Frankivsk, Ukraine: GOTsPND/IWP, 157.

2.2. Principle of proportionality

In accordance with the principle of proportionality, if significant harm to civilian objects and civilians cannot be escaped, such an attack should be considered under the proportionality rule. Hence, the military personnel which is in the responsibility for planning any attack should refrain from conducting or should postpone an attack that may result in damage to civilian objects, collateral losses among civilians, or contain both of the abovementioned, which could be superfluous in connection to the expected military advantage.[73] The disproportionality of the military attack could be defined only in the direct comparison. In case a launched attack resulted in incidental damage to civilians or civilian objects and the damage is considered to be excessive in relation to the achieved military advantage, such an attack could be characterised as a disproportionate one, thus, further could qualify as a war crime.[74]

Having regard to the above-mentioned, one could refer that the principle of proportionality is applicable only to the physical domain of Information warfare where the attacks on the tangible info sphere infrastructure, for instance, telecommunication technology and electrical grids, could have a direct effect not only on the adversary's armed forces but also on the civilian population, which will affect the work of the critical services provided by civilian authorities and medical institutions concerned with the attacked infrastructure.[75]

Nonetheless, a notable ethical conundrum about the principle of proportionality emerges in the symbolic and cognitive domains. Conceding that the majority of IO do not attack materially based infrastructure or the physical state of human beings, according to the afore-described principle of proportionality, such attacks comply with the principle regardless of the severity of non-physical consequences caused by the attack.[76]

Therefore, one can infer that the offensive and defensive IO which do not result in the excessive violent physical disruptions are not regulated by the principle of proportionality because such attacks (if they can be qualified so in the cognitive and symbolic domains of Information warfare) do not have a severe physical but psychological impact on the civilian population. Besides, the principle of proportionality is not relevant in connection to the material harm caused

[73] AP I, *supra nota* 8, Article 51(5)(b).
[74] Rome Statute of the International Criminal Court, Article 8(2)(b)(iv).
[75] Melzer, N. (2016), *supra nota* 3, 102.
[76] Taddeo, M. (2019). Just information warfare. *Ethics and Policies for Cyber Operations*, 124, 77.

to military objectives or personnel of armed forces, unless such harm caused to civilians is superfluous in connection to the achieved military advantage.

2.3. Principle of military necessity

The Law of Armed Conflicts is founded on the balancing edge of military necessity and humaneness. Hence, IHL admits the possibility of death, injury or destruction to emerge due to the military necessity in order to defeat the enemy. However, the attacks should not be deliberate and target only military objectives and personnel, in the interim, the destruction and damage caused to the civilian population and civilian objects should be proportionate in connection to the expected military advantage to be achieved. Moreover, in accordance with IHL, the military attack has limitations in the variety of means and methods of warfare for it to be launched.[77]

According to the open letter of Luis Moreno-Ocampo, the Chief Prosecutor at the International Criminal Court, about the investigation of the war crimes during the invasion of Iraq in 2003, the death of civilians in time of armed conflict does not constitute a war crime directly unless the attack was carried disproportionally. Thus, IHL and the Rome Statute allow combatants to launch attacks against the military objectives in accordance with the principle of proportionality, even if it can result in the death of civilians.[78] Nonetheless, war crimes emerge when such an attack was carried out deliberately against civilians and civilian objects[79] or such an attack was conducted against the military objective with the knowledge that it could result in excessive harm to civilians and civilian objects in connection to the achieved military advantage[80].

As was mentioned before, the military necessity also applies to the means and methods of warfare, consequently, the IHL prohibits those means and methods which could inflict unnecessary severe suffering and damage. The Hague Regulations indicate that the sole legitimate aim of the armed forces during the armed conflict is to weaken the military personnel

[77] Melzer, N. (2016), *supra nota* 4, 17; *Military necessity*. Military Wiki. (n.d.). Retrieved from https://military-history.fandom.com/wiki/Military_necessity#CITEREFMoreno-Ocampo2006, 10 April, 2022.
[78] Moreno-Ocampo, L. (2006). OTP letter to senders re Iraq. International Criminal Court, 4-5.
[79] Rome Statute of the International Criminal Court, Article 8(2)(b)(i).
[80] *Ibid*., Article 8(2)(b)(iv).

of the enemy, which includes the aim to disable the biggest possible number of the adversary party personnel without inflicting superfluous injury or unnecessary suffering.[81]

In the application to Information warfare, the principle of military necessity is limited because of the aforementioned problems in the application of principles of distinction and proportionality to the IO. Consequently, in the symbolic and cognitive domain of Information warfare, it is problematic to attack only legitimate military objectives and personnel of armed forces, as there is a serious difficulty in distinguishing the military objectives and personnel involved in the interconnected cyberspace, for instance, social media. Furthermore, one can infer the problem with the regulation of the means and methods in the Information warfare, as the concept of the severe, unnecessary suffering, as will be discussed further, is bound to the material physical domain, while most of the IO is handled in the cyberspace without any kinetic force used, thus avoiding the causation of the destruction and direct physical suffering.

[81] Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, *supra nota* 1, Article 23(e).

3. CONCEPTUAL ISSUES IN THE REGULATION OF INFORMATION WARFARE UNDER THE INTERNATIONAL HUMANITARIAN LAW

The previously discussed applicability of the IHL and its key principles is evidently hindered by the ambiguity of the Information warfare multidimensionality, where the conventional concept of attack is concerned with the thresholds to be passed by the IO in order to be qualified as the attack. What is more, the limiting criteria for the definition of the attack, as well as other concepts such as the 'spread of terror' and 'severe suffering' in the IHL, result from the rules which were interpreted in the light of the war practices of the twentieth century and which seems to apply only to one domain - physical dimension of material objects.[82] Therefore, the following discussion will be based on the consideration of the aforementioned concepts in regard to the twenty-first century IO.

3.1. Defining 'attack'

As was hinted above, there is a dilemma in defining whether certain conducts of offensive and defensive IO could be eligibly considered as the military attack within the limits of IHL, in order for such operations to be governed by the principle of distinction, the principle of proportionality and the principle of military necessity.[83]

Following Article 49 of the Additional Protocol I, attacks, in the conventional understanding, constitute the offensive or defensive acts of violence directed against the enemy's armed forces.[84] Hence, the concept of violence relates to the act or its effect, as the result of the violent conduct (for example, the effect of a biological or chemical weapon, which is not always instantaneous).[85]

[82] Lahmann, H. (2020). Protecting the global information space in times of armed conflict. *International Review of the Red Cross*, 102 (915), 1234.
[83] *Ibid*., 1241.
[84] AP I, *supra nota* 9, Article 49.
[85] Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 94 (886), 557.

Considering the obscurity of Information warfare, one could regard that the closest definition of the attack for the IO would be the 'cyber-attack' used in the symbolic and cognitive domain, even though IO is assumed as a distinct type of operation from cyber ones. The Tallinn Manual 2.0 emphasizes that a cyberattack is a cyber operation of offensive or defensive nature, that is anticipated to inflict injury or even death to individuals or destruction to objects.[86] Consequentially, the connection between the instance of an information manipulative act and the physical damage should be sufficient enough to qualify such an act as an attack.[87] However, for the act to be considered a 'military attack', there should be a direct relationship between the death or physical harm caused to the person or object and the IO. Here the difficulty in the causation's tracing is related to the wide range of IO effects which over the time can have unpredictable results, for example, hardly detectable logic bombs (a piece of code inserted in software) as the conducts in the symbolic domains of IO have no immediate effect and could result into the data change or deletion over the time.

Once the conduct of IO was qualified as the attack, it should be examined if such an act complied with the IHL principles. Given that, according to the principle of distinction, the attack should target the personnel of the adversary's armed forces. Meanwhile, it is controversial if an informational attack will be in accordance with the principles of proportionality and military necessity, as it could be expectable for the disinformation, misinformation or any other manipulated data to be shared not only among the personnel of the enemy's armed forces but because of the modern social media platforms, also among the civil population.[88]

However, considering the aforementioned discussion on the definition of the attack, one should also note that it is enormously hard to establish the chain of the direct causation in most IO cases, which leads to the mal-regulation of such operations under the premises of undefined attack. The main harm and damage caused by the IO is located in cyberspace (within the symbolic and cognitive domains) and has no imminent direct impact on the material objects of the physical domain. Evidence for that is the deployment of the data destructive malware by Russia against

---

[86] Schmitt, M. N. (Eds.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* United Kingdom: Cambridge University Press, rule 30.
[87] Lahmann, H. (2020), *supra nota* 1, 1241.
[88] Choudhary, V. (2021, August 9). *The truth under siege: Does international humanitarian law respond adequately to information warfare?* Groningen Journal of International Law. Retrieved from https://www.grojil.org/blog2/2019/03/21/the-truth-under-siege-does-international-humanitarian-law-respond-adequately-to-information-warfare, 9 April, 2022.

the Ukrainian governmental agencies and financial institutions during the current events of the Russian invasion of Ukraine.[89] Such 'attack' was successfully repelled, although it had an aim to disrupt the cyberspace infrastructure of the governmental institutions, which could have a further impact on providing basic financial and administrative services to the population, thus, consequences could be of far-reaching instance.

In any case, in the absence of the connection to the causation chain which leads to the physical harm, the IO military conducts in time of Information warfare supposedly falls outside the scope of the traditional law of armed conflict.[90]

3.2. Defining 'severe suffering'

The Tallinn Manual 2.0 indicates that the defensive or offensive IO of symbolic and cognitive domains could be determined as an attack in the case if such an operation inflicts a psychological condition upon the individual or group of individuals, which causes 'mental suffering'.[91] Furthermore, in compliance with the Additional Protocol I, any acts or conducts of violence that aim to distribute terror among civilians are prohibited.[92] Therefore, one should note that the mental suffering and actions with the initial purpose of inflicting mental harm are in the diapason covered by the IHL regulations.

The conundrum emerges in the discussions about defining the degree of mental suffering which is covered by the Law of Armed Conflicts, thus, the mere fear and stress fall outside the IHL sphere of influence. Consequently, it is apparent that not all human reactions to the specific IO in the symbolic and cognitive domains are sufficient in order for such operations to amount to the concept of an attack. Notably, the consideration of the degree of suffering could be advanced towards the supposition of the term 'severe mental suffering' under the widespread impact of the IO if it leads to extensive delirium, disorder and continuous despair among civilians of the attacked state. Thus, for the extended appliance of the IHL rules and norms, clear, measurable

[89] Brandt, J., Pita, A. (2022, March 3). *How is Russia conducting Cyber and Information Warfare in Ukraine?* Brookings. Retrieved from https://www.brookings.edu/podcast-episode/how-is-russia-conducting-cyber-and-information-warfare-in-ukraine/, 9 April, 2022.
[90] Lahmann, H. (2020), *supra nota* 2, 1242.
[91] Schmitt, M.N. (2017), *supra nota* 1, rule 92.
[92] Choudhary, V. (2021, August 9), *supra nota* 1.

criteria for the assessment of the mental suffering caused by the offensive MISO and military deception as the elements of IO should be defined.[93]

However, in the scenarios where the 'severe mental suffering' could be defined, the IHL governing would be concerned with the scope of consequences for the mental well-being of civilians and, alas, not with the health and probity of the attacked information space, which could have a further impact on the aftermaths of the armed conflict, when the trust to the state-building and state authorities will be affected. Therefore, doubts arise regarding the sufficiency of the current IHL's protection provided for the civilians and information space against the insecurities brought upon modern society by the contemporary Information warfare.[94]

3.3. Defining 'spread of terror'

It was already mentioned that the IHL prohibits any act or threat, the primary purpose of which constitutes the spread of terror among the civilian population[95], thus, it contributes to the protection of the civilians against some offensive IO. The above-mentioned prohibition is indicated in Article 51(2) of AP I and also is a part of IHL customary law.

Nonetheless, the aforementioned rule consists of two initial elements, either of which should be satisfied in order for the prohibition to be enacted upon such offensive military action. Hence, in connection to the IO and Information warfare, an offensive or defensive act in any of the IO domains should amount to the concept of 'attack' in the scope of IHL, or such an act should qualify as a 'threat of violence'.[96]

The case of IO defined as an attack was discussed in the subchapter above, thus, one could consider that the majority of IOs do not amount to the concept of an 'attack', although the IO conducts could disseminate disinformation with the intent to spread terror among civilians. Consequently, in the logical lead, if the IO act does not account for the 'attack' then such conduct could not be regulated under the aforementioned Article 51(2) of AP I, even if its initial aim was

[93] Lahmann, H. (2020), *supra nota* 3, 1243.
[94] *Ibid*.
[95] AP I, *supra nota* 10, Article 51(2).
[96] Schmitt, M.N. (2017), *supra nota* 2, rule 98.

to spread terror among a targeted group of people unless such act could be qualified as a threat or an act of violence.[97]

Considering the concept of 'threat of violence', it may be defined in Information warfare as the acts of the information being addressed to the audience with the implication for the forthcoming unfavourable events and violence.[98] In such cases, any efforts of IO to take advantage of the state of terror in order to destabilize the adversary's party in the armed conflict will not automatically enact the prohibition unless the real threat of a violent act emerges. This entails that the act cannot be qualified as the one that spreads terror unless such conduct does not amount to the concepts of 'attack' or 'threat of violence' and does not conceal the primary aim to informationally terrorize the civil population of the targeted state, regardless of the fact, if such an act could result in the direct spreading of the terror.

The dilemma emerges as to whether it is sufficient enough to consider the IO act, which has the terrorizing effect, in accordance with the conventionally defined concepts of an 'attack' and 'threat' in order to apply the prohibition under Article 51(2). Hence, the prohibition on the spreading of terror should be reconsidered following the effect that modern IO conduct has on the civil population in the globally interconnected space of telecommunication means.

[97] Lahmann, H. (2020), *supra nota* 4, 1239.
[98] Winther, P. (2019*). International Humanitarian Law and Influence Operations: The Protection of Civilians from Unlawful Communication Influence Activities during Armed Conflict*. (PhD dissertation). Acta Universitatis Upsaliensis, Swedish Defence University, Department of Security, Strategy and Leadership (ISSL), Centre for International and Operational Law. Department of Law, Uppsala University, Sweden, 148.

4. SOLUTIONS FOR THE EFFECTIVE REGULATION OF INFORMATION WARFARE

Due to the rapid development of telecommunication means, technologies used in cyberspace and the complexity of Information warfare regarding the number of domains where the IO of elements are located, the discussions in the previous chapters indicate that the traditional conventional IHL regulations have obscurity in their application to IO. In regards to the afore-discussed vagueness of the conceptual implication of the Law of Armed Conflict, it is indisputable that Information warfare requires more detailed regulation, notwithstanding its nonviolent consequences in accordance with the challenges of the contemporary world.

It is significant to emphasize the need for the IO regulations among the domains where such operations do not result in direct material damage, for example, the coercion of the media ecosystem could be a result of Information warfare with a long-lasting effect even after the resolution of an armed conflict. The distortion of the media ecosystem emerges when the IO campaigns in its cognitive domain during the armed conflict aim to undermine the public support of the adversary party with the propaganda and disinformation spread via social media, its own and also the adversary's television channels (access to which is usually earned with the cyberattacks).[99] The above-described media coercion could achieve its primary result when the affected adversary party will be forced to retreat from the fight due to the lack of state-population support. Moreover, a long-term consequence of the media ecosystem distortion could emerge in connection to the lost public trust for state media and the governmental structures, which can turn into continuous political instability and affected state being exploited by the adversary state.[100]

Besides the aforementioned situation with the media coercion, one can note that the regulation of Information warfare is required upon the majority of other IO in the symbolic and cognitive domains, which, due to several reasons, do not amount to the conventionally defined concepts of

[99] Lahmann, H. (2020), *supra nota* 5, 1231.
[100] *Ibid.*

'attack', 'severe suffering' and 'spread of terror', also, have non-physical damage to the targeted state and its population.

Hence, considering regulations of IO in the symbolic domain, it is undoubtful that cyberspace and its elements are the least ruled by the legal system of conventions, protocols, and customary norms of the IHL. Furthermore, there are no internationally recognized binding documents on the detailed and specific regulation of cyberwarfare, elements of which are used in Information warfare. Nonetheless, due to the danger enacted by the further development of cyber technologies and the use of cyberspace, some international organizations led the discussions concerning the applicability of international law to the cyber dimension.

Thus, the Group of Experts, on the side of the North Atlantic Treaty Organization (NATO), in its collective attempts to solve the matter, produced two manuals on the applicability of the IHL and other instances of international law to cyber operations, those manuals are Tallinn Manual on the International Law Applicable to Cyber Warfare (Tallinn Manual) and Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Tallinn Manual 2.0).[101] The common generalization about the manuals is that the initial Tallinn Manual is concerned merely with the way how the international law regulations on the use of force are applied to the cyber warfare (cyber operation amounting to 'use of force' if the effect of such operation is comparable with the non-cyber operations)[102], in the interim, Tallinn Manual 2.0 considers the vast range of cyber operations which do not amount to the concept' use of force'.[103] What is more, both above-indicated documents have no binding power and are used as mere instruments for the authorities to translate international law into the cyber dimension for the regulation of the cyber affairs in the traditional way, where the major kinetic impact of the operations is discussed. Hence, there is no direct conventional or customary regulation on cyber operations. The mere instructions given by Tallinn manuals provide a hint for the development of further regulations on the matter.

Lastly, regulation of the IO in the cognitive domain is partially covered by the traditional conventional IHL, if such operations correspond to the classical definition of the attack (as was discussed above). The paradox of Information warfare is that the more implausible is to define the

[101] Schmitt, M. N. (Eds.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare.* United Kingdom: Cambridge University Press.; Schmitt, M.N. (2017), *supra nota* 3.
[102] Schmitt, M. N. (Eds.) (2017), *supra nota* 4, Foreword.
[103] Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law*,48 (3),738-739.

launched IO as a conventional attack, the more probable is that such IO conduct will be permitted to be used against civilians and civilian objects, regardless of the severity of its indirect consequences.[104] As a result, Information warfare should not be treated homogenously and the regulation of IO should be considered in all possible details in order to avoid the extensive influence of the cognitive domain IO on the targeted state and its population after the armed conflict.[105]

Firstly, the new framework for Information warfare should be established with the fundamental reconsideration of the main IHL concepts to enhance the effectiveness of its application towards IO. In this order, the 'attack' should be defined in the inclusion of the influential IO range in the cognitive and symbolic domains, also in accordance with the nature of some IO to have a long-lasting or indirectly visible impact on the population and the targeted state. With the widening of the range for the determination of the IO conduct as an attack, the application of the principle of distinction, the principle of proportionality and the principle of military necessity will be advanced. Also establishing clear rules for distinguishing between the combatants and civilians, as well as civilian objects and military objectives under the principle of distinction, will prevent the emergence of negative consequences of IO in the symbolic and cognitive domains, thus, it will relieve the majoring issues in the IO governing.

Secondly, the definitions for the concepts of 'severe suffering' and 'spread of terror' should be reviewed upon the technological realities of IO where a new threshold will be established for the IO act and its consequences to amount to these concepts in order to be regulated under IHL. Lastly, the implementation form for new legislation is significant. A new regulative framework should be dedicated solely to Information warfare with the separate regulations for the IO of the symbolic and cognitive domains since IO in these domains is the most problematic for the regulation. Besides, such legislation should have internationally binding conventional power upon its member states, based on the example of the Geneva Conventions of 1949.

Consequentially, the potential legal solution to the problem with the Information warfare regulation should be a new Convention as the set of rules on the regulation of IO in times of armed conflict with the inclusion of the afore discussed factors. Such a convention could be prepared and executed

[104] Hollis, D. B. (2007). Why States Need an International Law for Information Operations. *Lewis & Clark Law Review*, 11 (2008-43),1043.
[105] Haslam, E. (2000, December 1). Information warfare: Technological changes and international law. *OUP Academic. Oxford University Press*, 5 (2), 167.

by the international body in its connection to the IHL, for instance, under the watch of the International Conference of the International Red Cross and Red Crescent Movement or the UN. The focus of the convention should be shifted towards the maximum prevention of the non-kinetic or indirect kinetic consequences of the IO use within the new technological realities that will develop even further. Considering the internationally binding power of such a convention, one should note that it will be enormously difficult to reach the level of ratification as the Geneva Conventions of 1949 have, however, the international community should understand the purpose of the convention creation and the upcoming impact of the rapid development of technologies in order to aim for such convention to be a future customary norm.

CONCLUSION

The IHL is primarily focused on the confinement of the humanitarian outcomes in the armed conflicts with the help of the restrictions on the means and methods of warfare. Besides, the law of armed conflicts endeavours to ensure protection against the perils of armed conflicts for the civilians, prisoners of war, injured military personnel, and also civilian objects, in assistance of its main three principles: the principle of distinction, the principle of proportionality and necessity. Consequently, the IHL regulations must be strictly pursued during the armed conflict by the parties to such conflict so as to receive minimal damage as a result of the military collisions.

In reference to Information warfare and its IO, the application of the IHL's regulations, customs and norms are hindered due to the emergence of IO's new elements with the rapid technological development. The IO is a multidimensional paradox, the complexity of which is connected to the location of its army objectives and elements in the traditional physical, cyber-connected symbolic and cognitive domains, also because of its major non-kinetic consequences during the armed conflict. As a result, there are several issues in the distinguishing the military targets, namely, defining military personnel, due to the inability to define those who are involved in the symbolic and cognitive domains of the cyber element (for instance, social media) and military objectives, because of growing interconnectivity between the military and civilian information resources (use of social media for the military purposes) in Information warfare domains. The above-presented issues open the need for the discussion on the application of the IHL towards Information warfare and its potential enhancement in the regulation of IO.

The previously presented hypothesis of this research constitutes that there are conceptual factors that preclude the application of the Law of Armed Conflict to the doctrine of information operations in times of military hostilities. Considering the existence of the major problems in the interpretation of the IHL's main fundamental concepts in the context of Information warfare, also the focus of the existing Law of Armed Conflict on the direct physical disruption of military objectives and personnel, which could be easily avoided in the information operations, one can

conclude that the initial research hypothesis was proved in the sequence of the discussions in the chapters above on the main concepts in the regulation of operations under IHL.

Consequentially, apart from the traditional conventional regulation being applicable to the physical domain and partially symbolic (cyber element) domains of the IO, the proposal for the potential regulation of the problem was presented in the form of the new internationally binding legislative framework-convention, where the concepts of the 'attack', should be reconsidered with the regards to the influential IO range in the cognitive and symbolic domains. This will enhance the applicability of the principles of distinction, proportionality and military necessity towards Information warfare. In the interim, the definitions for the concepts of 'severe suffering' and 'spread of terror' are proposed to be reviewed upon the technological realities of IO, thus, a new threshold should be defined for the IO act and its consequences to amount to the above-mentioned concepts in order to be regulated under IHL.

There should be a thorough reconsideration of the IHL in accordance with the modern challenges to prevent unwanted and unessential, avoidable consequences for the state and its civilians during the armed conflict, which will hinder further development and well-being of the society.

LIST OF REFERENCES

Scientific Books:

1. Alberts, D. S. (1996). *Defensive information warfare*. Defense Technical Information Center. National Defense University Washington DC, USA: NDU Press Book.

2. Armistead, L. (Ed.) (2011). *Information operations: Warfare and the hard reality of Soft Power* (1st ed.). Joint Forces Staff College (U.S.), National Security Agency/Central Security Service. Washington DC, USA: Potomac Books, Inc.

3. Fleck, D. (Ed.). (2021). *The Handbook of International Humanitarian Law* (4th ed.). Oxford, United Kingdom: Oxford University Press.

4. Marcellino, W., Smith, M. L., Paul, C., Skrabala, L. (2017, January 1). *Monitoring Social Media: Lessons for Future Department of Defense Social Media Analysis in support of information operations*. Rand National Defense Research Inst Santa Monica Ca. Santa Monica, USA: Rand Corporation.

5. Melzer, N. (2016). *International humanitarian law: A comprehensive introduction.* Geneva, Switzerland: International Review of the Red Cross, ICRC.

6. Schmitt, M. N. (Eds.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, United Kingdom: Cambridge University Press.

7. Schmitt, M. N. (Eds.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, United Kingdom: Cambridge University Press.

8. Waltz, E. (1998). *Information warfare: Principles and operations*. Boston, USA: Artech House.

Scientific Articles:

9. Agrell, Wilhelm (1987) Offensive Versus Defensive: Military Strategy and Alternative Defence. *Journal of Peace Research*, 24 (1), 75–86.

10. Araźna, M. (2015). Conflicts of the 21st century based on multidimensional warfare – "hybrid warfare", disinformation and manipulation. *Security and Defence Quarterly*, 8 (3), 103-129.

11. Bakshi, B. (2018). Information Warfare: Concepts and Components. *International Journal of Research and Analytical Reviews*, 5 (4), 178-185.

12. Brazzoli, M. S. (2007). Future prospects of information warfare and particularly psychological operations. In L. L. Roux (Author), *South African Army Vision 2020: Security challenges shaping the future South African Army* (217-235). Pretoria/Tshwane, South Africa: Institute for Security Studies.

13. Carter, R. M. (1998). The Information Operations Coordination Cell-Necessary for Division Offensive Actions?. *School Of Advanced Military Studies United States Army Command and General Staff College Fort Leavenworth*, (98-99), 1-58.

14. Deka, R. K., Kalita, K. P., Bhattacharya, D., Kalita, J. K. (2015). Network defense: Approaches, Methods and Techniques. *Journal of Network and Computer Applications*, 57, 71-84.

15. Doyle, M. P., Deckro, R. F., Kloeber, J. M., Jackson, J. A. (2000). Measures of Merit For Offensive Information Operations Courses of Action. *Military Operations Research*, 5 (2), 5–18.

16. Droege, C. (2012). Get off my cloud: Cyber warfare, international humanitarian law, and the protection of civilians. *International Review of the Red Cross*, 94 (886), 533–578.

17. Haslam, E. (2000, December 1). Information warfare: Technological changes and international law. *OUP Academic*. *Oxford University Press*, 5 (2), 157-175.

18. Hoffman, F.G. (2009). Hybrid Warfare and Challenges. Joint Forces Quarterly. *NDU Press*, 52. Washington, 34-39.

19. Hollis, D. B. (2007). Why States Need an International Law for Information Operations. *Lewis & Clark Law Review*, 11 (2008-43), 1023-1046.

20. Hutchinson, W. K., Warren, M. (2017). Attack and defence. In *Information warfare: Corporate attack and Defence in Digital World* (1st ed., 82-89). London; New York: Routledge.

21. Jensen, E. T. (2017). The Tallinn Manual 2.0: Highlights and Insights. *Georgetown Journal of International Law*, 48 (3). 735-778.

22. Khaldarova, I., Pantti, M. (2016). Fake News. The narrative battle over the Ukrainian conflict. *Journalism Practice*, 10 (7), 891–901.

23. Lahmann, H. (2020). Protecting the global information space in times of armed conflict. *International Review of the Red Cross*, 102 (915), 1227–1248.

24. Nichiporuk, B., Marshall, A. W. (1999). U.S. Military Opportunities: Information-Warfare Concepts of Operation. In Z. M. Khalilzad, J. P. White (Eds.*), Strategic Appraisal: The Changing Role of Information in Warfare* (1st ed., 179–216). RAND Corporation.

25. Quénivet, N. (2010). The “War on Terror” and the Principle of Distinction in International Humanitarian Law. *ACDI Anuario Colombiano De Derecho Internacional*, 3, 155-186.

26. Roche, J. (2010). Offensive information operations: a key enabler for the land force. *Australian Army Journal*, 7 (3), 169–182.

27. Schmitt, M. N. (2002). Wired warfare: Computer network attack and jus in Bello. Revue *Internationale De La Croix-Rouge/International Review of the Red Cross*, 84 (846), 365–399.

28. Stahn, C. (2006) 'Jus ad bellum', 'jus in bello'. . . 'jus post bellum'? –Rethinking the Conception of the Law of Armed Force. *European Journal of International Law*, 17 (5), 921–943.

29. Taddeo, M. (2019). Just information warfare. *Ethics and Policies for Cyber Operations*, 124, 67–86.

30. Tsybulenko E., Kajander A. (2021) The Hybrid Arsenal of Russia's War Against the Democratic World. In: H. Mölder, V. Sazonov, A. Chochia, T. Kerikmäe (eds) *The Russian Federation in Global Knowledge Warfare*. (173-194). Contributions to International Relations. Cham, Switzerland: Springer.

31. Tsybulenko E., Tetera, I. (2021) Occupation of Crimea and military invasion of Donbas: International law and responsibility of the Russian Federation. In: Lodyn, P. (ed) Surviving near the empire: Price of the modern Kremlin's aggression. (152-182), Ivano-Frankivsk, Ukraine: GOTsPND/IWP.

32. Tsybulenko, E., Platonova, A. (2019). Violations of Freedom of Expression and Freedom of Religion by the Russian Federation as the Occupying Power in Crimea. *Baltic Journal of European Studies*, 9 (3 (28)),134−147.

33. Vadnais, D. M. (2012). Law of armed conflict and information warfare-how does the rule regarding reprisals apply to an information warfare attack? *United States: BiblioScholar*, 97 (3), 1-27.

34. van Niekerk, B., Maharaj, M. (2009). The Future Roles of Electronic Warfare in the Information Warfare Spectru. *Journal of Information Warfare*, 8 (3), 1–13.

35. Waltz, D., (1998). The Critical Role of Cognitive Models in Next-Generation Intelligence Architectures, In: Proc. of 8th Annual AIPA Symp., Washington DC, 20-32.

36. Waters, G., Ball, D., Dudgeon, I. (2008). Information Warfare: Attack and Defence. In *Australia and Cyber-warfare* (33–58). ANU Press.

EU and International Legislation:

37. Convention (IV) respecting the Laws and Customs of War on Land and its annex: Regulations concerning the Laws and Customs of War on Land, The Hague, 18 October 1907.

38. Charter of the United Nations, 26 June 1945.

39. Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 18 June 1977.

40. Rome Statute of the International Criminal Court, 17 July 1998.

Other Sources:

Web materials:

41. Brandt, J., Pita, A. (2022, March 3). *How is Russia conducting Cyber and Information Warfare in Ukraine?* Brookings. Retrieved from https://www.brookings.edu/podcast-episode/how-is-russia-conducting-cyber-and-information-warfare-in-ukraine/, 9 April 2022.

42. Choudhary, V. (2021, August 9). *The truth under siege: Does international humanitarian law respond adequately to information warfare?* Groningen Journal of International Law. Retrieved from https://www.grojil.org/blog2/2019/03/21/the-truth-under-siege-does-international-humanitarian-law-respond-adequately-to-information-warfare, 9 April 2022.

43. Ghia, U. (2018, December 17). *International humanitarian law in a Post-Truth World*. Cambridge International Law Journal. Retrieved from http://cilj.co.uk/2018/12/17/international-humanitarian-law-in-a-post-truth-world/, 11 March 2022.

44. Henkhaus, L. (2022, April 15). *The role of the internet in Ukraine's Information War.* Texas A&M Today. Retrieved from https://today.tamu.edu/2022/03/14/the-role-of-the-internet-in-ukraines-information-war/, 16 April 2022.

45. *Legality of the Threat or Use of Nuclear Weapons,* Advisory Opinion (1996, July 8), ICJ. Retrieved from https://www.icj-cij.org/files/case-related/95/7497.pdf, March 2022.

46. *Military necessity.* Military Wiki. (n.d.). Retrieved from https://military-history.fandom.com/wiki/Military_necessity#CITEREFMoreno-Ocampo2006, 10 April 2022.

47. *What is International Humanitarian Law?* (2004). Advisory Service on International Humanitarian Law, ICRC. Retrieved from https://www.icrc.org/en/doc/assets/files/other/what_is_ihl.pdf, 11 March 2022.

Graduation Thesis:

48. Winther, P. (2019). *International Humanitarian Law and Influence Operations: The Protection of Civilians from Unlawful Communication Influence Activities during Armed Conflict.* (PhD dissertation). Acta Universitatis Upsaliensis, Swedish Defence University, Department of Security, Strategy and Leadership (ISSL), Centre for International and Operational Law. Department of Law, Uppsala University, Sweden.

Reports:

49. Theohary, C. A. (2021). Defense Primer: Cyberspace Operations. Washington, D.C: Congressional Research Service. CRS In Focus, IF10537, 1-3.

50. Institute for the Study of War. (2022). Ukraine: CONFLICT UPDATE 19. Institute for the Study of War. Critical Threats Project, AEI. 19, 1-10.

51. Waltz, E. (2001, January 1). Data Fusion in offensive and defensive information operations. Defense Technical Information Center, ADA400192, 1-15.

Letters:

52. Moreno-Ocampo, L. (2006). OTP letter to senders re Iraq. International Criminal Court.

APPENDICES

Appendix 1. Non-exclusive licence

A non-exclusive licence for reproduction and publication of a graduation thesis[1106]

I _____ (*author's name*)

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis
_____
_____
_____,
(*title of the graduation thesis*)

supervised by_____,
(*supervisor's name*)

1.1 to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;

1.2 to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.

2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.

3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

_____ (date)

[106] *The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.*