Bogusław Olszewski

University of Wroclaw

From a*d hoc* cyber peace operations to HyperState.
The outline of the future peace support.
Part I

Anything that reduces war-related destruction should not be considered altogether immoral

Herman Kahn

Abstract

The article raises the question of the possibility of hackers' involvement in the cyber peace operations. Currently, in the evolving surroundings of post-Westphalian regime, reveals a trend to progressive militarization of cyberspace which affects the social sphere and citizens. Facing the proposed and actual participation of IT professionals in hostilities, as well as noticeable indolence of the States in the context of ensuring security for non-combatants, it falls to focus on the possible ways of use this potential in the field of enforcement of humanitarian law. This leads to the conclusion that the civilian population from a passive recipient of International Humanitarian Law could become its maker, as an active participant in peace operations carried out in inflammatory points of the globe. The two models described below provide for a gradual involvement of the civilian population, leading ultimately towards structural change. All these solutions are just a starting point, a short introduction to the broader discussion in perspective of the future studies and peace science. The proposed point of view is more pragmatic than an idealistic one.

Keywords: cyberspace, cyber peace operations, hackers, civilians, post-Westphalian, HyperState.

Introduction

The war has been accompanying the man since almost the dawn of time – as it is claimed by some researchers in the field of anthropology, psychology, archeology or history, among them there are also scientists locating the source of armed conflicts in the human nature itself, perceiving it as being inherently evil, imbued with lust for murder and destruction, and treating the war itself as indispensable in human relations. For the ancient thinkers waging the war was justified,[1] for Romans it was a 'just' war (*bellum iustum*) or 'unjust' war (*bellum iniustum*) depending on whether its characteristic procedures of its denounce and conduct, which until about the third century BC were complied by *ius fetiale*. In this way the basics were founded, on which the later Middle Ages built the concept of a 'just war' (*ius bellum iustum*).[2] Also the theories of the Enlightenment had recognized armed struggle as legitimate, even if it had offensive character.[3]

Massification of the war, the introduction of universal conscription and the rapid spread of warfare technology, accompanying the Industrial Revolution, contributed to the escalation of violence on the battlefield. It took place in two directions: the part of the civilian population was forcibly and for large-scale embroiled in armed activities, whilst others, non-combatants, often became victims of their activities. Thus, people not involved directly in military operations, had felt the consequences of war even in historical times, dying at the hands of soldiers stationed in the villages or in urban barracks, not to mention about regular armed conflicts. The current ability of military influence on the all areas of social life meant that civilians are increasingly not only random victims of military operations, but they became the target group which even is chosen with premeditation, especially by non-state actors. They found themselves not only in the striking distance of advanced weapons used by the warring armies, but as a relatively easy target in the form of unarmed opponents are the victims of a series of war aberrations known as from the past, as well as contemporary asymmetrical conflicts. The ongoing radicalization of actions taken against non-combatants evolves from the acts of terrorism to the regular carnage that has gradually become the *modus operandi* of the entities applying their own notions of ethics on the battlefield, or which of rule that do not respect any norms. At present on the international stage the main features of modern war are actualising: dehumanisation, massification,

[1] See H. Syse 'Plato: The Necessity of War, the Quest or Peace' (2002) 1(1) Journal of Military Ethics 36–44; also Aristotle defined the conditions that make 'just war': Aristotle *The Politics* (A & D Pub. Blacksburg Virginia 2009); the ancient Romans belived that war could be *pium* or *iustum*: J. von Elbe 'The Evolution of the Concept of the Just War in International Law' (1939) (33) American Journal of International Law 666-667; also: A. Nussbaum 'Just War – A Legal Concept?' (1943) 42(3) Michigan Law Review 453-479; Cicero about 'just war': M. T. Cicero, N. Rudd and J. G. F. Powell *The republic, and The laws* (Oxford University Press Oxford 2008).

[2] Just war does not have to be purely defensive, but also offensive; see Augustine Saint Bishop of Hippo and M. Dods *The city of god*, (Hendrickson Publishers Peabody Massachusetts 2013); also: Isidore of Seville and W. M. Lindsay *Isidori Hispalensis Episcopi Etimologiarum Sive Originum*, Libri XVIII (1) (E Typographeo Clarendoniano Oxoni; Oxford University Press Oxford 1911).

[3] See F. Bacon *New Atlantis* (Cambridge University Press Cambridge 2010); also: F. Suarez and L. Pereña *Guerra, Intervención, Paz Internacional* (Espasa-Calpe Madrid 1959) at pp. 76-77.

totality, a general mobilization, militarised all areas of life, the fascination with technology.

Though the following text has the characteristics of an informal, active normative forecast, it is purely illustrative and does not claim right to suggest any law solutions or axiological ones. The main objective of this publication is an attempt to diversify the spin which is visible in mainstream discourse about cyberspace. An outline of the concept of alternative cyber peace operations presented hereafter of this paper, has to provide the inspiration for the search for effective forms of support relevant institutions operating in the field of establishing and maintaining peace. The main intention of the author is submitting the proposed models under discussion that would indicate their legal restrictions, the consequences of implementation, and real guidelines for the future transformation.

War, State and cyberspace

Currently, the nature of war is changing, and the range of military operations and methods of combat known from historical times are replaced with newer, more and more effective, moving towards post-modern forms. High technology, the evolution of military strategy and the erosion of traditional standards for the conduct of the armed struggle are accompanied by the transfer of joint responsibility for the war to the civilian sphere: 'War [...] now takes place *everywhere* [...] and involves or affects nearly everyone in the area.'[4] One of the reasons for this position, is the growing inability of authorized entities to enforce the provisions of international humanitarian law (IHL), which despite its universality (although with hindsight in some cases questionable) increasingly do not fulfill its role. This fact has significant implications for citizens, excluded hitherto from the broader context of military action. There is an impression arising that the society of the modern world gravitates towards the total war, carried out of new ways and using previously unknown means. It takes place mainly locally, including the form of proxy wars, frozen conflicts and low-intensity conflicts, but its effects are global, destabilizing the international environment. The introduction and evolution of electronic means of fighting meant that the war was intensified and it is accompanied by the increasing development and implementation of advanced information technologies. In the focus of the international community there is also the issue of the military impact through cyberspace on the real world,[5] as well as all the consequences of this fact, including the possibility of obtaining combat goals through it, especially physical effects (kinetic): 'Our increasing dependence on computerized and highly networked environments is generating considerable new threats where the two spaces

[4] L. Blank and A. Guiora 'Teaching an Old Dog New Tricks: Operationalizing the Law of Armed Conflict in New Warfare' in E. L. Gaston (ed) *The Laws of War and 21st Cenury Conflict* (International Debate Education Association New York 2012) at p. 87.

[5] S. K. Das, K. Kant and N. Zhang *Handbook on Securing Cyber-Physical Critical Infrastructure* (Morgan Kaufmann Waltham Massachusetts 2012).

overlap'.[6] The progressive militarisation of civilian cyberspace is also a response to the growing influence of non-state actors.

Issues relating to cybersecurity, including the cyber terrorism, cyber crime and cyber war, currently occupy an important place in discussions not only on the academic grounds, but primarily in the field of international politics. All of this is reflected in two major trends accompanying this state of affairs, namely relevant to securitisation and desecuritisation[7] of cyberspace as well as its growing share in ongoing and potential hostilities. In the context of military conflicts, the civilians' participation in defensive operations in cyberspace is postulated openly.[8] It blurs the status of persons who are not soldiers and the right to protection of the rights flowing from the status of being civilian is now becoming one of the most important legal issues. *Consensus omnium* in the formula of the involvement of civilians in peace operations, including the conflicts which in the long run could deprive them of that status, seems to be in this context as the most possible.

War and peace in the post -Westphalian cyberspace

Westphalian regime 'covers the period of international law and regulation from 1648 to the early twentieth century (although elements of it, it can be argued plausibly, still have application today).'[9] It is closely related to the issue of sovereignty, due to this fact countries are independent and equal in the international arena. One of the most important documents of the Westphalian order came into being in the frame of the most important documents included in the canon of IHL: from the Declaration of Paris of 1856, through the Geneva Convention of 1864, to the Hague Conventions (of 1899 and 1907), as well as the Geneva Conventions (of 1929 and 1949). They became the starting point for further evolution of standards: 'As a result, arms control and regulation have become a permanent feature of international politics.'[10] Cyberspace seen from the point of view of the state actors is therefore an element which is subject to their sovereignty.[11] The exception from this approach can only be the implementation of the regulation developed on the international platform: 'Many

[6] G. Loukas *Cyber-Physical Attacks: A Growing Invisible Threat* (Elsevier/Butterworth-Heinemann Oxford United Kingdom Waltham Massachusetts 2015) at p. 2.

[7] Temporary desecuritisation of cyberspace took place after the Cold War period.

[8] The Lithuanian authorities assume the participation of citizens in cyberwarfare in the event of an attack and possible occupation of the country; see K. Aleksa (ed), *Ką turime žinoti apie pasirengimą ekstremaliosioms situacijoms ir karo metui* (Krašto apsaugos ministerija Vilnius 2014) p. 70 <www.kam.lt/download/46229/ka%20turime%20zinoti%20(knyga%202014)%20sk.pdf> (date accessed 13 November 2015).

[9] D. Held 'The changing structure of international law: sovereignty transformed?' in D. Held, A. McGrew (eds) *The Global Transformations Reader: an Introduction to the Globalization Debate* (Polity Press Cambridge UK), p. 162 at <https://www.polity.co.uk/global/pdf/GTReader2eHeld.pdf> (date accessed 13 November 2015).

[10] *Ibid*, at 165.

[11] See M. N. Schmitt (ed) *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, New York 2013) at <https://ccdcoe.org/tallinn-manual.html> (date accessed 13 November 2015) pp. 15-18.

recent agreements, moreover, have created mechanisms of verification or commitments that intrude significantly on national sovereignty and military autonomy.'[12] Alone peacekeeping operations now concern primarily actions on the physical plane, including kinetic military actions, even if they are backed by actions in cyberspace or by means of electronic warfare. This follows from the still axial role of the geographical territory and the physical realm in the modern war, hence peace operations are still discussed in the context of legal regulations specific to the Westphalian order, and invariably are associated with this issue.

Acceptance of this perspective affects the concepts related to cyber war. Given that, beyond violence, the additional attribute of war as itself is its instrumental and political nature, it is dispute the very possibility of war in cyberspace. Some authors, including Thomas Rid, argue that nowadays 'cyberwar will not take place', since: 'A real act of war is always potentially or actually lethal, at least for some participants on at least one side.'[13] This does not change the fact that at any moment can appear an incident in cyberspace directly affecting the low-intensity conflict or interstate tensions, which may ultimately lead to the outbreak of kinetic war at local or regional level. Even while maintaining the above perspective, at the present stage acts of cyber espionage or cyber-sabotage are a potential prelude to physical combat, and as such should be the target of the cyber peace operation (even cyber conflict prevention). In this context, one can locate Dinstein's words, who says about the following sequence: 'non violent means, but violent consequences.'[14] In addition, Thomas Rid concludes that 'political purpose legitimates the use of force; an intention has to be articulated.'[15] Meanwhile, it is worth noting in the case of many hybrid wars that formal declaration does not occur, just as precise goal formulation. The involvement of violent non-state actors makes maintaining rigid principles of armed conflict is not formalized in a manner characteristic of the Westphalian order, especially in the environment of cyberspace. Due to the multiplicity of approaches to this problem, some authors stress that currently the international system is not yet post-Westphalian, but late-Westphalian.[16] For the purpose of this article is, however, highlighted a two-stage international order: Westphalian and post-Westphalian. The latter will also mean the Westphalian order in transition.

It should be noted that even if the current cyber operations can not yet be called a cyberwar, all attempts to desecuritisation of this field are now doomed to failure. An important question is, in this context, whether at the present stage of doctrine evolution of cyberwar its range can be still reduced, even by recognizing certain resources of cyberspace as intangible heritage of humanity and entering

[12] D. Held, *op cit*, at 165.

[13] T. Rid, 'Cyber war will not take place' in P. Ducheine, F. Osinga, and J. Soeters (eds) *Cyber Warfare. Critical Perspectives* (Asser Press Hague 2012) p. 75.

[14] Y. Dinstein 'Computer Network Attacks and Self-Defense' in M. N. Schmitt and B. T. O'Donell (eds) International Law Studies (2002) (76) 99-119.

[15] T. Rid, *op cit*, p. 76.

[16] See M. Pietraś and K. Marzęda (eds) *Późnowestfalski ład międzynarodowy* (Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej Lublin 2008).

them on the Representative List of the Intangible Cultural Heritage of Humanity.[17] In the case of ephemeral data sets it seems to be completely unrealistic, since today the neutral status of physical protected natural areas is still disputed – example of acts of military and economic nature which are currently run around the Arctic or Antarctic[18] seem to confirm this fact. This question makes 'fresh discussion about the development, use and control of cyberweapons and of surveillance technologies in cyberspace. What are the implications of these technologies for arms production and arms control? How realistic is it to try to control them through traditional arms control mechanisms?'[19]

Cyberspace and global security

Contemporary polemology and irenology were confronted with the reality shaped by cyber operations conducted in electronic communication space. The evolution of ICT systems is in fact partly the result of the defense research conducted in the realities of the Cold War,[20] and like that in the near future will remain, given the current saturation of military art by cutting-edge technologies, as well as its further evolution and the increasing complexity of measures of fighting. The concept of global order, based on the Westphalian system, is becoming a subject to verification towards post-Westphalian regime, which does not automatically mean that the previous approach will ultimately be rejected in its entirety. It can be concluded that it is in the moment of transition, which in perspective may even, paradoxically, lead to its strengthening. Being still in the stage of transformation, makes it enables to effectively resolve completely new international legal problems its functioning unknown for centuries.

Implications connected with the advent of post-Westphalian regime relate generally to a level at which international or regional operations act, much space is devoted to the emancipation trends occurring in societies: 'Security, defence of privilege, identity, recognition and cultural traditions, which once coincided with the boundaries of the post-Westphalian state, are now altered, uncertain, liquid.'[21] From the point of view of the citizen, the erosion of national sovereignty causes the threats posed by these violent non-state actors (VNSA) who had hitherto had limited field of action, or who had not acted at all. This raises the question whether in the context of globalization one can talk about increasing sovereignty of the individual and its ability to maintain their own security, or is it only

[17] Lists of Intangible Cultural Heritage and the Register of Best Safeguarding Practices, <http://www.unesco.org/culture/ich/en/lists> (date accessed 13 November 2015).

[18] The Antarctic Treaty (1 December 1959) expires in 2041, which could cause a series of territorial claims submitted by its signatories; more: 'The Antarctic Treaty' <http://www.ats.aq/e/ats.htm> (date accessed 13 November 2015).

[19] V. Boulanin, *Arms production goes cyber: a challenge for arms control* (SIPRI 2015) at <http://www.sipri.org/media/newsletter/essay/Boulanin_May13> (date accessed 13 November 2015).

[20] See J. Abbet *Inventing the Internet* (The MIT Press Cambridge Massachusetts 2000).

[21] C. Bordoni 'A Crisis Of The State? The End Of The Post-Westphalian Model' (12 February 2013) at <http://www.socialeurope.eu/2013/02/a-crisis-of-the-state-the-end-of-post-westphalian-model/> (date accessed 13 November 2015).

exposed to increasing danger connected with blurring of traditional national boundaries and with a growing inability of governments to protect their rights. Positive answer associated automatically with the need to determine the exact catalog of rights of the individual in the context of human security, including those that are not strictly related to IHL standards characteristic for the order based on the Peace of Westphalia. Most of the provisions of IHL concern the status of the individual in conflicts involving the State-actor often seems to be inadequate: 'These inadequacies of humanitarian law are, to some degree, psychological: it is illusory to think that the law can keep pace with evolving reality, which become more and more complex and tends to slip past the constraints of legal rules.'[22]

The dominant approach to cyberspace in the form of layers is State-centric, geographical and physical components (hardware) are considered as its base, underlying logical layer (software)[23] and social (including cyber social). Hence, from the classical (kinetic), military point of view, the physical part of cyberspace ultimately seems to be the most important[24] and and in this perspective it is defined by U.S. Army: 'A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.'[25] An attack on any part of the ICT critical infrastructure, without which the State is excluded from the global information grid and data flow is primarily considered in the context of kinetic effects (geographical location and physical components of the network, the target devices supported by ICT), and only then logical (software, protocols network data) and social (cyber-identity, real individuals, groups). A shift of focus on the logic and social layers of cyberspace can diversify this approach, also in view of the conclusions related to the psychology of cyberspace[26] to the effect that: 'Human minds are the targets, not machines.'[27]

Thus, the reference point remains the construct relating to post-Westphalian regime based structurally on the States and on the existing international institutions. It will be a logical-centric and law-centric model, relating to human rights and human security. Shifting the focus to the individual takes places due to the fact that currently, as writes Kohki Abe, we are facing the process of 'Human Rights-ization of International Law.'[28] This is due to the fact that 'there is a need to see modern international politics not as an era or epoch, but as a practice of distinguishing the present from the

[22] A. Cassese 'Current challenges to international humanitarian law' in A. Clapham and P. Gaeta (eds) *The Oxford handbook of international law in armed conflict* (Oxford University Press Oxford 2014) p. 7.

[23] *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028* Department of the Army USA TRADOC Pamphlet 525-7-8 (22 February 2010) at <http://fas.org/irp/doddir/army/pam525-7-8.pdf> (date accessed 14 November 2015) p. 6.

[24] See also 'Sovereignty, jurisdiction and control' in M. N. Schmitt (ed), *op cit*, pp. 15-41.

[25] *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, *op cit*, p. 8.

[26] A. Barak and J. Suler 'Reflections on the Psychology and Social Science of Cyberspace' in A. Barak (ed) *Psychological Aspects of Cyberspace: Theory, Research, Applications* (Cambridge University Press Cambridge New York 2008) pp. 1-12.

[27] T. Rid, *op. cit*, p. 90.

[28] K. Abe 'Human Rights-ization of International Law: a Critical Analysis of the «Ethical Turn»' in Kokusaihō gaiko zasshi(2013) (111) 1-28 at <http://catalogue.ppl.nl/DB=1/SET=1/TTL=211/SHW?FRST=216> (date accessed 13 November 2015).

past as a way of making claims about the foundations of legitimate authority.'[29].

The outline of *ad hoc* cyber peace operations

Like the classic peace operations, cyber peace operations would be implemented by Member States within the framework of the United Nations Department of Field Support (DFS), or directly by the Department of Peacekeeping Operations (DPKO).[30] In category 'Troop and police contributors'[31] there could appear the category 'cyber forces' and all the States would provide IT professionals in the same way as they provide military experts, troops and police for UN peacekeeping and other types of peace operations. This combined group would support the classic peace enforcement missions, and in the early stages would be effective even without a broader physical intervention – if only State which is responsible of breach of IHL standards could have a sufficiently developed IT infrastructure. Cyber forces of the States, operating under the aegis of the UN, would create separate *ad hoc* teams responsible for the conduct of cyber peace operations in the given region. This would be consistent extension current *modus operandi* of the United Nations into cyberspace. Depending on the basis of interventions they would remain in collaboration with the government of the country embraced peacekeeping operations or they would act in the direction of peace and its maintenance, regardless of his position. Cyber operations can be used in each of the types of peace operations, from conflict prevention to the peace building.

Thus, for example, The United Nations-African Union Hybrid Force in Darfur (UNAMID) would have a mandate authorizing them to conduct all necessary operations in cyberspace of that State, which would be carried out with the support of dedicated cyber forces of the UN Member States and as such increase the chances for success of the mission. This type of support is not unfounded, especially in view of the expected development of ICT in the areas previously considered to be insufficiently equipped in this respect – South Sudan[32] and Liberia[33] are here a prime example. The challenge for this type of operation would be a precise definition of the responsibilities for the effects,[34] and precise

[29] T. Marshall 'Perpetual Westphalia? Exploring Westphalian and Non-Westphalian Politics Through Aleatory Materialism' at <https://www.google.nl/urlsa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDQQFjABahUKEwj1iPPys4DJAhXEUhQKHTPiDp0&url=https%3A%2F%2Fmillenniumjournal.files.wordpress.com%2F2012%2F10%2Fmarshall-materialism-paper.docx&usg=AFQjCNGr5Xw5Cc1wBZabzJrtIw1hlLw1g&bvm =bv.106923 889,d. d24&cad=rja> (date accessed 13 November 2015).

[30] See 'United Nations Peacekeeping Group: Capacities to Ensure Integration' at <http://www.un.org/en/peacekeeping/documents/dpkodfs_org_chart.pdf> (date accessed 13 November 2015).

[31] 'Troop and police contributors' <http://www.un.org/en/peacekeeping/resources/statistics/contributors.shtml> (date accessed 13 November 2015).

[32] 'South Sudan accelerates ICT in all sectors' at <http://www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/in-focus-articles/2015/south-sudan-accelerates-icts-in-all-sectors> (date accessed 13 November 2015).

[33] 'Liberia's ICT and Telecom Policy' The Ministry of Commerce and Industry' at <http://www.moci.gov.lr/doc/ICT%20_%20Telecom%20Policy%20Main%20Body.pdf> (date accessed 13 November 2015).

[34] See B. Boutin *The Role of Control in Allocating International Responsibility in Collaborative Military Operations*

definition of the objectives and methods of operation, which *de facto* would remain often on the verge of legality. This would allow to put a question about the possibility of use in such cases the principles of necessity, known for criminal law.[35] Support for peace operations would occur in the range also known from the field of military: 'cyber warfare (CyberWar), cyber network operations (CyNetOps), cyber support (CyberSpt).'[36] Another solution could be the creation of teams of civilian IT professionals who would have a mandate to lead cyber operation on behalf of the UN, excluding military component. This form would autonomize them a little from the good will of the Member States which post their resources in varying degrees. Due to the purpose and nature of these activities, they would do not provoke so much controversy as the involvement of civilians in the interstate cyber conflict whether in internal conflict with the participation of violent non-state actor.

In addition to the potential involvement of civilian computer scientists and cyber security specialists, invaluable service in the conduct of peace cyber operations which would support UN peace missions, could give hacktivists and hackers (crackers). Because it is the States' control of the armed forces, trying to use them to interact with cyber security in local and global scale, the use of hackers and hacktivists would bypass the limitations and risks associated with the use cyber forces within the DPKO, which would expose the country of their origin for a possible retaliation. This would allow for a more effective and wider intervention of peacekeepers and strengthening the enforcement provisions of IHL in countries such as South Sudan (UNMISS) and the Democratic Republic of Congo (MONUSCO), and also where there exists a genuine lack of effective response to the unlawful operation of non-state actors and where the escalation of violence against the civil population takes place. Offensive cyber attack coordinated by the UN and aimed at those who make violations of IHL would be an acceptable option. Also psychological aspects of such an attack can not be overestimated, apart from the obvious embarrassment of the government or non-state actor which are fleeing to violations provisions of humanitarian law. This would be requirement to UN to legalize the use of force in cyberspace for the purposes of peace operations and development towards offensive cyber warfare.

Extension of the model of *ad hoc* cyber operations would be network of hosts made available by organizations such as the UN, NATO or the EU. In order to fulfill a specific range of operational activities, exclusively verified and licensed hackers would be entitled to connecting to the hosts. They would provide services to support the cyber peace operations conducted by Joined Cyber Commands with a UN mandate, or as part of stabilization operations under the aegis of NATO. They would be personally responsible for the implementation of outsourced tasks associated with the missions, they would be subject of strict regulations, and the hosts would be separated from the military part of the Internet to minimize the risk of unauthorized intrusions into military systems. Cyber attacks

(SHARES Amsterdam 2015) Ph.D. thesis Amsterdam Center for International Law of the University of Amsterdam.

[35] E. B. Arnolds and N. F. Garland 'The Defense of Necessity in Criminal Law: The Right to Choose the Lesser Evil' Journal of Criminal Law and Criminology (1974) 65(3) 289-301.

[36] *The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028*, *op. cit*, p. iv.

conducted by ideologically motivated hackers could also be used in operations providing peace. Such a possibility would find perhaps a wide response among hacktivists and hackers, as we are talking primarily about the so called White Hats.[37]

In this way, the potential would be involved in the cyber peace operations, which is currently used in acts of contestation of social and political realities, which in fact are the result of global processes, including armed conflicts in the local and regional level. Wikileaks, Anonymous or splinter-group of Anonymous, LulzSec (Black Hats), could therefore rethink its approach to global issues through participation in these activities. In addition to direct employment in the framework of the UN, some hackers could carry out short-term orders, and some of them (on the basis of the certificate obtained in the UN) could be hired by institutes associated with the research on peace, as SIPRI, RAND or other non-governmental organizations. Similar groups of hackers, engage as a full-time position or volunteers, could have the ICRC. In addition, for the purpose of the peacekeeping operation, including the development of an effective plan of that support, international organizations would engage hackers on the principle of competition, offering determined financial gratification for the best group. In the case of option which assumes the use of hard power and assumes the leading role of the army, hackers could attach themselves to military operations by downloading the appropriate software from milCERT or MoD Defence Cyber Command.

The next level of *ad hoc* peace operations conducted in cyberspace assumes a broad involvement of the civilian population. The UN employs at present 16.791 people in the frame of civilian personnel, which are used for the purpose of conducting 16 missions.[38] Knowledge-based economy generates a large number of people with university computer degree. Rising expenditure on education in the field of IT and the relatively high numbers of talented professionals from the industry could make the human resources available in a wider range. Pioneering solutions for the participation of civilians in the broadly defined humanitarian operations have already been implemented, as actions relating to emergency telecommunications networks[39], as well as the UN Global Pulse[40] program, which involve a wide social participation in the area of Big Data. It seems that in the face of the controversy connected with ceding the potential of such powers to contractors (PMCs) is a solution worthy of attention. The more it contributes to an even greater democratization of peace operations and to the direct involvement of citizens.

As part of the operation would have been authorized and carried out by the UN, civilians could

[37] D. Barney 'White Hat Hackers – the forgotten good guys' (31 March 2015) at <http://www.gfi.com/blog/white-hat-hackers-the-forgotten-good-guys/> (date accessed 13 November 2015).

[38] 'Peacekeeping Fact Sheet' (31 August 2015) at <http://www.un.org/en/peacekeeping/resources/statistics/factsheet.shtml> (date accessed 13 November 2015).

[39] 'Emergency Communications for Disaster Relief Deployment Archive' at <http://www.unfoundation.org/what-we-do/legacy-of-impact/technology/disaster-relief-deployments/> (accessed 13 November 2015).

[40] 'United Nations Global Pulse. Harnessing big data for development and humanitarian action ' at <http://www.unglobalpulse.org/about-new> (accessed 13 November 2015).

download so called Peace Software, operating in the same way as the SETI@home software,[41] allowing to share their own computer as part of the computational grid of DPKO or setting it up as a part of botnet used in conflict prevention, peace enforcement, peacekeeping and peace building operations carried out in cooperation with authorized institutions and international organizations. Such a botnet used in peace operations would have authorized by legal and military institutions. It could be similar to operations already known from contemporary conflicts, as '«Operation „Cast Lead» in January 2009 [...] One notable pro-Israeli initiative was a voluntary botnet «Help Israel Win», which allowed individuals to voluntarily delegate control of their computers to the botnet server after down-loading the «Patriot DDoS Tool».'[42] Politically engaged citizens and hired hackers could also work in cloud computing dedicated to a particular peacekeeping mission. The impact is mainly possible on the level of social engineering, even in frames of UN actions promoted in the social media. Aforementioned cyber peace actions under the aegis of the UN have to also correspond to the provisions of Tallinn Manual, e.g. the principle 36. of the handbook: 'Cyber attacks, or the threat thereof, the primary purpose of which is to spread terror among the civilian population, are prohibited.'[43]

Conclusions

The variants of an *ad hoc* cyber operations could be used not only in the area concerning observance of IHL, in frames of any measures accompanying armed conflict – including asymmetric. They could be also effective as support measures targeting the criminal and cyber criminal activities (EUROPOL). Outline of the model of peace operations with the use of cyberspace is thus a modular design, the hallmark of which is the scalability of conflict management at the global level. It has large enough flexibility to tailor it to the specific situation, depending on the specifics of the cyber operations it assumes the presence of the military component (hard power), or it is deprived of it (soft power).[44] In the former case, hackers involved in supporting peace operations could e.g. cooperate together with the NATO Response Teams (NATO CIRC). Among the tools used in achieving the objectives set by the DPKO there are the network-enebled operations, cyber-sabotage and espionage. 'Only very few sophisticated strategic actors may be able to pull off top–range computer sabotage operations'[45] - these activities can significantly support military operations in frame of UN mandate. This would be extremely useful, because as Rid stated: 'Sabotage on its own may not be an act of war.'[46] In case of violation of Article 2 pt. 5 Charter of the United Nations, such measures could be taken in the

[41] 'SETI@home' at <http://setiathome.ssl.berkeley.edu/> (accessed 13 November 2015).

[42] T. Rid, *op cit*, p. 93.

[43] M. N. Schmitt (ed), *op cit*, p. 122.

[44] See J. S. Nye *Soft Power: The Means to Success in World Politics* (PublicAffairs New York 2006).

[45] T. Rid, *op cit*, p. 96.

[46] *Ibid*, p. 84.

State which would deliberately escalate conflict towards its internationalization.[47] The catalog of available funds also could include acts of cyber espionage as the 'many spying operations are unknown to the victim.'[48] The aim of the legally sanctioned surveillance, blocking bank accounts, interfering of communications and the interception of computers in order to gain evidence (including the image of the perpetrator), could also be individuals that violate the provisions of IHL and favour such violations (e.g. working towards sustaining the conflict by their functions, traders weapons, pirates, etc.). Such activities are in fact ultimately targeting at other citizens and their human security.

In the course of expecting evolution and dissemination of tools which will become more and more available to freely interact on critical infrastructure, talented hackers who are already engaged by corporations 'to scan networks and manage patches'[49] could work in the area of internal and external cyber security assurance of States covered by peace operations. If in combat 'the mobilisation of popular support is essential for subversion, perhaps helpful in espionage'[50], why not take advantage of such tools and resources in activities for peace, especially as the domain of cyberspace is conducive to this type of action? This question implies, of course, a number of ethical and political concerns. No less doubts rise attempts to use cyberspace mainly to achieve targets of warfare. If eliminating war as the ultimate form of achieving political objectives is impossible, then with the help of new technology we can mitigate its causes, course and consequences, what is also in the interest of the armed forces themselves.

A shift of focus from the geographical territory to the logical layer and society is the result of moving away from the physical paradigm, closely associated with the axial elements of the Westphalian system – State and territory. Therefore, to realise aforementioned alternatives we need only the break of the mental barrier. At this stage, they don't need to automatically entail the creation of a new code of the law of peace operations in cyberspace. However, the effect of these operations would be to create a catalog of specific cases of violation of law, which could prevent exploitation in this area vulnerabilities, typical for the law of armed conflict. Civilians aren't effectively protected today and there's no sign it will change in the near future in the ordinary way: 'We live in a constant state of crisis, and this crisis also involves the modern state, whose structure, functionality, effectiveness (including the system of democratic representation) are no longer suited to the times in which we live.'[51] That's why: 'The changing nature of conflicts following the end of the Cold War made it imperative for the UN to launch a new era of humanitarian interventions, some of which came into conflict with the concept of sovereignty.'[52] For this reason, a conflict may be considered from the point

[47] 'All Members shall give the United Nations every assistance in any action it takes in accordance with the present Charter, and shall refrain from giving assistance to any state against which the United Nations is taking preventive or enforcement action'.

[48] T. Rid, *op cit*, p. 96.

[49] B. Doug, *op cit*.

[50] T. Rid, *op cit*, pp. 94-95.

[51] C. Bordoni, *op cit*.

[52] E. Osmançavuşoğlu 'Challenges to United Nations peacekeeping operations in the post-Cold War era' Journal

of view of non-state actors, including from the perspective of the individual. This means that future peace operations may be formed on the basis of currently marginal elements, including primarily 'human security'. By limiting the military component, they may become an important element of soft power in the universal and global conflict management.

All of this is the starting point for the model which puts civilians and hackers at a higher level of conflict management and which will be located directly in an post-Westphalian environment. For the purpose of this article it is named as 'HyperState' and because the introducing structural changes it relates rather to the 'management of peace'. The existence of such a conglomerate could create a counterweight to the progressive militarisation of cyberspace, by wider ceding part of responsibility for world peace to the realm of hackers and citizens (global-citizens). The model assumes their increased involvement in peace operations which could constitute the essence of direct democracy and affect further evolution of international relations.

End of Part I

of International Affairs (December 1999 – February 2000) IV(4) at <http://sam.gov.tr/wp-content/uploads/2012/02/EmelOsmanCavusoglu.pdf> (date accessed 13 November 2015).

BIBLIOGRAPHY

MONOGRAPHS

Abbet, Janet *Inventing the Internet* (The MIT Press Cambridge Massachusetts 2000)

Aristotle, *The Politics* (A & D Pub. Blacksburg Virginia 2009)

Augustine Saint Bishop of Hippo, and Dods, Marcus *The city of god* (Hendrickson Publishers Peabody Massachusetts 2013)

Bacon, Francis *New Atlantis* (Cambridge University Press Cambridge 2010)

Boutin, Berenice *The Role of Control in Allocating International Responsibility in Collaborative Military Operations* (SHARES Amsterdam 2015)

Cicero, Marcus T., Rudd, Niall and Powell, Jonthan G.F. *The republic, and The laws* (Oxford University Press Oxford 2008)

Das, Sajal K., Kant, Krishna and Zhang, Nan *Handbook on Securing Cyber-Physical Critical Infrastructure* (Morgan Kaufmann Waltham Massachusetts 2012)

Lindsay, Wallace M. *Isidori Hispalensis Episcopi Etimologiarum Sive Originum* Libri XVIII (1) (E Typographeo Clarendoniano Oxoni; Oxford University Press Oxford 1911)

Loukas, George *Cyber-Physical Attacks: A Growing Invisible Threat* (Elsevier/Butterworth-Heinemann Oxford UK Waltham Massachusetts 2015)

Nye Jr., Joseph S. *Soft Power: The Means to Success in World Politics* (Public Affairs New York 2006)

Pietraś, Marek and Marzęda, Katarzyna (eds) *Późnowestfalski ład międzynarodowy* (Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej Lublin 2008)

Schmitt, Michael N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, Cambridge New York 2013)

Suarez, Francisco and Pereña, Luciano *Guerra, Intervención, Paz Internacional* (Espasa-Calpe Madrid 1959)

CHAPTERS IN EDITED COLLECTIONS

Barak, Azy and Suler, John 'Reflections on the Psychology and Social Science of Cyberspace' in Barak, Azy (ed) *Psychological Aspects of Cyberspace: Theory, Research, Applications* (Cambridge University Press Cambridge New York 2008) 1-12

Blank, Laurie and Guiora, Amos 'Teaching an Old Dog New Tricks: Operationalizing the Law of Armed Conflict in New Warfare' in Gaston E. L. (ed), *The Laws of War and 21st Cenury Conflict* (New York, London & Amsterdam 2012) 87-95

Cassese, Antonio 'Current challenges to international humanitarian law' in Clapham Andrew and Gaeta, Paola (eds) *The Oxford handbook of international law in armed conflict* (Oxford University Press Oxford 2014) 3-19

Dinstein, Yoram 'Computer Network Attacks and Self-Defense' in Schmitt, Michael N. and O'Donell, Brian T. (eds) *Computer Network Attack and International Law* (Naval War College Newport 2002) 99-119

Held, David 'The changing structure of international law: sovereignty transformed?' in Held, David and McGrew, Anthony (eds) *The Global Transformations Reader: an Introduction to the Globalization Debate* (Polity Press Cambridge UK 2003) 162-176

Rid, Thomas 'Cyber war will not take place' in Ducheine, Paul, Osinga, F and Soeters, J (eds) *Cyber Warfare. Critical Perpectives* (T.M.C. Asser Press Hague 2012) 73-99

JOURNAL ARTICLES

Arnolds, Edward B. and Garland, Norman F. 'The Defense of Necessity in Criminal Law: The Right to Choose the Lesser Evil' (1975) 65(3) Journal of Criminal Law and Criminology 289-301

Kohki, Abe 'Human Rights-ization of International Law: a Critical Analysis of the «Ethical Turn»' (2013) col. 111 Kokusaihō gaikō zasshi 1-28

Nussbaum, Arthur 'Just War – A Legal Concept?' (1943) 42(3) Michigan Law Review 453-479

Osmançavuşoğlu, Emel 'Challenges to united nations peacekeeping operations in the post-cold war era' (1999-2000) IV(4) Journal of International Affairs

Syse, Henrik, 'Plato: The Necessity of War, the Quest or Peace' (2002) 1(1) Journal of Military Ethics 36–44

von Elbe, Joachim 'The Evolution of the Concept of the Just War in International Law' (1939) 33(4) The American Journal of International Law 665–688

ELECTRONIC ARTICLES

Barney, Doug 'White Hat Hackers – the forgotten good guys' (31 March 2015) at <http://www.gfi.com/blog/white-hat-hackers-the-forgotten-good-guys/> (date accessed 13 November 2015)

Bordoni, Carlo 'A Crisis Of The State? The End Of The Post-Westphalian Model' (12 February 2013) at <http://www.socialeurope.eu/2013/02/a-crisis-of-the-state-the-end-of-post-westphalian-model/> (date accessed 13 November 2015)

Boulanin, Vincent 'Arms production goes cyber: a challenge for arms control' (2015) at <http://www.sipri.org/media/newsletter/essay/Boulanin_May13> (date accessed 13 November 2015)

Marshall, Tom 'Perpetual Westphalia? Exploring Westphalian and Non-Westphalian Politics Through Aleatory Materialism' at <https://www.google.nl/urlsa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=0CDQQFjABahUKEwj1iPPys4DJAhXEUhQKHTPiDp0&url=https%3A%2F%2Fmillenniumjournal.files.wordpress.com%2F2012%2F10%2Fmarshall-materialism-paper.docx&usg=AFQjCNGr5Xw5Cc1w BZabzJrtIw1hlLw1g&bvm=bv.106923889,d. d24&cad=rja> (date accessed November 2015)

MISCELLANEOUS DOCUMENTS AND REPORTS

Aleksa, Karolis (ed), *Ką turime žinoti apie pasirengimą ekstremaliosioms situacijoms ir karo metui* (Krašto apsaugos ministerija Vilnius 2014) at <www.kam.lt/download/46229/ka%20turime%20zinoti%20(knyga%202014)%20sk.pdf> (date accessed 13 November 2015)

'Emergency Communications for Disaster Relief Deployment Archive' at <http://www.unfoundation.org/what -we-do/legacy-of-impact/technology/disaster-relief-deployments/> (accessed 13 November 2015)

'Liberia's ICT and Telecom Policy' The Ministry of Commerce and Industry at <http://www.moci.gov.lr/doc/ICT%20_%20Telecom%20Policy%20Main%20Body.pdf> (date accessed 13 November 2015)

'Lists of Intangible Cultural Heritage and the Register of Best Safeguarding Practices' (UNESCO) at <http://www.unesco. org/culture/ich/en/lists> (date accessed 13 November 2015)

'Peacekeeping Fact Sheet' (31 August 2015) at <http://www.un.org/en/peacekeeping/resources/statistics/factsheet.shtml> (date accessed 13 November 2015)

'SETI@home' at <http://setiathome.ssl.berkeley.edu/> (accessed 13 November 2015)

'South Sudan accelerates ICT in all sectors' (2015) at <http://www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/in-focus-articles/2015/south-sudan-accelerates-icts-in-all-sectors> (date accessed 13 November 2015)

'The Antarctic Treaty' at <http://www.ats.aq/e/ats.htm> (date accessed 13 November 2015)

The United States Army's Cyberspace Operations Concept Capability Plan 2016-2028 Department of the Army USA TRADOC Pamphlet 525-7-8 (22 February 2010) at <http://fas.org/irp/doddir/army/pam525-7-8.pdf> (date accessed 13 November 2015)

'Troop and police contributors at <http://www.un.org/en/peacekeeping/resources/statistics/contributors..shtml> (date accessed 13 November 2015)

'United Nations Global Pulse. Harnessing big data for development and humanitarian action' at <http://www.unglobalpulse.org/about-new> (accessed 13 November 2015)

'United Nations Peacekeeping Group: Capacities to Ensure Integration' at <http://www.un.org/en/peacekeeping/documents/dpkodfs_org_chart.pdf> (date accessed 13 November 2015)

'What We Do: Emergency Communications for Disaster Relief Deployment Archive' (United Nations Fundation) at <http://www.unfoundation.org/what-we-do/legacy-of-impact/technology/disaster-relief-deployments/> (date accessed 13 November 2015)