BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 10, NUMBER 1 (2017)
ISSN 2029-0454

DE GRUYTER OPEN

Cit.: *Baltic Journal of Law & Politics* 10:1 (2017): 63–89
DOI: 10.1515/bjlp-2017-0003

CYBER ATTACKS, INFORMATION ATTACKS, AND POSTMODERN WARFARE

Jozef Valuch

Assistant Professor; PhD.
Comenius University in Bratislava, Faculty of Law (Slovak Republic)

Contact information
Address: Šafárikovo nám. č. 6, P.O.BOX 313, 810 00 Bratislava, Slovakia
Phone: 00421 2 592 44 237
E-mail address: jozef.valuch@flaw.uniba.sk

Tomáš Gábriš

Associate Professor; PhD., LL.M., MA
Comenius University in Bratislava, Faculty of Law (Slovak Republic)

Contact information
Address: Šafárikovo nám. č. 6, P.O.BOX 313, 810 00 Bratislava, Slovakia
Phone: 00421 2 592 44 560
E-mail address: tomas.gabris@flaw.uniba.sk

Ondrej Hamuľák

Assistant Professor; Ph.D.
Palacký University Olomouc, Faculty of Law (Czech Republic)

Contact information
Address: tr. 17. listopadu 8, 771 11 Olomouc, Czech Republic
Phone: 00420 585 637 635
E-mail address: ondrej.hamulak@upol.cz

Received: April 3, 2017; reviews: 2; accepted: June 15, 2017.

ABSTRACT

The aim of this paper is to evaluate and differentiate between the phenomena of cyberwarfare and information warfare, as manifestations of what we perceive as postmodern warfare. We describe and analyse the current examples of the use the postmodern warfare and the reactions of states and international bodies to these phenomena. The subject matter of this paper is the relationship between new types of postmodern conflicts and the law of armed conflicts (law of war). Based on ICJ case law, it is clear that under current legal rules of international law of war, cyber attacks as well as information attacks (often performed in the cyberspace as well) can only be perceived as "war" if executed in addition to classical kinetic warfare, which is often not the case. In most cases perceived "only" as a non-linear warfare (postmodern conflict), this practice nevertheless must be condemned as conduct contrary to the principles of international law and (possibly) a crime under national laws, unless this type of conduct will be recognized by the international community as a " war" proper, in its new, postmodern sense.

KEYWORDS

International law, law of war, cyber attacks, information attacks, postmodern warfare

INTRODUCTION

The issue of cyberspace currently attracts a lot of attention even in the context of international conflicts. News regularly report about cyber warfare and information warfare, where lines are blurred between a traditional war, in which only state actors are participants, and new forms of enmities and warfare which include non-state actors and civilians. Experts speak of nonlinear wars, or of a postmodern blurring of differences between war and peace, good and evil, and often predict terrible futures full of wars against each other,[1] unless a new standard for assessment of such conflicts will be introduced – in order to overcome uncertainties in international relations. Lawyers are already talking about options to include civilians and civilian facilities in military operations, about "cyber conscriptions" – i.e. mobilization of civilian resources for the purpose of war,[2] but also about new possibilities to respond to the new forms of war.[3] While mostly speaking of cyberwarfare, information warfare as another manifestation of nonlinear war (dissemination of conspiracies with the aim of demoralization of population) is often neglected. The aim of our paper is to differentiate between the phenomena of cyber warfare and information warfare, as manifestations of what we perceive as postmodern warfare.

1. CYBER- AND INFORMATION WARFARE

In what follows, we are primarily interested in a different kind of conflict than an "armed conflict" in proper sense. We shall focus on "wars" that may take various other forms, closer or more distant to the classical concept of war, while mostly they take a "cyber", or "information/electronic" form. Not all illegal activities in cyberspace necessarily have to do with war – e.g. the CRN at the University of Zurich distinguished between various levels of illegal conduct in cyberspace: activism, hactivism, cybercrime, cyberterrorism and cyberwar.[4] Thereby, even the most intensive illegal conduct is sometimes denied the nature of a "war" proper

[1] Roman Kanda, *et al*., *Podzim postmodernismu: Teoretické výzvy současnosti (The Fall of Postmodernism – the Theoretical Challenges of Present Days)* (Praha: Filosofia, 2016), 237, 286.
[2] Susan W. Brenner and Leo L. Clarke, "Civilians in Cyberwarfare: Conscriptions," *Vanderbilt Journal of Transnational Law* 43 (2010): 1031.
[3] Peter Margulies, "Sovereignty and Cyber Attacks: Technology's Challenge to the Law of State Responsibility," *Melbourne Journal of International Law* 14 (2013): 496.
[4] Elgin Brunner, Anna Michalkova, Manuel Suter, and Myrian Dunn Cavelty, *Focal Report 3: Critical Infrastructure Protection – Cybersecurity – Recent Strategies and Policies: An Analysis, CRN Reports*, (Zurich: Center for Security Studies, 2009), 16-17. See also Pauline C. Reich, Stuart Weinstein, Charles Wild, and Allan S. Cabalong, "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity," *European Journal of Law and Technology* 1 (2010): 28.

(being considered rather a sort of sabotage, espionage, or subversion).[5] Still, there are also opinions that cyberspace actually represents a laboratory of early human society and therefore can be seen as an area of a Hobbesian war of all against all. For the purposes of this paper, we shall not pay attention to illegal activities taking place among private entities, such as, for example, trolling[6] or cyber-bullying,[7] which can be hindered by state or by private tools (e.g. autonomous regulation, codes of conduct, best practices).[8] Rather, we focus on cases of possible abuse of cyberspace by states in the form of cyberwarfare (direct electronic interference with foreign military and civilian targets with the intent to cause damage) and information warfare (controlling or influencing the mood in the society via social engineering).[9] In respect of the latter, we might take the example of the third (non-profit) sector in Slovak, which presents numerous hypotheses on the society in the Slovak Republic as well as in the neighbouring Czech Republic as an object of social engineering, or even of information warfare. NGOs and non-profit think-tanks in Slovakia and in the Czech Republic argue mainly by pointing to the unclear financial background of some websites disseminating pro-Russian and anti-American or anti-Western European propaganda. While the financial background is unclear, the ideological background and content of the information apparently refer to Russian sources.[10] This is what leads the NGOs to fear that Slovak and Czech servers are possibly tools of a foreign-funded non-linear information warfare, aimed to demoralize the civilian population of the two Republics. The second possible answer, being a less serious one, would be that of a natural inclination to conspiracies among the population, which is a characteristic feature of our post-factual age, not only in these Republics but in general across Europe – this trend can be fought only by rational counter-arguments, but these often do not fall on

[5] Thomas Rid, "Cyber War Will Not Take Place," *The Journal of Strategic Studies* 35 (2012): 5.
[6] Arthur Gaus, "Trolling Attacks and the Need for New Approaches to Privacy Torts," *University of San Francisco Law Review* 47 (2012-2013): 353. There are various categories of trolling, such as snerts, trolls, and haters. *Cf*. Jonathan Bishop, "The effect of de-individuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater," *International Journal of Cyber Criminology* (IJCC) 7 (2013).
[7] "Cyber-bullying is using technology to deliberately and repeatedly cause harm and distress. Trolling is deliberately trying to distress someone online but usually just to disrupt and often anonymously. It is frequently inflammatory and abusive. Cyber-bullies usually know the person they are attacking and it is ongoing" (Sarah Nicol, "Cyber-bullying and trolling," *Youth Studies Australia* 31 (2012): 3-4).
[8] See e.g. the fight of Microsoft against botnets misused for DDOS and for spam distribution, in 2010. *Cf*. Janine S. Hiller, "Civil Cyberconflict: Microsoft, Cybercrime, and Botnets," *Santa Clara High Technology Law Journal* 31 (2015): 177.
[9] Glenn Greenwald, "How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations" (November 2016) // https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/.
[10] Ivana Smoleňová, "Campaign in the Czech Republic and Slovakia: Types of Media Spreading Pro-Russian Propaganda, their Characteristics and Frequently Used Narratives" (November 2016) // http://www.pssi.cz/download/docs/253_is-pro-russian-campaign.pdf: "These pro-Russian media show a high level of similarity, using the same language and narratives. Individual disinformation campaigns appear to be spreading in a joint effort, re-posting the same articles, using identical arguments, citing Russian sources, and referring to the same pro-Kremlin public personalities. Their appearance correlates with the Ukrainian crises, however, many were founded before 2014, suggesting that the system might have been years in making."

fertile soil within a generally irrational context. A final answer as to whether the situation in Slovakia and Czech Republic is a manifestation of independent national development, or rather an action initiated and supported from abroad, is not available for the time being. Of course, one cannot rule out a combination of both, relying on the popularity of electronic sharing of "secret, exclusive, non-mainstream" information.

Uncertainties associated with identification of sources, background and the real goals of "information wars" are elements that information warfare shares with the cyberwarfare. In the case of cyberwarfare it is often difficult to prove the source of the initiative, as well as the actual share of military and civilian participants necessary to correctly determine the legal categorization and responsibility for such actions. The classical doctrine of humanitarian international law, respectively of the law of war, requires both the presence of states as entities waging war, as well as that the conflicts are both "armed" and "international".[11] Neither information warfare nor cyberwarfare usually satisfies these conditions – especially that of being "armed". While there are many theoretical attempts to prove that cyber warfare should be considered an armed conflict[12] within the context of the use of force under Art. 2 (4) of the UN Charter (valid as a customary rule of *ius cogens*, thus applicable also to States that might not be UN Members),[13] these attempts have not so far been accepted generally.[14] For example, Schmit proposed to take into account several criteria in order to assess whether a cyber attack meets the characteristics of use of force, and therefore of a "cyberwar": severity, immediacy, directness, invasiveness, measurability and presumptive illegitimacy.[15] However, Schmit´s criteria were refused as allowing for subjective interpretation.[16] An "information war" must then be perceived as even more ambiguous; it can in fact never be fundamentally considered an "armed conflict", and within international law of war we can see at most an attack on civilian targets (protected in the time of war under the 4th Geneva Convention of 1949 and under the Additional Protocol of 1977), or a demoralization technique employed in relation to enemy civilian

[11] Michael Schmit, "Classification of Cyber Conflict," *Journal of Conflict & Security Law* 17 (2012): 250.
[12] *Ibid*.: "cyber operations can have highly destructive, even deadly, results. A State involved in an exchange of cyber attacks at this level would be very likely to characterize the situation as international armed conflict, much as it would if it fell victim of another State's non-kinetic bacteriological attack."
[13] E.g. focusing on the actual damage caused by cyber attacks, including economic damage. *Cf*. Walter Gary Sharp, *Cyberspace and the use of force* (Falls Church, Virginia: Aegis Research Corp., 1999), 88-91. For refuting of this viewpoint see Titiriga Remus, "Cyber-attacks and International law of armed conflict; a 'jus ad bellum' perspective," *Journal of International Commercial Law and Technology* 8 (2013): 182.
[14] Arguing that nobody is yet willing to escalate computer attacks to match the armed conflict. Thus, so far, cyber attacks are labelled as cyber wars only metaphorically (Titiriga Remus, *supra* note 13: 189).
[15] Michael N. Schmitt, "Computer network attack and the use of force in international law: thought on a normative framework," *Columbia Journal of Transnational Law* 37 (1999): 885.
[16] Stephenie Gosnell Handler, "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare," *Stanford Journal of International Law* 48 (2012): 229.

facilities. These institutes of international law of war are, however, only applicable in the time of an ongoing war, which in case of "information wars" and "cyberwars" usually means that the conventions do not apply if these take place independently from armed/military operations, or (in case of so-called information warfare) if no actual harm to civilians occurs.[17]

As far as possible solutions to the problem of cyberwarfare are concerned, there was the well-known so-called Tallinn manual drafted some time ago on this issue (by its nature legally non-binding[18]), and legal scholarship also suggests some other solutions to this issue – e.g. Peter Margulies proposes to shift the burden of proof onto a suspect state within the so-called theory of virtual control; [19] furthermore, Scott Shackleford recommends adopting in the long term an international convention on cybersecurity, defining cyber attack and its various levels which can be perceived as an armed attack, while creating a Multinational Cyber Emergency Response Team (MCERT), or at least while introducing a closer cooperation between the already existing CERTs in order to identify the hidden sponsors of cyber attacks.[20] It remains questionable, however, to what extent such an international convention (potentially including also information warfare) would be acceptable and subsequently enforceable in practice, given the current international practice of blurring the origin of cyber- (and information-) attacks – such an obfuscation being yet another manifestation of the postmodern situation in international relations, and an expression of the postmodern nature of non-linear wars.

2. POSTMODERN AND NON-LINEAR WARS

It is mostly in relation to the "war on terror" and to "cyberwars" where traditional characteristics of war under the legal definition of war are absent. Indeed, while already Cicero considered war traditionally as a conflict between state entities,[21] in case of postmodern international conflicts it may be questionable whether the conflicts are initiated by the states, executed by the states and whether they involve the use of armed force at all. On the other hand, what is

[17] Susan W. Brenner and Leo L. Clarke, *supra* note 2: 1031.
[18] It draws from the International Law Commission's Draft Articles on Responsibility of States for Internationally Wrongful Acts, which recognize responsibility of states for private entities' conduct attributable to the states. The International Court of Justice thereby adopted a special effective control test. The International Criminal Tribunal for Former Yugoslavia speaks here of the criteria of "overall control". See Peter Margulies, *supra* note 3: 497–498.
[19] *Ibid*.: 514.
[20] Scott J. Shackelford, "Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks" (November 2016) // https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849; Scott J. Shackelford, "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law," *Berkeley Journal of International Law* 27 (2009): 192.
[21] *Cf*. Stephen C. Neff, *War and the Law of Nations. A General History* (Cambridge: Cambridge University Press, 2005), 18-19.

rather clear is that they affect not only military, but also (often primarily) civilian targets. While history is not unfamiliar with the concept of private wars, which have been present in Western Europe particularly in the High Middle Ages,[22] these are still rather close to civil war or to self-help in a situation of missing state monopoly of violence,[23] while the modern non-linear wars/postmodern conflicts are closer to wars in which states stands in the background – either directly and openly such as the USA in the "war on terror", or indirectly as in some cases of cyberwarfare and information warfare which we shall pay particular attention to in this paper.

A similar evaluation of the current situation was penned by the postmodern Slovenian philosopher Slavoj Zizek: "we no longer have wars in the old sense of a regulated conflict between sovereign states in which certain rules apply (the treatment of prisoners, the prohibition of certain weapons, etc.)."[24] Instead, he distinguishes between two types of current armed conflicts - (1) "ethnic-religious conflicts" which violate the rules of universal human rights, do not count as wars proper, and call for 'humanitarian pacifist' intervention by Western powers, and (2) direct attacks on the USA or other representatives of the new global order, in which case, again, we do not have wars proper, merely prosecution of "unlawful combatants",[25] which is the case with the war on terror. The following applies to the US:

> Is obviously not in a state of war, at least not in the old conventional sense of the term (for the great majority of people, daily life goes on, and war remains the exclusive business of state agencies): the very distinction between the state of war and the state of peace is thus blurred; we are entering a time in which a state of peace itself can at the same time be a state of emergency.[26]

Hence, blurring of war and peace seems to be the major sign of postmodern situation in international relations. This is mostly due to the fact that no traditional "armed conflict" is present; the issue here is also the applicability of other requirements of a traditional war, such as the status of warring entities (including often non-state actors). In this line, Michael Hauser, a contemporary Czech philosopher, speaks of a situation of heterogeneous and momentary alliances, lack of unifying discourse, and military operations run by no logical plan, thus war being

[22] Justine Firnhaber-Baker, "From God's Peace to the King's Order: Late Medieval Limitations on Non-Royal Warfare," *Essays in Medieval Studies* 23 (2006/7): 20. Justine Firnhaber-Baker, "Introduction: History, historians, and seigneurial war": 2; in: *Violence and the State in Languedoc, 1250–1400* (Cambridge: Cambridge University Press, 2014).
[23] Max Weber, "Politics as a Vocation" (November 2016) // http://anthropos-lab.net/wp/wp-content/uploads/2011/12/Weber-Politics-as-a-Vocation.pdf.
[24] Slavoj Žižek, *Welcome to the Desert of the Real! Five Essays on September 11 and Related Dates* (London: Verso, 2002), 93.
[25] *Ibid*.
[26] *Ibid*., 107.

not logocentric,[27] and indeed representing a postmodern war of all against all[28] (e.g. by using countermeasures[29]). He considers the above (together with the Žižekian diagnosis) to be features of postmodern and non-linear warfare, the notions of which will be employed throughout this article.

In order to better grasp these postmodern phenomena, in the following we offer an analysis and some examples of cyber warfare, from which certain principles can also be derived for information warfare, both showing specificities which make them distant from traditional warfare, and a part of postmodern conflicts as defined above.

3. INTERNATIONAL LAW AND INTERNATIONAL SECURITY IN CYBERSPACE

On the most general level, the task of ensuring international security is entrusted to the United Nations (UN) organization. In this respect, it incorporated the Charter of the United Nations, signed already on 26th June 1945.[30] The UN Charter features in a prominent place the objectives of the United Nations to maintain international peace and security.[31] The security system of the UN is thereby further institutionalized in the form of one of its main bodies – the Security Council. This has the primary responsibility for maintenance of international peace and security.[32] Since the establishment of this organization, however, more than seventy years have passed, and the international community and individual states are now facing various new (postmodern) challenges and security threats that are

[27] Michael Hauser, "Za hranice postmodernismu" (Beyond the Frontiers of Postmodernism): 237; in: Roman Kanda, *et al*., *Podzim postmodernismu: Teoretické výzvy současnosti (The Fall of Postmodernism – the Theoretical Challenges of Present Days)* (Praha: Filosofia, 2016).
[28] *Ibid*.: 286.
[29] Mary Ellen O'Connell, "Cyber Security without Cyber War," *Journal of Conflict & Security Law* 17 (2012): 204: "countermeasures are the mechanisms through which international law allows parties to carry out self-help, coercive enforcement of their rights. ... The International Court of Justice, in the Gabčíkovo – Nagymaros case, laid out four elements of a lawful countermeasure: 1. In the first place it must be taken in response to a previous international wrongful act of another State and must be directed against that State; 2. The injured State must have called upon the State committing the wrongful act to discontinue its wrongful conduct or to make reparation for it; 3. The effects of a countermeasure must be commensurate with the injury suffered, taking account of the rights in question; 4. Its purpose must be to induce the wrongdoing State to comply with its obligations under international law, and the measure must therefore be reversible."
[30] *Cf*. John P. Grant and Craig J. Barker, *Parry & Grant Encyclopaedic Dictionary of International Law,* 3rd ed. (Oxford: Oxford University Press, 2009), 635. *Cf*. also Peter Vršanský, "The United Nations Charter entered into force 70 years ago (is the twilight of the United Nations near?)," *Slovak yearbook of international law* 5 (2015).
[31] *UN Charter*, Art. 1(1): "To maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace."
[32] *UN Charter*, Art. 24(1): "In order to ensure prompt and effective action by the United Nations, its Members confer on the Security Council primary responsibility for the maintenance of international peace and security, and agree that in carrying out its duties under this responsibility the Security Council acts on their behalf."

different from those which were known at the time of establishment of the UN. All the more, the Charter of the United Nations underwent so far only minor "cosmetic changes" and its fundamental reform is not in sight.

The changing nature of security threats is a fact of which many state officials and authorities are well aware. Their worries and thoughts are manifested in numerous international documents of varying legal force. One of the documents related to the issue of international security is, for example, the high-level panel report entitled "A more secure world: Our shared responsibility",[33] prepared by a team of recognized authorities, under the aegis of the then UN Secretary-General Kofi Annan in 2004. The report states that we live in a world of new threats that could not be known or anticipated at the time when the United Nations were established, namely in 1945. At the beginning of the new millennium the report outlined following six categories of the most serious threats to international security: inter-state conflicts, violence within states, economic and social threats, weapons of mass destruction, terrorism and international organized crime. In the meantime, however, more than a decade has past, and progress in the development of new technologies and their availability makes us reflect on whether the above calculation is still relevant and sufficient. Several events from the recent years confirm that the international community is again facing some new challenges.

Simple availability, as well as anonymity and the spatial intangibility of information technology lead currently to a growing proportion of activities taking place in the cyberspace, with only a negligent risk of prosecution. Cyberspace is indeed in many respects different from any previously known and exploited space dimensions. For a long time, humanity basically used only two dimensions of space – namely the Earth's surface and water (i.e. the sea). Later on, due to the development of technology, sky and outer space were added. Now we know that in addition to these four dimensions, there is also a fifth one available for international conflicts – cyberspace. This fifth spatial dimension is very different in comparison to the above enumerated examples. It has a global reach, which blurs the physical boundaries between countries, and allows for operating regardless of the political system, with an extremely wide range of actors – from individuals, through various groupings, up to states.[34]

It may also be noted in addition that in the previously exploited four dimensions of space the seizure of each area had required a sufficient military and

[33] *Report of the Secretary-General's High-level Panel on Threats, Challenges and Change (2004)* // http://www.un.org/en/peacebuilding/pdf/historical/hlp_ more_secure_world.pdf.
[34] *Cf*. Michaela Melková and Tomáš Sokol, "Kybernetický priestor ako nová dimenzia národnej bezpečnosti" (Cyber Space as the New Dimension of the National Security): 55-56; in: *Bezpečnostné fórum 2015* (Banská Bystrica: Belianum, 2015).

material capacity. For example, to ensure superiority at sea, it was necessary to dispose of the prevailing maritime power. In contrast, in cyberspace it is almost impossible to achieve, even for a short time, absolute hegemony – given the number of actors, simple access and anonymity. Finally, it is also very difficult to determine the source of a cyber attack.[35] Due to all these reasons, this type of space offers in addition to substantial possible benefits also ample possibilities for cyber crime or cyber attacks, covering a wide range of negative phenomena including cyber warfare. Other negative examples of cyber attacks may include cyber espionage, hacking, DDoS attacks,[36] or other undesirable activities, including extremism and abuse of the Internet for terrorist activities and terrorist propaganda (e.g. in the form of making available manuals for manufacturing explosives) and the like. Relatively easily and cheaply accessible cyber technology and the necessary skills allow even the weaker states or non-state actors to cause serious damage to states disposing with strong conventional armed forces. Hence, as indicated in the "Australia's cyber security strategy",[37] the differences between traditional actors of illegal phenomena – hackers, terrorists, organized criminal networks, industrial espionage and foreign intelligence services – is becoming increasingly blurred with state actors, being one of the features of postmodern non-linearity.[38]

In this context, there is a long-lasting discussion going on regarding the applicability of international law in cyberspace. Most Western countries are favourable to the application of existing international law. Some other countries, like Russia and China, have proposed to introduce a specific set of standards.[39] Still, one can conclude that it is generally accepted that international law is and should be also in the future applicable to cyberspace. This is confirmed by the 2013 report of the Group of Governmental Experts, established by the United Nations (UN) General Assembly. It states that "international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment."[40] However, there is also the question of how to apply international

[35] *Ibid*.: 57. *Cf*. Franklin D. Kramer, Stuart H. Starr, Larry K. Wentz, and Daniel T. Kuehl, *Cyberpower and National Security* (Washington: Potomac Books Inc., 2009), 664.
[36] *Distributed Denial of Service* (DDoS).
[37] *Australian Government Cyber Security Strategy, 2009* // http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.
[38] Marco Roscini, *Cyber Operations and the Use of Force in International Law* (Oxford: Oxford University Press, 2014), 1-2.
[39] *Letter dated 9 January 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations, addressed to the Secretary-General*, United Nations, General Assembly, A/69/723, 2015.
[40] *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations, General Assembly, Group of Governmental Experts (GGE), A/68/98, June 24, 2013. The Group consisted of representatives of 15 nations, including the United

law in this sector, and this is not a debate that will be resolved easily in the near future.[41]

At present, there is no consensus among the leaders of United Nations on the international law character of cyberwarfare. It is interesting here that the 2015 Group of Governmental Experts (GGE), which was tasked to look at the application of international law to cyber conflicts,[42] found this topic to be the most difficult. Disagreements prevailed between Russia, China and several other countries on one hand, and the Member States of NATO on the other.

The crux of the disagreement was in the applicability of specific provisions of the UN Charter (the general applicability of the Charter had been agreed upon within the GGE), in particular the applicability of Article 2(4), renouncing the use of force, and Article 51 on the inherent right to self-defence. Another issue was whether it is possible to overcome the norms enshrined in the UN Charter and in the international conventions governing the conduct of war and armed conflicts, in order to establish new and specific standards for this type of conflicts. One (the simplest) possibility would be here to re-interpret the UN Charter commitment to avoid actions that threaten territorial integrity or political independence of a state (found in Articles 2(4) and 51) so as to explicitly include cyber actions.[43]

Besides the (unlikely) re-interpretation of the UN Charter, or introduction of a new convention on cyberwars, according to J. A. Lewis there are still four categories of international legal standards applicable currently to the issue of cyber warfare (and possibly also other forms of postmodern international conflicts):

- those that call for observation of existing international law regarding state responsibility, especially the laws of armed conflict;

- those that seek to exempt from cyber attack infrastructures where an attack could have an indiscriminate effect (such as critical infrastructures, including the infrastructure of the global Internet);

- norms on the state obligation to assist other states that are victims of cyber attacks; and

States, Russia, and China. In their Report of July 2015, the GGE recommended a set of norms of behaviour of states in cyberspace (Jan Stinissen, "A Legal Framework for Cyber Operations in Ukraine": 124; in: Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCD COE Publications, 2015)).

[41] *Ibid*.

[42] *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*, United Nations, General Assembly, Group of Governmental Experts, A/70/174, July 22, 2015// http://www.un.org/ga/search/view_doc.asp?symbol= A/70/174.

[43] James Andrew Lewis, "Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine": 42–43; in: Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCD COE Publications, 2015).

- norms on the proliferation of cyber technologies that could be abused for malevolent purposes (which is still nascent and suffers from definitional problems, though).[44]

4. SELECTED CASES OF CYBERSPACE ABUSE

From among the threats connected to cyberspace, we analyze those that have or may have the greatest relevance for international security, being close to cyber warfare as a type of non-linear postmodern conflict.

4.1. ESTONIA (2007)

As an initial example, one can mention the case of April 2007, when Estonia faced a three-weeks-long DDoS (distributed denial of service) attack. The stimulus was supposed to have been a decision of the Estonian authorities to relocate a Soviet war memorial from the centre of the capital Tallinn to a military cemetery. This act triggered riots among the Russian minority, whose members perceived this monument as a memorial to war victims. (Estonians saw this monument as a symbol of foreign occupation.) This has also led to a blockade of the Estonian Embassy in Moscow. The DDoS attacks first hit the websites of governmental institutions and later also websites of some major newspapers, TV stations, banks and other targets. Several of the attacked websites were replaced by sites with Russian propaganda or with false apologies for websites being non-functional, but most attacks focused simply on turning the websites off. A spokesman for the Estonian Ministry of Defence compared these attacks to those against the USA on September 11, 2001. Estonia thereby claimed that several of the first attacks came from Russia, but most of them came later on from many thousands of ordinary computers from all around the world, making it difficult to ascribe the responsibility to a (single) state actor (Russia). Several computers were operated by Russian civilians angry with Estonia, and some Russian websites featured anonymously circulated instructions on how to perform the DDoS attacks. Many more attacks, however, came from computers infected with a virus in order to hijack the computers and involve them in these attacks without any knowledge of their owners.[45] Some sources claim that in this second phase of attacks, more than one million computers (as non-linear non-state actors of cyber warfare) were involved from over a hundred countries. Overall, however, these attacks resulted "only" in

[44] *Ibid*.: 44.
[45] The Economist, "A Cyber-riot" (May 10, 2007) // http://www.economist.com/node/9163598.

economic and communication disruption, and caused no significant property damage, injury or loss of life.[46]

4.2. RUSSIA - GEORGIA CONFLICT (2008)

Cyber operations against Georgia took place in late July and early August 2008, before and during an armed conflict with Russia. They caused that governmental websites were offline and Internet services were slowed down. Especially immediately before and after the Russian troops entered the Georgian province of South Ossetia, several governmental websites were disabled or their content had been replaced by anti-Georgian propaganda, while the DDoS attacks prevented Georgian authorities from dissemination of any information to the citizens. Georgia accused the Russian Federation of these cyber attacks, but Russia denied this and claimed that the attacks were a work of private individuals who did so voluntarily. These cyber operations were then addressed in a report of an independent fact-finding mission on the conflict in Georgia in 2009,[47] which did not, however, recognize their imputability to Russia, and only stated that "if these attacks were controlled by governments or government, it is likely that this form of warfare was used for the first time in an inter-State armed conflict".[48] Some sources state that the origins of the attacks were in five anonymous systems, out of which four were in Russia and one in Turkey, and at the same time all were controlled by the RNB crime syndicate (a non-state actor, making this hence a non-linear, postmodern conflict).[49]

4.3. IRAN (2010)

Iran was also a target for cyber attacks in recent years, namely in 2010, in connection with its nuclear program. This was the case of a computer worm called Stuxnet, which was one of the most sophisticated and most intelligent computer worms. It was discovered in the second half of 2010, spreading easily through Microsoft Windows, and focused mainly on industrial software by Siemens and its equipment. The attack was relatively simple. It could hit extremely important points in the system, for example programs that manage and monitor industrial

[46] Marco Roscini, *supra* note 38, 4-5.
[47] *Report of Independent International Fact-Finding Mission on the Conflict in Georgia,* Vol I, September 2009 // http://echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf.
[48] Marco Roscini, *supra* note 38, 7-8. *Cf. Report of the Independent Fact-Finding Mission on the Conflict in Georgia*, Vol II, September 2009, pp. 217-219 // http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf.
[49] *The Russian Business Network*. *Cf.* Michaela Melková and Tomas Sokol, *supra* note 34: 59. *Cf.* David J. Smith, "Russian Cyber Strategy and the War Against Georgia" (January 17, 2014) // http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.

processes, or that cooperate with various other systems and applications. So far, five different types of Stuxnet are known, which were used against Iranian facilities. As a result of these attacks, Iran's nuclear program has been damaged.[50] This is a proof of further qualitative step in the use of cyber attacks – despite the fact that the extent of damage is unclear, this incident confirms the potential dangers of malware that can engulf important computer systems managing energy supplies or traffic networks. This case is thus considered the first proof of cyber attacks potentially causing real physical damage and endangering human lives.[51] On this basis one can indeed conclude that Stuxnet was the first global cyber weapon of geopolitical importance.[52] Still, however, no specific state actor was accused or attributed responsibility in this postmodern warfare case.

4.4. 2014 AND 2015

From the more recent years, one may further invoke events such as an attack on the movie studios of Sony Pictures Entertainment, from which many important documents about movies, celebrities and access data were stolen. The attack was attributed to North Korea in connection with the fact that the studio had just prepared a movie in which the North Korean leader was to die. Another instance of a cyber attack, this time ascribed to Islamic State (ISIS, in fact rather a non-state actor), was focused on a Twitter account and YouTube channel of the Central Command of the US Army. Central Command is the part of the US military responsible for the regions of the world where US military operations take place – i.e. about twenty countries, including Afghanistan, Iran, Iraq, Saudi Arabia and Syria. Next to the slogan "We won't stop! We know everything about you," the names and phone numbers of military personnel were shown on the attacked channels. Other social media displayed an office with people in uniforms, picture being taken probably through a web camera. Other displayed reports contained the words "In the Name of Allah, the Most Gracious, the Most Merciful, the CyberCaliphate continues its CyberJihad." The YouTube account of the Central Command showed an image of a man in scarf with the phrase "i love you isis". A representative of the Pentagon has then said that although this had caused some embarrassment, it has not been shown that this was an actual security threat.[53]

[50] Veronika Macková, "Cyber War of the States: Stuxnet and Flame Virus Opens New Era of War": 5 // http://cenaa.org/wp-content/uploads/2014/05/Veronika-Mackova-PP-No.-15-2013-Vol.-2.pdf.
[51] *Nové hrozby - kybernetické dimenzie (New risks – cyber dimensions)*, NATO Review // http://www.nato.int/docu/review/2011/11-september/cyber-Threads/SK/index.htm.
[52] Veronika Macková, *supra* note 50: 7.
[53] Dave Lee, "Top US military Twitter feed 'hacked by Islamic State'" (January 12, 2015) // http://www.bbc.co.uk/newsbeat/article/30781377/top-us-military-twitter-feed-hacked-by-islamic-state.

4.5. THE UKRAINE CRISIS (2013-2016)

The beginning of the so-called Ukraine crisis, or so-called Russia-Ukraine conflict, dates back to 2013 andpersists to this day. Overall, this conflict is often referred to as a hybrid war (hybrid warfare) – a mixture of unconventional tactics and strategies, secret actions, irregular forces, cyber operations and political manipulations in order to achieve political objectives. This basically seems to be a set of tactics to avoid military retaliation and not to exceed the limit, which could be considered a use of force, making it a postmodern conflict *par excellence*. Conventional warfare is thus only a part of a larger range of coercive actions available to states in the postmodern situation.[54]

Interestingly for us, in this case cyber operations were also used as a tool of information war (information warfare). They encompassed digital propaganda, website defacements, denial-of-service (DoS) campaigns, information leaks by hacktivist groups, and cutting-edge cyber espionage malware. However, apart from disruptions to Internet connectivity between Crimea, Donbass, and the rest of Ukraine, there have been no known attacks against civilian or military critical infrastructures.[55] According to some authors, Russian cyber activities, especially those associated with the recent conflict in Ukraine and with the annexation of Crimea, probably offer the best example of the employment of cyber attacks in information warfare – to shape the overall political course of a dispute.[56]

5. RESPONSES BY INTERNATIONAL BODIES

The above examples are only a selection of cases of postmodern and non-linear conflict with the use of cyberspace in a way approaching level of warfare. Many other states have actual experience with similar interventions. This has quite naturally prompted the international bodies, namely various regional groupings and organizations, to respond to this kind of threat, whether by adopting domestic laws, building relevant capacities, or strengthening international cooperation. Cyber operations have created a risky space in which states can conduct offensive action with less political risk, given the grey zones of international law, and given the fact that opponents can find it difficult to respond.[57]

[54] James Andrew Lewis, *supra* note 43: 40.
[55] Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCD COE Publications, 2015) // https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html.
[56] James J. Wirtz, "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy": 30; in: Kenneth Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine* (Tallinn: NATO CCD COE Publications, 2015).
[57] James Andrew Lewis, *supra* note 43: 40.

5.1. NATO

NATO is an international organization of a military and political nature, which brings together countries for the sake of cooperation in the security field. Through the institute of collective defence it provides Member States with protection via political as well as military means.[58] New forms of threats can therefore not go unnoticed by the organization; its various strategic documents now consider cyberspace as a new operation domain. One can mention, for example, the "NATO Strategic Concept" adopted at Lisbon Summit in 2010. Under this conception, cyber attacks are one of the key threats today. They occur more often and are able to reach a level that threatens the national and Euro-Atlantic prosperity, security and stability. The actors of such attacks can be foreign military and intelligence services, terrorist and extremist groups, as well as organized or individual criminals.

In 2011, NATO adopted the "NATO Policy on Cyber Defence". It defines the role and activities of NATO in the field of cyber defence to be developed in the future. In addition to this Policy, a "NATO Cyber Defence Action Plan" was adopted, giving details on tasks and resources on order to achieve the objectives of cyber defence. The Policy and Plan were updated in May 2014 via the "Enhanced NATO Policy on Cyber Defence" and at the summit in Wales where the updated "NATO Cyber Defence Action Plan" was approved. This sets out specific tasks in order to fulfil the above Policy, and one of its key tasks is to enhance mutual cooperation between the public sector, private sector and academia.[59]

Especially the abovementioned attacks in Estonia in 2007 resulted in fundamental questions being raised in NATO: "If a member state's communications centre is attacked with a missile, you call it an act of war. So what do you call it if the same installation is disabled with a cyber-attack?"[60] Consequently, NATO Secretary-General Fogh Rasmussen after the meeting in Wales said: "Today we declare that cyber defence is part of a collective defence." This statement is thereby a shift from the traditional perception of collective defence within NATO, since so far the article on collective defence[61] referred only to the classical, conventional or

[58] Jozef Valuch, Michaela Rišová, and Radoslav Seman, *Právo medzinárodných organizácií (The Law of International Organisations)* (Praha: C. H. Beck, 2011), 289.
[59] *Koncepcia kybernetickej bezpečnosti Slovenskej republiky (Conception of Cyber Security of the Slovak Republic).*
https://lt.justice.gov.sk/Attachment/Vlastn%C3%BD%20materi%C3%A1l_docx.pdf?instEID=-1&attEID=75645& docEID=413095&matEID=7996&langEID=1&tStamp=20150218154455240.
[60] The Economist, *supra* note 45.
[61] Art. 5 of the NATO Treaty reads: "The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will assist the Party or Parties so attacked by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic

nuclear threats and was only marginally associated with new security challenges. Leaders of NATO Member States seem thus have newly agreed that a cyber attack on one of the NATO members could be considered an attack on the entire Alliance, and could therefore give rise to a military response.[62]

5.2. EUROPEAN UNION

The need to ensure cyber security arises also within the EU. From among the more recent actions in this area one can name, *inter alia*, the document entitled "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace",[63] which represents the vision of the EU in relation to preventing cyber disruptions and attacks, as well as with respect to potential countermeasures. The aim is foremost to increase the resilience of information systems against cyber attacks and to strengthen the EU policy on international cyber security and cyber defence. This document thereby defines cyber security as follows:

> Cyber-security commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields, from those threats that are associated with or that may harm its interdependent networks and information infrastructure. Cyber-security strives to preserve the availability and integrity of the networks and infrastructure and the confidentiality of the information contained therein.[64]

In response to this, European Council endorsed an "EU Cyber Defence Policy Framework", which was approved at a meeting of defence ministers in November 2014. Its key objectives are to support the development of cyber defence in the Member States, to support the missions and operations within the joint defence and security policy, science and research, and to use synergies with other actors outside the EU, mainly NATO. Significant in this regard is that the security of cyberspace should be one of the main priorities for future EU foreign policy in the field of security.[65]

One of the latest results of the European Commission's intention to legislate on cyber security is also the Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of

area. Any such armed attack and all measures taken as a result thereof shall immediately be reported to the Security Council. Such measures shall be terminated when the Security Council has taken the measures necessary to restore and maintain international peace and security."

[62] Monika Masariková, "Potvrdené. Kyberútoky predmetom článku 5 NATO" (Confirmed. Cyberattacks are subject to Art. 5 NATO) (September 5, 2014) // http://www.cybersec.sk/spravy/politika/potvrdene-kyberutoky-predmetom-clanku-5-nato/.

[63] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN (2013) 1 final, Brussels, 2013.

[64] *Ibid*.: 3.

[65] *An outline for Europen Cyber Diplomacy Engagement*, 9967/4/14 REV 4, DG D 1C, Brussels, September 2014.

security of network and information systems across the Union, which is a key part of the overall strategy of cybersecurity in the EU. Besides mutual cooperation, the Directive requires that each Member State adopts a national strategy for network and information security, establishes a national authority responsible for the security of networks and information systems, and sets up a group to respond to cyber threats, a so-called CERT (Computer Emergency Response Team).

5.3. THE UNITED STATES OF AMERICA

One of the most recent US documents related to cyber threats is a paper presented by James R. Clapper, Director of National Intelligence, in September 2015, entitled "Worldwide Cyber Threats".[66] Among other things, this document states that cyber threats are increasing in the frequency, sophistication and intensity of the action. Furthermore, the range of actors of cyber threats, attack methods, targets and victims are also expanding. It is likely that even in the future attempts aimed at infringement of computer and information systems will continue, but "catastrophic attack" is considered unlikely in the USA. Rather than "cyber Armageddon" which would paralyze the entire US infrastructure, a series of cyber attacks on low or moderate level is expected instead, possibly coming from different sources. This document thereby distinguishes the following potential actors of cyber attacks against the USA:

a) states with highly sophisticated cyber programs (such as Russia or China),

b) states with lesser technical capabilities but possibly more disruptive intent (such as Iran or North Korea),

c) profit-motivated criminals,

d) ideologically motivated extremists or hackers.

The distinction between state and non-state actors (a sign of postmodern conflict proper) is extremely difficult to ascertain, especially when working together (directly or indirectly), or when states are overlooking crime detrimental to foreign victims, or even using similar cyber tools themselves.[67]

6. POSTMODERN WARFARE IN LIGHT OF IUS AD BELLUM AND IUS IN BELLO

Although cyber tools and techniques can be used in harmful ways, they are still not weapons *per se*, which can make it difficult to decide about

[66] James R. Clapper, "Worldwide Cyber Threats" (September 10, 2015) // http://intelligence.house.gov/sites/intelligence.house.gov/files/documents/ClapperOpening09102015.pd.
[67] *Ibid*.

countermeasures.[68] A cyber attack can produce results equivalent to a kinetic attack, but this is not its primary effect; instead it is (at least for now) to manipulate the data, knowledge, and opinion – simply put to produce political or psychological effect rather than physical damage.[69] What is thereby the relationship between this kind of attack and the principles of *ius ad bellum* and *ius in bello*? A particularly important role in searching for an answer in this respect was played by an international expert group that was invited by the NATO Centre of Excellence to clarify this relationship. The result was the so-called Tallinn manual, drawn up in 2012,[70] but being only the result of work by independent experts, which is not legally binding. This document pays particular attention to cyber security and the relationship between cyber attacks and ius ad bellum, i.e. the international law governing the resort to force (I), and the ius in bello, i.e. the international law regulating the conduct of armed conflict (II). Related bodies of international law, such as the law of state responsibility, are dealt with in greater detail in the context of these topics.[71]

Concerning legally binding sources, from an International Court of Justice (ICJ) award in the issue of nuclear weapons,[72] it becomes clear that the law of armed conflict applies to any use of force, irrespective of the weapon.[73] In order to assess whether a cyber attack is an instance of using force under Art. 2(4) of the UN Charter,[74] one can resort to a helpful Nicaragua case,[75] which shows that the decisive factor in determining the existence of an armed conflict is the scope and scale of operations. Therefore, non-destructive cyber operations aimed, for example, at undermining the confidence of population in the government or at undermining a domestic economic situation, would most likely not be classified as attacks with the use of force.[76]

On the basis of the given viewpoint, a difference can be seen in the above described cases of Estonia in 2007 and Georgia in 2008. In Estonia the attacks did not reach the level of an armed attack and thus the international law of armed conflict did not apply. On the other hand, the operations within the Russia-Georgia

[68] James Andrew Lewis, *supra* note 43: 41.
[69] *Ibid*.: 40.
[70] *Tallinn Manual on the International Law Applicable to Cyber Warfare, 2012*.
[71] The Tallinn Manual is not an official document, but instead an expression of the scholarly opinions of a group of independent experts acting solely in their personal capacity. CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence): "Tallinn Manual - Research" // https://ccdcoe.org/research.html.
[72] *ICJ Opinion on Legality of Threat or Use of Nuclear Weapons*, July 8, 1996, alinea 39.
[73] Katarína Šmigová, "Kybernetické útoky a medzinárodné právo" (Cyber Attacks and International Law): 1225; in: *Bratislavské právnické fórum 2013 (Bratislava Legal Forum 2013)* (Bratislava: Univerzita Komenského, Právnická fakulta, 2013).
[74] 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."
[75] *Nicaragua v. USA*, ICJ Judgment of June 27, 1986, al. 195.
[76] Katarina Šmigová, *supra* note 73: 1226.

conflict have been made to support the kinetic attack, and thus the international law of armed conflict was to be applied. It was namely a case of cyber operations carried out in the context of armed conflict, which included cyber operations (cyber attacks), but at the same time was not limited to them.

This approach to cyber attacks was confirmed even by the Tallinn manual, which states that cyber operations fall under the law of armed conflict, if they are made in the context of an armed conflict, whether international or non-international.[77]

Recently, a follow-up to the above-mentioned Tallinn manual, the Tallinn Manual 2.0 was launched in 2017 within a project hosted by the NATO Cooperative Cyber Defence Centre of Excellence from 2013 to 2016. This was aimed at expanding the expert analysis to international law during peacetime. The result of this project is an extended edition of the Tallinn Manual, dealing with (among others) the following issues: internal and external sovereignty, violations of sovereignty, jurisdiction, due diligence, prohibition of intervention, cyber espionage, etc.[78]

Still, while the issue of cyber warfare and cyber attacks that go hand in hand with the development and availability of information technology, are the best examples of new threats in international relations, cyberspace is providing substantial opportunities for many other types of (postmodern and non-linear) security threats. The documents dealing with cyber security do not pay attention to one specific field related to cyber security, namely, that of misusing cyberspace for waging an information warfare. This aspect of cyberwarfare, often a tool of subversion, was addressed by Thomas Rid already in 2012, refuting the idea of cyberwars at all.[79]

Since the term "cyberwar" itself is mostly used only as a metaphor (especially in case of attacks performed outside actual use of armed force), the concept of "information war" cannot be understood otherwise, by analogy. In terms of *lex lata*, therefore, information warfare is not to be perceived as a war in legal sense (if not accompanied by kinetic attacks).[80]

The mutual relationship between cyberwarfare and information warfare could (in line with arguments proposed by Rid) be understood as being two partially overlapping areas, since "information war" can also be pursued by other than

[77] *Ibid*.: 1227.
[78] The Tallin 2.0 project explores how the general principles of international law apply in the cyber context. CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence): "Tallinn Manual - Research". https://ccdcoe.org/research.html.
[79] Thomas Rid, *supra* note 5: 5.
[80] Jack M. Beard, "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target under International Humanitarian Law," *Vanderbilt Journal of Transnational Law* 47 (2014): 139.

electronic means. Fundamentally, however, the same reservations and conclusions apply by analogy to information warfare as well as to cyber warfare. Similarly as with respect to categorization of cyber attacks, it might therefore be possible to propose a specific scale or categorization of degrees of "information attacks" – from the positive promotion, through negative promotion, false propaganda, up to the information warfare (connected to kinetic attacks).

At any rate, it can be concluded that information warfare (using electronic media/cyberspace), just like cyberwarfare, is one of the relatively new kinds of international conflicts that use modern technology, while they are blurring the differences between war and peace, which is considered an expression of the current postmodern period, marked with non-conventional conflicts. Is there yet any possibility of correctly grasping such conflicts and to have them legally categorized in the future? The previously quoted Czech philosopher Michael Hauser suggests in this regard to look for a way out of postmodernism in general, not only with respect to armed conflicts.[81] He proposes a way of negative, or transcendent modernism – in terms of rejection of negative consequences of the postmodernism,[82] leaving the self-destructive mood.[83] Should his recommendation be applied to the issue of non-linear wars, this would probably require condemning related practices as a conduct contrary to the principles of international law (such as the principle of compulsory cooperation among states,[84] non-interference in internal affairs[85] etc.), or considering this conduct as an act of crime, if meeting conditions imposed under domestic laws, thus fighting against the negative phenomena primarily with the domestic means of prevention and prophylaxis, leaving aside theoretical polemics as to whether such conduct is a war or not – especially since there is currently no will of the international community to legally categorize such acts clearly as a war in its new, postmodern sense.

CONCLUSIONS

The fact that cybersecurity is one of the key postmodern challenges was sufficiently shown in the cases referred to in this paper: be it the Russia-Georgia

[81] Michael Hauser, *supra* note 27: 245.
[82] *Ibid*.: 271.
[83] *Ibid*.: pp. 284-285.
[84] "The duty of States to co-operate with one another in accordance with the Charter" (*Cf. Declaration of Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations*, Resolution adopted by the General Assembly on October 24, 1970, Res. 2625 (XXV)).
[85] "The principle concerning the duty not to intervene in matters within the domestic jurisdiction of any State, in accordance with the Charter" (*ibid.*; *cf*. John P. Garnt and Craig J. Barker, *supra* note 30, 229; *cf*. also Peter Vršanský, Jozef Valuch, *et al*., *Medzinárodné právo verejné. Všeobecná časť (Public International Law. The General Part)* (Bratislava: Eurokódex, 2012), 150; *Cf. Nicaragua Case (Military and Paramilitary Activities in and against Nicaragua; Nicaragua v. USA)*, ICJ Reports, 1986, al. 202).

conflict (2008), in which cyberspace has become a scene of conflict between two states, or a computer worm Stuxnet deployed to harm the Iranian nuclear program (2010), regarded by many as the first cyber weapon of geopolitical significance, or the Ukrainian crisis that persists to this day. All of the examples show that traditional legal definitions of war as well as traditional expectations of a linear state-to-state conflict fail in the postmodern era. NATO Member States have therefore resolved that cyber defence is a part of collective defence, which is a shift in the traditional meaning of the collective defence within this organization. The seriousness of the situation indeed leads international bodies to take precautionary measures and to enact documents of varying legal force in order to address the respective (mostly labelled as "cyber") threats.

The essential subject matter of this paper is the relationship between new types of postmodern conflicts and the law of armed conflicts (law of war). Based on the ICJ case law, it is clear that under current legal rules of international law of war, cyber attacks as well as information attacks (often performed in the cyberspace as well) can only be perceived as "war" if executed in addition to a classical kinetic warfare, which is often not the case. In most cases, perceived "only" as a non-linear warfare (postmodern conflict), this practice nevertheless must be condemned as a conduct running contrary to principles of international law and (possibly) a crime under national laws, unless this type conduct will be recognized by the international community as a "war" proper, in its new, postmodern sense.

BIBLIOGRAPHY

1. Beard, Jack M. "Legal Phantoms in Cyberspace: The Problematic Status of Information as a Weapon and a Target under International Humanitarian Law." *Vanderbilt Journal of Transnational Law* 47 (2014): 67–143.
2. Bishop, Jonathan. "The effect of de-individuation of the Internet Troller on Criminal Procedure implementation: An interview with a Hater." *International Journal of Cyber Criminology* (IJCC) 7 (2013): 28–48.
3. Brenner, Susan W., and Leo L. Clarke. "Civilians in Cyberwarfare: Conscriptions." *Vanderbilt Journal of Transnational Law* 43 (2010): 1011–1076.
4. Brunner, Elgin, Anna Michalkova, Manuel Suter, and Myrian Dunn Cavelty. *Focal Report 3: Critical Infrastructure Protection – Cybersecurity – Recent Strategies and Policies: An Analysis, CRN Reports*. Zurich: Center for Security Studies, 2009.

5. Clapper, James R. "Worldwide Cyber Threats" (September 10, 2015) https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/clapperopening09102015.pdf.
6. Firnhaber-Baker, Justine. "From God's Peace to the King's Order: Late Medieval Limitations on Non-Royal Warfare." *Essays in Medieval Studies* 23 (2006/7): 19–30.
7. Firnhaber-Baker, Justine. "Introduction: History, historians, and seigneurial war": 1–23. In: *Violence and the State in Languedoc, 1250–1400* (Cambridge: Cambridge University Press, 2014).
8. Gaus, Arthur. "Trolling Attacks and the Need for New Approaches to Privacy Torts." *University of San Francisco Law Review* 47 (2012-2013): 353–376.
9. Geers, Kenneth, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015 // https://ccdcoe.org/multimedia/cyber-war-perspective-russian-aggression-against-ukraine.html.
10. Gosnell Handler, Stephanie. "The New Cyber Face of Battle: Developing a Legal Approach to Accommodate Emerging Trends in Warfare." *Stanford Journal of International Law* 48 (2012): 209–237.
11. Grant, John P., and Craig J. Barker. *Parry & Grant Encyclopaedic Dictionary of International Law.* 3rd ed. Oxford: Oxford University Press, 2009.
12. Greenwald, Glenn. "How Covert Agents Infiltrate the Internet to Manipulate, Deceive, and Destroy Reputations" // https://firstlook.org/theintercept/2014/02/24/jtrig-manipulation/.
13. Hauser, Michael. "Za hranice postmodernismu" (Beyond the Frontiers of Postmodernism): 223–286. In: Roman Kanda, *et al*., *Podzim postmodernismu: Teoretické výzvy současnosti (The Fall of Postmodernism – the Theoretical Challenges of Present Days)*. Praha: Filosofia, 2016.
14. Hiller, Janine S. "Civil Cyberconflict: Microsoft, Cybercrime, and Botnets." *Santa Clara High Technology Law Journal* 31 (2015): 163–214.
15. Kanda, Roman, *et al*. *Podzim postmodernismu: Teoretické výzvy současnosti (The Fall of Postmodernism – the Theoretical Challenges of Present Days).* Praha: Filosofia, 2016.
16. Kramer, Franklin D., Stuart H. Starr, Larry K. Wentz, and Daniel T. Kuehl. *Cyberpower and National Security*. Washington: Potomac Books Inc., 2009.
17. Lee, Dave. "Top US military Twitter feed 'hacked by Islamic State'." (January 12, 2015) // http://www.bbc.co.uk/newsbeat/article/30781377/top-us-military-twitter-feed-hacked-by-islamic-state.

18. Lewis, James Andrew. "Compelling Opponents to Our Will: The Role of Cyber Warfare in Ukraine": 39–47. In: Kenneth Geers, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015.
19. Macková, Veronika. "Cyber War of the States: Stuxnet and Flame Virus Opens New Era of War" // http://cenaa.org/wp-content/uploads/2014/05/Veronika-Mackova-PP-No.-15-2013-Vol.-2.pdf
20. Margulies, Peter. "Sovereignty and Cyber Attacks: Technology´s Challenge to the Law of State Responsibility." *Melbourne Journal of International Law* 14 (2013): 496–519.
21. Masariková, Monika. "Potvrdené. Kyberútoky predmetom článku 5 NATO" (Confirmed. Cyberattacks are subject to Art. 5 NATO) (September 5, 2014) // http://www.cybersec.sk/spravy/politika/potvrdene-kyberutoky-predmetom-clanku-5-nato/.
22. Melková, Michaela, and Tomáš Sokol. "Kybernetický priestor ako nová dimenzia národnej bezpečnosti" (Cyber Space as the New Dimension of the National Security): 54–64. In: *Bezpečnostné fórum 2015.* Banská Bystrica: Belianum, 2015.
23. Neff, Stephen C. *War and the Law of Nations. A General History*. Cambridge: Cambridge University Press, 2005.
24. Nicol, Sarah. "Cyber-bullying and trolling." *Youth Studies Australia* 31 (2012): 3–4.
25. O'Connell, Mary Ellen. "Cyber Security without Cyber War." *Journal of Conflict & Security Law* 17 (2012): 187–209.
26. Reich, Pauline C., Stuart Weinstein, Charles Wild, and Allan S. Cabalong. "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity." *European Journal of Law and Technology*, 1 (2010): 1–58.
27. Remus, Titiriga. "Cyber-attacks and International law of armed conflict; a 'jus ad bellum' perspective." *Journal of International Commercial Law and Technology* 8 (2013): 179–189.
28. Rid, Thomas. "Cyber War Will Not Take Place." *The Journal of Strategic Studies* 35 (2012): 5–32.
29. Roscini, Marco. *Cyber Operations and the Use of Force in International Law.* Oxford: Oxford University Press, 2014.
30. Schmit, Michael. "Classification of Cyber Conflict." *Journal of Conflict & Security Law* 17 (2012): 245–260.

31. Schmitt, Michael N. "Computer network attack and the use of force in international law: thought on a normative framework." *Columbia Journal of Transnational Law* 37 (1999): 885–937.
32. Shackelford, Scott J. "Estonia Two-and-a-Half Years Later: A Progress Report on Combating Cyber Attacks" // https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1499849.
33. Shackelford, Scott J. "From Nuclear War to Net War: Analogizing Cyber Attacks in International Law." *Berkeley Journal of International Law* 27 (2009): 192–251.
34. Sharp, Walter Gary. *Cyberspace and the use of force*. Falls Church, Virginia: Aegis Research Corp., 1999.
35. Šmigová, Katarína. "Kybernetické útoky a medzinárodné právo" (Cyber Attacks and International Law): 1224–1230. In: *Bratislavské právnické fórum 2013 (Bratislava Legal Forum 2013)*. Bratislava: Univerzita Komenského, Právnická fakulta, 2013.
36. Smith, David J. "Russian Cyber Strategy and the War Against Georgia" (January 17, 2014) // http://www.atlanticcouncil.org/blogs/natosource/russian-cyber-policy-and-the-war-against-georgia.
37. Smoleňová, Ivana. "Campaign in the Czech Republic and Slovakia: Types of Media Spreading Pro-Russian Propaganda, their Characteristics and Frequently Used Narratives" // http://www.pssi.cz/download/docs/253_is-pro-russian-campaign.pdf.
38. Stinissen, Jan. "A Legal Framework for Cyber Operations in Ukraine": 123–134. In: Kenneth Geers, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015.
39. The Economist. "A Cyber-riot" (May 10, 2007) // http://www.economist.com/node/9163598.
40. Valuch, Jozef, Michaela Rišová, and Radoslav Seman. *Právo medzinárodných organizácií (The Law of International Organisations).* Praha: C. H. Beck, 2011.
41. Vršanský, Peter. "The United Nations Charter entered into force 70 years ago (is the twilight of the United Nations near?)." *Slovak yearbook of international law* 5 (2015): 6–21.
42. Vršanský, Peter, Jozef Valuch, *et al*. *Medzinárodné právo verejné. Všeobecná časť (Public International Law. The General Part)*. Bratislava: Eurokódex, 2012.
43. Weber, Max. "Politics as a Vocation" // http://anthropos-lab.net/wp/wp-content/uploads/2011/12/Weber-Politics-as-a-Vocation.pdf.

44. Wirtz, James J. "Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy": 29–37. In: Kenneth Geers, ed. *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn: NATO CCD COE Publications, 2015.
45. Žižek, Slavoj. *Welcome to the Desert of the Real! Five Essays on September 11 and Related Dates.* London: Verso, 2002.

LEGAL REFERENCES

1. *An Outline for European Cyber Diplomacy Engagement*. 9967/4/14 REV 4, DG D 1C, Brussels, September 2014.
2. *Australian Government Cyber Security Strategy, 2009* // http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf.
3. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. JOIN(2013) 1 final, Brussels, 2013.
4. *Declaration of Principles of International Law Concerning Friendly Relations and Cooperation among States in Accordance with the Charter of the United Nations*. Resolution adopted by the General Assembly on October 24, 1970, Res. 2625 (XXV).
5. *ICJ Opinion on Legality of Threat or Use of Nuclear Weapons*. July 8, 1996, alinea 39.
6. *Koncepcia kybernetickej bezpečnosti Slovenskej republiky (Conception of Cyber Security of the Slovak Republic)* // https://lt.justice.gov.sk/Attachment/Vlastn%C3%BD%20materi%C3%A1l_docx.pdf?instEID=-1&attEID=75645&docEID=413095&matEID=7996&langEID=1&tStamp=20150218154455240.
7. *Letter dated January 9, 2015 from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations, addressed to the Secretary-General*. United Nations, General Assembly, A/69/723, 2015.
8. *Nicaragua Case (Military and Paramilitary Activities in and against Nicaragua; Nicaragua v. USA)*. ICJ Reports, 1986, al. 202.
9. *Nicaragua v. USA*. ICJ Judgment of June 27, 1986, al. 195.
10. *Nové hrozby - kybernetické dimenzie (New risks – cyber dimensions)*. NATO Review //

http://www.nato.int/docu/review/2011/11-september/cyber-Threads/SK/index.htm.

11. *Report of Independent International Fact-Finding Mission on the Conflict in Georgia*. Vol. I., September 2009 // http://echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf.
12. *Report of the Independent Fact-Finding Mission on the Conflict in Georgia*. Vol. II, September 2009 // http://www.mpil.de/files/pdf4/IIFFMCG_Volume_II1.pdf.
13. *Report of the Secretary-General's High-level Panel on Threats, Challenges and Change (2004)* // http://www.un.org/en/peacebuilding/pdf/historical/hlp_more_secure_world.pdf.
14. *Report on Developments in the Field of Information and Telecommunications in the Context of International Security.* United Nations, General Assembly, Group of Governmental Experts, A/70/174, July 22, 2015 // http://www.un.org/ga/search/view_doc.asp?symbol= A/70/174.
15. *Report on Developments in the Field of Information and Telecommunications in the Context of International Security*. United Nations, General Assembly, Group of Governmental Experts (GGE). A/68/98, June 24, 2013.
16. *Tallinn Manual – Research*. CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) // https://ccdcoe.org/research.html.
17. *Tallinn Manual on the International Law Applicable to Cyber Warfare, 2012*.