ABUSE OF CYBERSPACE WITHIN THE CRISIS IN UKRAINE

Jozef Valuch,* Ondrej Hamuľák**

Abstract: *The cyber sphere forms a fifth domain of activities were interactions between state and non-state actors could happen. It starts to play an important role within the conflicts and hostilities. Especially in these situations, international society does not have a unified view on the question how to deal with the activities in cyberspace. We could see the different forms of abuse of cyberspace also within the crisis in Ukraine. This crisis is a good example of the complexity of the legal approach and the (non)capability of the legal understanding of cyber operations and attacks. The goal of this article is to highlight this complexity and to determine the status of cyber incidents realized in the Ukraine from the perspective of international law.*

Keywords: *Ukraine, crisis, conflict, cyberspace, international law*

INTRODUCTION

It is possible to observe the crisis in Ukraine from multiple angles. One may focus on the events on the Kyiv's "Maidan", the annexation of Crimean peninsula by the Russian Federation, the hybrid war and deployment of Russian troops in Ukraine Donbass area,[1] the EU sanctions against Russia etc. from the view of international politics, international relations, security and global studies, and of course the international law. In addition, observations and opinions on that crisis vary among several scholars, state leaders and representatives of international organizations. When we opt for the optic of contemporary international law, we shall find out that the evaluation and analysis of this complex crisis is considered as very complicated and controversial.[2]

In this article, we focus on a very narrow and particular question within the multifaceted topic of crisis in Ukraine. Hereafter we devote particular attention to the use of cyberspace during the conflict from the perspective of international law.

We use the term "crisis", as we are trying to elucidate the situation in Ukraine in wider context. It has several political, legal and sociological branches. Even in the light of international law, one may focus on the law of arm conflicts, humanitarian law, human rights law[3] and other perspectives. The abuse of cyberspace in connection to the situation in this country has taken place not only during the armed conflict (that persists), but also outside this conflict and therefore needs more complex analysis.

* JUDr. Jozef Valuch, Ph.D., Faculty of Law, Comenius University in Bratislava, Bratislava, Slovak Republic
** JUDr. Ondrej Hamuľák, Ph.D., Faculty of Law, Palacký University Olomouc, Olomouc, Czech Republic and Visiting Professor in Implementation of EU law, School of Business and Governance, TTU Tallinn, Tallinn, Estonia

[1] TSYBULENKO, E., PAKHOMENKO, S. The Ukrainian Crisis as a Challenge for the Eastern Partnership. In: Kerikmäe, T., Chochia, A. (eds.). *Political and Legal Perspectives of the EU Eastern Partnership Policy*. Switzerland: Springer, 2016, p. 168.

[2] BÍLKOVÁ, V. Mezinárodněprávní aspekty vývoje na Krymu [International law aspects of the develoments in Crimea]. *Working Papers České společnosti pro mezinárodní právo* [CSIL Working Papers]. 2014, Vol. 1, No. 1, p. 1.

[3] At the same time, there is a danger that the label of "human rights" can be misused by interest groups in the case of new phenomena such as cyberspace related legal rights or duties. See: KERIKMÄE, T., NYMAN METCALF, K. Less is more or more is more. Revisiting Universality of Human Rights. *International and Comparative Law Review*. 2012, Vol. 12, No.1, p. 17.

The purpose of our research is to define the nature and legal concept of cyber operations in Ukraine. We also seek to approach and deploy the relevant international law issues that arise in connection with the definition of these cyber operations. At the same time, however, we are aware that the view on the nature of these operations and their definition as well as the analysing of the conflict itself evolves and depends on the available data and information sets.

I. CYBERSPACE AND INTERNATIONAL LAW

Cyberspace is flexible and variable, simple and accessible to wide masses. Nevertheless, all its advantages give rise to wide range of malicious intents and opportunities. Cyberspace is a new universe for information criminality and cyber threats of a different rank of gravity (hackers' attacks, cyber espionage, DDoS (Distributed Denial of Service) attacks, propaganda and the dissemination of wrong or dangerous information, internet fraud, the misuse or abuse of personal data etc.). The current threats are coming from a wide range of entities including hackers, hacktivists (ideologically motivated hackers), states, criminal or terrorist groups with variant technical resources and background. The common feature of all cyber attacks is the complicated process of identifying the real source of them.[4] With relevant skills and with the appropriate technology (which is now quite accessible without requiring a big investment) it is possible to cause serious threats and immense damage even to the states that have modern and big conventional forces. The character and "opportunities" of cyberspace blurred the distinction between the traditional threat actors – hackers, terrorists, organised criminal networks, industrial spies and foreign intelligence services[5] and therefore complicates also the identification of the attacker.[6]

The complexity of cyberspace itself gives rise to the different views on the content of this domain. The common feature of particular definitions of cyberspace is the multilayer approach to its content. According to some views cyberspace composes of three layers – the physical (composed of hardware, satellites, cables and other technical equipment), the syntactic (software, applications and operating systems) and semantic layer (which includes concrete information, human activities, considerations and judge-

[4] MELKOVÁ, M., SOKOL, T. Kybernetický priestor ako nová dimenzia národnej bezpečnosti (Cyberspace as the new dimension of national security). In: *Bezpečnostné fórum 2015. I. zväzok*. Banská Bystrica: Vydavateľstvo Univerzity Mateja Bela - Belianum, 2015, p. 57. See also: KRAMER, D. F., STARR, H. S., WENTZ, L., KUEHL, D. *Cyberpower and National Security*. National Defense University, Dulles Virginia: Potomac Books Inc., 2009, p. 664.

[5] AUSTRALIAN GOVERNMENT. Australian Cyber Security Strategy. In: *Australian Government* [online]. 2009 [2017]. Available at: <https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf>. At this point, it is appropriate to point to the difference between the national level of cybercrime regulation and cyber security (or cross-border cooperation in these fields) on the one hand and cyber security within an armed conflict which is regulated by international law standards on the other hand. However, the first area is not the subject of this article and therefore we do not focus on it more closely.

[6] ROSCINI, M. *Cyber Operations and the Use of Force in International Law*. Oxford: Oxford University Press, 2014, pp. 1–2. See also: Australian Cyber Security Strategy 2009, p 3.

ments).[7] Another view works also with the three-layer structure, but it distinguishes (more technically) the hardware layer, software layer and data layer. In all cases, all three layers (separately or as a whole) could stand as the target of cyber attacks.[8]

Not all cyber operations could be considered as cyber attacks. The definitions of cyber attacks opt for a more narrow approach. According to the so-called Tallinn Manual:[9] "A cyber attack is a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects". This classification has a significant importance especially in connection with the restrictive notion of "attack" in the law of armed conflicts. The general restriction that civilians and objects of a civilian nature shall not be subject to attacks is valid also in the domain of cyberspace.[10] On the other side, the Tallinn Manual accepts a cyber attack in the case of those, who are not civilians, specifically members of the armed forces, members of organized armed groups, civilians taking a direct part in the hostilities; and in an international armed conflict, participants in levée en masse.[11] In defining the notion of "attack" the Tallinn Manual refers to the First Additional Protocol to the Geneva Convention, which defines attack in article 49 para 1 as an "act or acts of violence against the adversary, whether in offence or defence". The violence here is determined by the results of the act. The use of violence against a target distinguishes attacks from other military operations.[12] Therefore, non-violent operations such as psychological cyber operations or cyber espionage are not qualified as cyber attacks.[13] In connection to that, we must deal with the question, whether cyber operations could be determined as the use of force in the meaning of international law. The prohibition of threat or use of force is part of the cogent norms of international law. According to the UN Charter, this prohibition relates to "attacks" on territorial integrity or political independence of any state but also to any other conduct inconsistent with the Purposes of the United Nations.[14] In this respect, according to the Tallinn Manual

[7] SHELDON, J. B. Cyberwarfare: The Invisible Threat. In: *Encyclopaedia Britannica, Book of the Year 2011*, pp. 182–183. Available also at: <https://www.britannica.com/topic/cyberwar>. See also: MRÁZEK, J. Mezinárodní právo v kybernetickém prostoru [International law in the cyberspace]. *Právník*, 2014, Vol. 153, No. 7, p. 541.

[8] TOBANKSY, L. Basic concepts in cyber warfare. *Military and Strategic Affairs*. 2011, Vol. 3, No. 1, pp. 75, 77–78. See also: TSAGOURIAS, N., BUCHAN, R. (eds.). *Research Handbook on International Law and Cyberspace*. London: Edward Elgar, 2015, p. 15. Available also at: <http://www.e-elgar.com/shop/eep/preview/book/isbn/9781782547396/>.

[9] Tallinn Manual On The International Law Applicable To Cyber Warfare Prepared By The International Group Of Experts At The Invitation Of The Nato Cooperative Cyber Defence Centre Of Excelence (Hereafter Recalled As "Tallinn Manual"), Rule 30.

[10] Tallinn Manual, Rule 32: "The Civilian Population As Such, As Well As Individual Civilians, Shall Not Be The Object Of Cyber Attack"; Rule 37 "Civilian Objects Shall Not Be Made The Object Of Cyber Attacks. Computers, Computer Networks And Cyber Infrastructure May Be Made The Object Of Attack If They Are Military Objectives."

[11] Tallinn Manual, Rule 34.

[12] BRUNER, T. K podmínkám a způsobu aplikace mezinárodního humanitárního práva na kybernetické operace [Conditions and ways of application of international humanitarian law in connection to cyber operations]. In: Bílková, V. (ed.). *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy* [International humanitarian law - the basis, developments and challenges]. Praha: Univerzita Karlova v Praze, Právnická fakulta, 2015, p. 161.

[13] Tallinn Manual, Rule 30 (2).

[14] UN Charter art. 2 (4): "All Members Shall Refrain In Their International Relations From The Threat Or Use Of Force Against The Territorial Integrity Or Political Independence Of Any State, Or In Any Other Manner Inconsistent With The Purposes Of The United Nations."

"a cyber operation constitutes a use of force when its scale and effects are comparable to a non-cyber operation rising to the level of a use of force".[15] In an attempt to determine, when cyber operations could be understood as a use of force in the meaning of article 2/4 of the UN Charter, we may recall the Nicaragua case.[16] The use of the ICJ findings for the purpose of cyberspace leads us to the conclusion that key factors are the effects and extent of the cyber operations. In this meaning the non-destructive cyber operations, like the attacks on the confidence of the national government could not be determined as attacks with the use of force.[17] On the other hand, this does not mean, that cyber operations which do not included the use of force are in harmony with international law. They could be covered by other international law rules, e.g. the prohibition of intervention, which forms part of the principle of the sovereign equality of states (article 2/1 of the UN Charter). The prohibition of intervention is also part of customary international law[18] and according to ICJ the non-intervention principle "forbids all states or groups of states to intervene directly or indirectly in the internal or external affairs of other states".[19]

In relation to cyber operations, we must point also at the analysis of Michael Schmitt, according to which "economic and political coercion can be delimited from the use of armed force by reference to various criteria."[20] "Professor Schmitt recognized that discerning the use-of-force threshold is really about predicting how states will characterize and respond to cyber incidents in light of prevailing international norms … his model consists of seven factors that represent the major distinctions between permissible (that is, economic and political) and impermissible (armed) instruments of coercion. When applying these factors, the more closely the attributes of a cyber operation approximate the attributes of armed force, the more likely states are to characterize the operation as a prohibited use of force."[21] Following criteria results from the Schmitts' analysis: Severity, Immediacy, Directness, Invasiveness, Measurability, Presumptive legitimacy and Responsibility. "According to Professor Schmitt, evaluating these factors is an imprecise and subjective endeavor. The factors are useful but not determinative, and they should not be applied mechanically. Rather, they need to be applied holistically according to the relevant context—that is, which factors are important and how they should be weighted will vary on a case-by-case basis."[22]

Relation between cyber attacks and rules on *ius ad bellum* and *ius in bello* was significantly covered by the work of the International Group of Experts at the Invitation of the NATO Cooperative Cyber Defence Centre of Excellence, which prepared the abovemen-

[15] Tallinn Manual, Rule 11.
[16] Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States), I.C.J. 1984 I.C.J. 39.
[17] ŠMIGOVÁ, K. Kybernetické útoky a medzinárodné právo [Cyber attacks and international law]. In: *Bratislavské právnické fórum 2013*. Bratislava: Univerzita Komenského, Právnická fakulta, 2013, p. 1226.
[18] Nicaragua v. United States, p. 202.
[19] Tallinn Manual, Rule 10 (6, 7). See also: Nicaragua v. United States, p. 205.
[20] SCHMITT, M. N. Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework. *Columbia Journal of Transnational Law*. 1998-9, Vol. 37, p. 914. Available at: <https://ssrn.com/abstract=1603800>.
[21] FOLTZ, A. C. Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force" Debate. *JFQ*. 2012, No. 67, p. 42–43. Available at: <http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf>.
[22] Ibid, p. 43.

tioned Tallinn manual in 2012. This manual covers in its two parts questions of cyber security (and *ius ad bellum*) as well as questions of armed conflicts (and *ius in bello*).[23] Although this document is only a non-binding research outcome of the expert group, it is inspiring and has a significant impact on the developments in the field of cyber law.

Currently there is quite a wide acceptation of the applicability of international law rules on the activities within cyberspace. It is confirmed by academia and as well as international organisations. For example, NATO clearly recognises the impact of general international law and international humanitarian law in the cyber-sphere.[24] Cyber security and potential threats in the field of information and communication technologies form also the stabile part of the UN agenda. Since 1998 annual reports are presented by the Secretary-General to the General Assembly on the ICT questions and international security. Additionally four Groups of Governmental Experts - GGE (2004, 2009, 2011 and 2014; composed of representatives of 15, respectively 20 countries, including the USA, Russia and China) were created to deal with the questions of cyber security, threats in cyberspace and developments in this field. All of these expert groups confirmed the necessity of applying international law rules and especially the UN Charter to gain peace and stability and to support open, safe, accessible and peaceful space of information and communication technologies. A significant contribution to the development of these questions was made by the fourth GGE. In its report from June 2015, GGE presented the set of norms, rules and principles applicable to the activities of States in the cyberspace. The set of norms covered a wide range of questions of how international law shall deal with the ICT problems. The UNODA summary of this report denote to these key principles presented by the GGE:

- In their use of ICTs, States must observe, among other principles of international law, State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.
- Existing obligations under international law are applicable to the State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms.
- States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts.
- The UN should play a leading role in promoting dialogue on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour.[25]

The identification of the main principles and attempt to present some general rules is very important, but still insufficient due to the lack of binding force. There is a crucial open question on the applicability of these rules in practice. Another problem arises in

[23] GÁBRIŠ, T. *Cyber Law*. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2014, p. 174.

[24] "Our policy also recognises that international law, including international humanitarian law and the un charter, applies in cyberspace." Wales summit declaration (issued by the heads of state and government participating in the meeting of the North Atlantic Council in Wales), 5 September 2014, Para 72.

[25] UNODA. Developments in the field of information and telecommunications in the context of international security. In: *UNODA – United Nations Office for Disarmament Affairs* [online]. 2015 [2017]. Available at: <https://www.un.org/disarmament/topics/informationsecurity/>.

connection to the promoted applicability of general international law norms on the particular features of cyberspace.[26]

It is clear that in the case of absence of specific rules we must look for the solutions in general international law. However, here the biggest problems lay in the (non)transferability of the classical notions to the cyberspace specifics. For example, the concepts of jurisdiction or the notion of state accountability for some conduct is so general that their applicability *vis-á-vis* indeterminate cyberspace features is misconceived and almost impossible. Also the applicability of the concept of due diligence approved by the ICJ in the *Corfu Channel Case*[27] may bring some doubts. When we'll accept the wide understanding of the notion of state territory including also the infrastructure for ICT posted on it, then we could use the due diligence principle even in connection with cyberspace.[28] On the other hand, we must always count with the special character of the cyber sphere using the global networks and causing particular difficulty in searching the source of concrete operations and attacks. Another problem in connection to cyberspace is the non-existence of stabile international executive structures, which would deal with its specifics. If we'll connect the abovementioned inconsistencies with the principle of the autonomy and freedom of choice for all states (in situations where there is no international rule prescribing or prohibiting some conduct), we must deal with the risk of fragmentation and the disability of the international community to govern cyberspace effectively. For all these reasons, cyberspace represents one of the most visible challenges to contemporary international law.[29]

II. THE ABUSE OF CYBERSPACE DURING THE CRISIS SITUATION IN UKRAINE

The crisis in Ukraine is far from being the first example of cyberspace abuse for some harmful operations. The fears and doubts about misuse and the exploitation of this virtual sphere are present from the very early times of internet.[30] The attacks and examples of malpractice appeared in numerous examples. They targeted governmental webpages, webpages of defence and security administrations, banks and financial institutions, media and press houses etc. And the numbers of these threats are growing perpetually.[31]

---

[26] STINISSEN, J. A Legal Framework for Cyber Operations in Unkraine. In: Geers, K. (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015, p. 124.

[27] Corfu Channel Case (U.K. v. Albania), I.C.J. Reports 1949. See further: BUCHTA, T., SÝKOROVÁ, M. *Najdôležitejšie rozsudky v medzinárodnom práve verejnom* [The most important cases in public international law]. Bratislava: C. H. Beck, 2016, pp. 13–14.

[28] ZIMMERMANN, A. International Law and 'Cyber Space'. *ESIL Reflections: European Society of International Law*. 2014, Vol. 3, No. 1.

[29] Ibid. See also: VRŠANSKÝ, P., BEDNÁR, D. Cyber Security and the International Law. *Bratislava Law Review*. 2017, Vol. 1, No. 2, pp. 38–49.

[30] KERIKMÄE, T, SÄRAV, S. *Normative Challenges of e-technology. New Paradigms for Valid Reasoning. Research Handbook in Law and Logic*. Duncker & Humblot, 2017.

[31] O'CONNELL, M. E., ARIMATSU, L., WILMSHURST, E. *Cyber Security and International Law. International Law: Meeting Summary*. London: Chatham House, 2012. Available at: <https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf>.

The crisis in Ukraine has evolved through several phases where more or less relevant events occurred: at the end of 2013 and the beginning of 2014 – the refusal to sign the association agreement between Ukraine and the European Union, as crucial part of the EU Eastern partnership Policy,[32] by president Yanukovych and the rise of a mass wave of anti-government protests in Kiev; March 2014 – the declaration of independence of the Republic of Crimea and the annexation of the Crimea by the Russian federation; April/May 2014 – elevation of armed conflict in the eastern parts of Ukraine; perpetual sanctions against Russia, peace and cease fire negotiations and the continuation of attacks in 2016[33] and 2017. From the very beginning of the conflict all, the protests, riots, armed actions and other kinetic acts were accompanied by cyber operations of a different nature and relevance. The threats that this cyber incidents brought are all the more serious because Ukraine belongs among the vulnerable countries in terms of cyber security. According to the Global Cybersecurity Index & Cyberwellness Profiles, April 2015, which reflects the countries readiness in connection to cyberspace and ICT risks, Ukraine is in17th position, however because one position could be held by several states in fact sixty-five countries were ahead of Ukraine.

The cyber incidents that occurred within the crisis in Ukraine are very wide and includes DDoS; website defacements; cyber espionage tools have been discovered in Ukraine and in NATO countries; new and more menacing forms of malware include Turla/Uroburos/Snake, RedOctober, MiniDuke, etc; cyber attacks against opposition servers, smartphones, websites, and internet accounts; continuously leak stolen sensitive information;[34] attacks target the mobile devices of Ukrainian parliament members; cyber attacks against the Ukrainian Central Election Commission on May 2014 (to undermine the credibility of the elections and present false election results); eastern Ukraine has been isolated from the rest of Ukraine via internet censorship and regular forensic checks on citizens' computers and mobile devices;[35] etc.

There is an important question how to deal with these cyber activities, which occur in clear connection to the ongoing conflict, and whether it is possible to include these cyber operations under the umbrella of international law of armed conflicts. The answer to this question depends on the gravity of their consequences. In the case, where a cyber operation gives rise to injuries, deaths, damage or destruction, the law of armed conflicts should

[32] See KERIKMÄE, T., CHOCHIA, A. (eds.). *Political and Legal Perspectives of the EU Eastern Partnership Policy*. Springer International Publishing, 2016, or: ŠIŠKOVÁ, N. et al. *From Eastern Partnership to the Association: A Legal and Political Analysis*. Newcastle: Cambridge Scholars Publishing, 2014.

[33] To the question of abuse of force in the context of development of relations between Russia and Ukraine see VRŠANSKÝ, P. Analýza právnej úpravy použitia sily v medzinárodnom práve v kontexte vývoja vzťahov medzi Ruskom a Ukrajinou [Analysis of the law on the use of force in international law in the context of the development of relations between Russia and Ukraine]. *Acta Facultatis Iuridicae Universitatis Comenianae*. 2014, Vol. 33, No. 1, pp. 106–137; or BEDNÁR, D. Súkromné vojenské a bezpečnostné spoločnosti - novodobé žoldnierstvo alebo legálne nadnárodné podnikanie v oblasti ozbrojených konfliktov? [Private military and security companies - modern mercenaries or legal transnational entrepreneurship in armed conflicts?]. *Právník*. 2016, Vol. 155, No. 1, pp. 80–92.

[34] GEERS, K. (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015, p. 11.

[35] Ibid.

apply. This may occur for example in the case when one country would start cyber operations against another country with the aim of destroying the critical infrastructure: like civil aviation control or national grids, what would lead to the disfunctioning of aircrafts and to consequent injuries, damage and deaths. When we take into considerations the consequences, there is no space for a distinction between conventional weapons and cyber operations.[36] It is clear from the abovementioned Tallinn Manual that "cyber operations executed in the context of an armed conflict are subject to the law of armed conflict".[37]

The question now is how these conclusions affect the evaluation of the situation in Ukraine. Here it is important to mention, that all members of the expert group that worked on the Tallinn Manual unanimously accorded with the necessity of the existence of a nexus between cyber activities and armed conflict. On the other side, they had disputes about the level and nature of this prescribed nexus. According to one group of experts, the law of armed conflicts is applicable to all cyber operations carried out by one side of the armed conflict against the enemy. According to the other group, only the operations undertaken in furtherance of the hostilities, that is, in order to contribute to the originator's military effort, could be included under the regulation of armed conflicts.[38] These activities are interconnected to other military (hostile) operations against the enemy, but at the same time, they alone are the acts of hostility.[39] Here, we are facing one of the stumbling-blocs within the evaluation of the nature of cyber incidents realized in Ukraine. The nexus between these incidents and the conflict itself could be considered as disputable and could give rise to some open doubts.

Another important relevant circumstance is the question of accountability. In connection to cyber incidents, this notion is one of the most challenging. Cyberspace is open, flexible, full of actors, simple to enter and leave and anonymous. The determination of responsible actors in the case of cyber operations is therefore very complicated. It raises many intertwined questions:

Who performed the cyber operation and on what basis?

If it is a non-state actor, is there any support or management by the State?

If so, what is the level of State involvement or support?[40]

Moreover, we must always count on the risk of the false use or misuse of devices, sources and connections of innocent owners by the cyber attackers.

---

[36] O'CONNELL, M. E., ARIMATSU, L., WILMSHURST, E. *Cyber Security and International Law. International Law: Meeting Summary*. London: Chatham House, 2012, p. 10. Available at: <https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf>.

[37] Tallinn Manual, Rule 20.

[38] Tallinn Manual, Rule 20 (5).

[39] BRUNER, T. K podmínkám a způsobu aplikace mezinárodního humanitárního práva na kybernetické operace [Conditions and ways of application of international humanitarian law in connection to cyber operations]. In: Bílková, V. (ed.). *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy* [International humanitarian law - the basis, developments and challenges]. Praha: Univerzita Karlova v Praze, 2015, p. 160.

[40] See O'CONNELL, M. E., ARIMATSU, L., WILMSHURST, E. *Cyber Security and International Law. International Law: Meeting Summary*. London: Chatham House, 2012, p. 11. Available at: <https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf>.

III. THE NATURE OF THE CONFLICT IN UKRAINE

The situation in Ukraine is described as a hybrid warfare situation. It is a mixture of non-conventional tactics and strategies, secret operations, cyber activities, the operation of irregular forces and political manipulations. One of the goals of all these mixed strategies is the attempt to avoid military reprisals. The activities are performed in a way and extent, which try not to encroach the boundaries of the definition of the use of force. Here the static actions have the same importance as the classical kinetic attacks. Conventional warfare is only one part of the broad set of actions[41] performed by not only the states but also non-state actors. Cyber operations are capable of producing comparable effects to kinetic weapons and their advantage is also their informational potential. These operations are able to manipulate public opinion and decision-making. They are aimed mostly at causing political and psychological effects, data manipulation and to influence the knowledge and opinions rather than at physical damage and injuries. In addition, they bring the advantage on the one side of the conflict in the form of the uncertainty and doubts on the part of the enemy.[42]

According to some authors, "cyber activities conducted as part of a wider conflict are governed by that conflict's legal framework."[43] Therefore, it is important to determine the nature of the conflict itself. The crisis in Ukraine is mixed and is an evolutive conflict with different types of situations and views on their determination:

The original riots in Kiev's Independence Square could be determined as the demonstrations and violent clashes between the protesters and police, rather than a military (armed) conflict. This first phase belonged to the Ukrainian internal affairs though it gave rise to the consequent events that developed into the armed conflict. Therefore, we cannot determine this phase as the (international) armed conflict and it is hard to include any cyber operations that occurred in this time under the legal framework of the law of armed conflicts.

The secession of the Crimea from Ukraine and its connection to the Russian Federation does not find any support in the current international law.[44] It can therefore be determined as an occupation. The law of armed conflicts applies both in a situation of total and also partial occupation even if this occupation did not lead to armed resistance on the occupied territory.[45] Occupation is a hostile substitution of territorial power and authority, what exactly fits with the situation in the Crimea, where Russia performs territorial control without the consent of the Ukrainian Government.[46] The cyber operations related to this situ-

[41] LEWIS, J. A. Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine. In: Geers, K. (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015, p. 40.
[42] Ibid.
[43] STINISSEN, J. A Legal Framework for Cyber Operations in Unkraine. In: Geers, K. (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015, p. 124.
[44] BÍLKOVÁ, V. Mezinárodněprávní aspekty vývoje na Krymu [International law aspects of the develoments in Crimea]. *Working Papers České společnosti pro mezinárodní právo* [CSIL Working Papers]. 2014, Vol. 1, No. 1, p. 12.
[45] Geneva Conventions, 1949, Common Article 2.
[46] STINISSEN, J. A Legal Framework for Cyber Operations in Unkraine. In: Geers, K. (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015, p. 128.

ation could be determined as military operations under the legal regime of law of armed conflicts in its abovementioned broad understanding.

The situation in eastern Ukraine was determined by an International Committee of the Red Cross in 2014 as the non-international armed conflict,[47] which is defined as "armed conflict not of an international character occurring in the territory of one of the High Contracting Parties."[48] In addition, some academic writings support this approach. For example, professor Heinsch analysed the conflict in Ukraine from different perspectives (as an international armed conflict; a non-international armed conflict and an "internationalized" armed conflict) and came to the conclusion that at least some acts belonging to the second category occurred within the conflict.[49] Further development in understanding and defining of this conflict occurred in 2016, when the Office of the Prosecutor of the ICC stated that: "the information available suggests that the situation within the territory of the Crimea and Sevastopol amounts to an international armed conflict between Ukraine and the Russian Federation. This international armed conflict began at the latest on 26 February when the Russian Federation deployed members of its armed forces to gain control over parts of the Ukrainian territory without the consent of the Ukrainian Government. The law of international armed conflict would continue to apply after 18 March 2014 to the extent that the situation within the territory of Crimea and Sevastopol factually amounts to an on-going state of occupation. A determination of whether or not the initial intervention, which led to the occupation, is considered lawful or not is not required. For purposes of the Rome Statute an armed conflict may be international in nature if one or more States partially or totally occupies the territory of another State, whether or not the occupation meets with armed resistance."[50] Notwithstanding the fact, that Russia in not a party to the Rome Statue and (most likely as the reaction on the statement of the Office of Prosecutor) it withdrew from the process of accession to the ICC at the end of 2016.

We must point out that Russia firmly denies any responsibility or participation in the conducted or ongoing cyber operations. It's the fact, that most of the agents of cyber operations in the Crimea were non-state actors, e.g. the pro-Russian hackers group known as CyberBerkut. For further evaluation of the cyber operations conducted in connection with the conflict in Ukraine, it is crucial to determine the status of these agents. In the case where these agents would be the integrated part of the Russian military forces, we could easily determine them as the combatants. We could also determine them as the

[47] ICRC. Ukraine: ICRC calls on all sides to respect international humanitarian law. News Release 14/125. In: *International Committee of the Red Cross* [online]. 23. 07. 2014 [2017]. Available at: <https://www.icrc.org/eng/resources/documents/news-release/2014/07-23-ukraine-kiev-call-respect-ihl-repatriate-bodies-malaysian-airlines.htm>.

[48] Geneva Conventions, Common Article 3.

[49] HEINSCH, R. Conflict Classification In Ukraine: The Return Of The "Proxy War"? *International Law Studies*. 2015, Vol. 91, pp. 323–360.

[50] THE OFFICE OF THE PROSECUTOR (ICC). Report on Preliminary Examination Activities 2016. In: *International Criminal Court* [online]. 2016 [2017]. Available at: <https://www.icc-cpi.int/iccdocs/otp/161114-otp-rep-PE_ENG.pdf>. See pp. 35–36.

combatants in the situation when they would act as a part of the armed group belonging to one of the parties of armed conflict and if they would (a) act under commanded of a person responsible for his subordinates; (b) have a fixed distinctive sign recognizable at a distance; (c) carry the arms openly and (d) conduct their operations in accordance with the laws and customs of war. These are the key criteria to distinguish the combatants and civilians. It is more than clear, that any non-state hacker group, which are actively influencing the conflict in Ukraine, would not fulfil those criteria. They represent the virtual group, organised in the cyber sphere and communicating only via internet. They do not carry weapons and act anonymously, so no distinctive sign could be discovered. Therefore, we must determine them as civilians, but ones who (as the direct participators in the activities of fighting parties) lost the protection offered to civilians by the law of armed conflicts. In this situation, they might be also the target of any countermeasures by the opposite fighting party.[51]

IV. THE NATURE OF CYBER OPERATIONS

Another important issue in attempts to determine cyber operations in the light of international law is the notion of damage and injuries. Until now, we have not registered any grave destructive consequences of cyber operations within the conflict in Ukraine. Several DDoS attacks occurred during the fights in eastern Ukraine, there were some operations leading to the change of content of official webpages, some attacks also touched the fluency and operability of communication channels. Some internet sites of the Ukrainian government as well as some sites of the Ukrainian embassies abroad were affected by the spy software in order to gain access to secret information. Even though these operations complicated the operability of the state administration and endanger state security in a certain way, most of the authors point out, that they do not have any direct connection to the ongoing military conflict and mostly that they did not lead to any destructive consequences. Therefore, they refuse the applicability of international law of armed conflicts, respectively international humanitarian law, in connection to them.[52]

Even though it is hard to classify the cyber operations in Ukraine under the regime of the law of armed conflicts or humanitarian law, when we look at them from the wider perspective of international law, we may find some deteriorations. One option is to consider them as the acts against rules on the protection of diplomatic information and communication. According to rule no. 84 of the Tallinn manual, the diplomatic archives and communication are protected against cyber attacks in all cases. This rule has a basis in the Vienna Convention on Diplomatic Relations (1961) and the ICJ judgement in the Tehran

[51] STINISSEN, J. A Legal Framework for Cyber Operations in Ukraine. In: Geers, K. (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015, p. 132.

[52] BRUNER, T. K podmínkám a způsobu aplikace mezinárodního humanitárního práva na kybernetické operace [Conditions and ways of application of international humanitarian law in connection to cyber operations.] In: Bílková, V. (ed.). *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy* [International humanitarian law - the basis, developments and challenges]. Praha: Univerzita Karlova v Praze, 2015, pp 169–170.

case,[53] which understands the diplomatic relations as the "self-contained regime". We might find another example of the breach of international law rules, e.g. the principle of Non-interference in domestic affairs, within the Ukrainian conflict, especially in connection with the disruption of elections, of course under the condition that these disruptions were operated or supported by the foreign state power.[54]

Until the present day, most of the cyber operations in Ukraine were used in order to obtain strategic information and also as the part of the "information war" between the two sides of the conflict. There were no destructive consequences in connection to the key infrastructure and no elimination of warfare equipment. Therefore, we may conclude, that the operations instigated were not forbidden by or breaching the international rules on armed conflicts. Of course it would be a completely different situation if the cyber operations would have been involved or interconnected to the kinetic war operations.[55]

The cyber operations in Ukraine have had mostly the political and ideological effect. Their impact on the development and results of the conflict itself has not been so significant, especially when we compare them to the impact and consequences of establishing, support and military back up for the pro-Russian separatist groups in the Ukrainian territories with the outnumbered Russian speaking minority.[56] Of course, cyber operations could be used also for military purposes, but this is not the situation of Ukraine. To speak about the strategic or military impact of the cyber operations some concrete requirements must be fulfilled. They must have a destructive impact; they must be integrated to the existing military structures, doctrine, planning and operations.

It is more than clear, that Russia had an opportunity to penetrate through the Ukrainian ICT networks, which could present them with an important advantage in connection to tactics and planning the kinetic operations. On the other side, it is obvious, that this advantage was not used to its whole potential. According to some commentators, Russia used this opportunity to test the possibilities and potential of cyber operations in gaining political benefits.[57] Therefore, the negative damaging consequences were minimalised.

CONCLUSION

Cyberspace, often called the fifth domain for the performance of military operations, represents a big challenge for contemporary international law theory but also practice, as we may see in the Ukrainian example. The application of international law on the activities in

[53] United States Diplomatic And Consular Staff In Tehran Case (U.S. V. Iran), I.C.J. Reports, 1980, Paras. 61-62, 77, 86. See further BUERGENTHAL, T., MAIER, H. G. *Public International Law*. St. Paul: West Publishing, 1985, p. 210, or: VALUCH, J. *Diplomatické výsady a imunity: sloboda jednotlivca alebo prerogatíva štátu?* [Diplomatic privileges and immunities: individual freedom or state competences?]. Bratislava: Univerzita Komenského v Bratislave, 2013, p. 78.

[54] STINISSEN, J. A Legal Framework for Cyber Operations in Unkraine. In: Geers, K. (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015, p. 133.

[55] Ibid, p. 134.

[56] LEWIS, J. A. Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine. In: Geers, K. (ed.). *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015, p. 45.

[57] Ibid, p. 47.

this domain is widely accepted, but still unclear, due to a lack of specific international law rules applicable to the cyber warfare and cyber operations. In this situation, only general international law rules are applicable, but they are very general and, as they were negotiated and adopted in the pre-cyber era, often non-applicable to the cyber sphere specifics.

Cyber operations are very wide, flexible and variable. They may have a different form and intensity; there is a variety of players, implementers, addresses etc. To determine cyber incidents as the cyber attacks which form the part of warfare, they must be either comparable to the use of force with a destructive impact or they must form a part of ongoing military operations. Without these attributes, they could be determined as other cyber operations not forbidden by the *ius in bellum*. The borderline between these two categories of incidents is often very thin and unclear. There are significant discrepancies also between representatives of doctrine.[58] Some authors claim, that cyber operations which do not lead to any destructive consequences are rather acceptable than forbidden which leads to the creation of so-called customs of the permissibility of cyber operations.[59] Still it is clear, that even in cases were cyber activities cannot be classified as military or warfare operations or attacks, they do not fall outside the interest and regulation of international law. Cyber operations could have different impacts and different consequences. They could be determined as breaches of prohibition of intervention, as breaches of diplomatic rules etc. In both cases – cyber warfare as well as cyber incidents that could not be determined as use of force – there is still a big challenge before international law, specifically the question of attribution and responsibility. Due to the fact, that cyberspace is an open domain where many anonymous actors could enter very easily, these two questions remain very open.

We have seen several cyber operations during the crisis in Ukraine. They give us a good example of the complexity and difficulty of their determination. We are facing the heterogeneity of actors and different gravities of cyber incidents. Therefore, problems with the identification of the responsible entity as well as the problem with the classification of operations under international law rules occurs here. The conflict in Ukraine is classified as a hybrid warfare situation, mixing the non-conventional tactics and strategies, secret operations, the operation of irregular forces and political manipulations. Cyber incidents are of course part of this hybrid situation. However, their classification is very complicated.

They are more the part of an information war than the component of military actions, because they did not have any destructive consequences and were not interconnected with any particular military operations. Therefore, they cannot be determined as cyber attacks in the light of the Tallinn Manual.

---

[58] BRUNER, T. K podmínkám a způsobu aplikace mezinárodního humanitárního práva na kybernetické operace [Conditions and ways of application of international humanitarian law in connection to cyber operations.] In: Bílková, V. (ed.). *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy* [International humanitarian law - the basis, developments and challenges]. Praha: Univerzita Karlova v Praze, 2015, p. 162.

[59] BROWN, G., POELLET, K. The customary law of cyberspace. *Strategic Studies Quarterly*. 2014, Vol. 6, pp. 126–145. See also: BRUNER, T. K podmínkám a způsobu aplikace mezinárodního humanitárního práva na kybernetické operace [Conditions and ways of application of international humanitarian law in connection to cyber operations.] In: Bílková, V. (ed.). *Mezinárodní humanitární právo: vznik, vývoj a nové výzvy* [International humanitarian law - the basis, developments and challenges]. Praha: Univerzita Karlova v Praze, 2015, p. 166.

Currently a numbers of sources in various forms (national strategies, manuals, legal materials and recommendations of different legal nature) exist that deal with the issue of cyber operations and develop the understanding of this phenomenon. These materials also form the behaviour of individual actors of the international community, influence *de lege ferenda* considerations and stimulate the focus of further research. However, many of them lack the legally binding character and therefore it remains at the discretion of individual actors how they would approach them. At this background, it will be interesting to follow how, and if at all, the states will deal with a problem of legally binding solution of some fundamental issues, e.g. the obligations stemming from the state sovereignty in relation to the cyberspace and the use of force in it.