JOURNAL OF SCIENCE OF THE MILITARY ACADEMY OF LAND FORCES

Volume 48 Number 2 (180) 2016

DOI: 10.5604/17318157.1216083

MILITARIZATION OF CYBER SPACE AND MULTIDIMENSIONALITY OF SECURITY

Bogusław OLSZEWSKI*

* *Center for Eastern Studies, Institute of International Studies, University of Wrocław*

email: boguslaw.olszewski@uni.wroc.pl

Received on June 22nd 2015; accepted after revision in February 2016

Abstract:

The development of theoretical foundations for computer networks and their practical implementation has given rise to the progressive computerization of armed activities. The idea of a communication medium resistant to a nuclear attack, which was developed in the late sixties of the twentieth century in the form of the ARPANET, affects strategic, operational and tactical dimensions of the modern battlefield. It is also an important element shaping the processes related to ensuring the security of the state, both in the internal dimension as well as in dealings with other actors of international relations. Multi-layeredness and the growing complexity of cyber space cause that cyber security policy has been placed not only in the context of critical infrastructure, but also all the aspects of ethical and legal issues are taken into account. The armed forces have become an integral part of the information society, and as such, have been increasingly influenced by the civil sphere. The militarization of cyber space results directly from increasing saturation of the state structure with ICT technologies and the growing importance of these components in the process of ensuring security. The wide access to ICT generates a new threat to the defense system, including the armed forces. The ability of the digital impact on the military sphere, evidenced by many non-state actors, is today the main reason for implementing regulations restricting the activity of citizens in the global network.

Keywords:

cyber space, cyber war, security, militarization, information society, informatization of military actions

INTRODUCTION

When in 1991 the hypertext network communication system World Wide Web began

a global expansion it was still, especially in the physical and logical layer, the structure closely referring to its beginnings in the late sixties. From 29 October 1969, when the first message was sent (based on the protocol 1822 and *Internet Message Processor* IMP) within the network ARPANET (*Advanced Research Projects Agency Network*) established between American universities, UCLA (the University of California, Los Angeles) and SRI (the Stanford Research Institute), a new communication medium developed rapidly. In 1982 the US Defense Communications Agency (DCA) established the communication protocol TCP/IP network standard – the ARPANET network constructed on the basis of local academic networks became henceforth an important element of the evolving Internet. In 1983 it was decided to separate the military internetwork called MILNET (*Military Network*)[1] within the research and development infrastructure ARPA. From that time MILNET served as the operating military network under the responsibility of the Ministry of Defense, and in the 1990s it was transformed into NIPRNET (*Non-secure Internet Protocol Router Network*), SIPRNET (*Secret Internet Protocol Router Network*) and JWICS (*Joint Worldwide Intelligence Communications System*). From the time the project ARPANET was closed (1990), the civil Internet began to evolve without the formal supervision of DARPA (*Defense Advanced Research Projects Agency*, until 1972 ARPA - *Advanced Research Projects Agency*), and the service WWW has given it a totally new quality; now it is still connected to the military network infrastructure, which is of significant importance for all users. DARPA is currently involved in two major programs for cyber security: CRASH (*Clean-slate Design of Resilient, Adaptive, Secure Hosts)* developing autonomous learning and self–healing (hardware immunologization) computer systems that respond to cyber attacks, and PROCEED (*Programming Computation on Encrypted Data*) allowing to carry out real-time operations on the encoded data[2].

1. CYBER SPACE AS A SOURCE OF THREATS

The increasingly widespread emphasis on the importance of cyber security in the category of contemporary international relations implies the need to transfer this issue to the military ground. In fact, as such it remains the effect of technological, social and political changes resulting in the recognition of cyber space as an integral part of the environment of human existence and its linkage to the category of national security and consequently - a citizen. It is true that following theoretical premises of the so-called Copenhagen school, the creation of cyber threats (securitization) should be partly recognized also in the military field. However, on the grounds of political realism one must admit that actually this medium and the infrastructure become progressively the tool, the area and the aim of conducting military operations, regardless of securitization actors, among whom there are "political leaders, bureaucrats, the government,

[1] S. Denett, E. J. Feinler, F. Perillo (ed.), Arpanet information brochure, Menlo Park 1985, p. 4 [online]. Available on the Internet: http://www.dtic. mil/dtic/tr/fulltext/u2/a164353.pdf.

[2] DARPA Goal for Cybersecurity: Change the Game, [online]. Available on the Internet: https://www.dvidshub.net/news/ 62356/darpa-goal-cybersecurity-change-game#. VONd3dpK_Wk [accessed on: 15.01.2015].

lobbying groups and pressure groups[3]". The degree of the impact of the progressive cyber space militarization on the evolution of international conflicts and internal security (local, human) of the state and accompanying challenges concerning, among others, future changes in the codification of international public and private law should be considered at several levels, as reference objects are digital resources, the state apparatus, the system of national security, as well as an individual himself/herself. This is due to the fact that cyber space as "the fifth dimension" includes all sectors, and the related safety devices are becoming highly interconnected. Also, the recipients (audience) of the securitization process are more and more diverse and at the same time settled in all possible areas of activity of the state, thus creating a multi-dimensional network of dependencies on the interfering reference objects and on each other. For this reason, information warfare measures (IW), also from the strictly information technology point of view, have now become the most important element in the process of the impact of the so-called soft (smart) power, and the potential effects of their use can be as devastating as the effects of the direct use of the kinetic military force. Characteristics of cyber space allow for emphasizing the possibility of its use, which can be destructive to the same extent as nuclear weapons[4].

Thus, the (r)evolution of the network society is also the revolution in military affairs RMA (but currently it is viewed as the evolution) with all its consequential implications, including interference with the digital resources of civilians under the pretext of combating threats. Therefore, the smoldering conflict between the apologists of complete freedom in the network and the supporters of stricter regulations on this medium intensifies, which in the military context results, among others, from the above mentioned duality of the network infrastructure, the access to sensitive data, computerization of military operations[5] and the weaponry equipped with advanced electronics. In this dispute, the attention is drawn to the ambivalent attitude of the commercial sector, which is equally, if not more, vulnerable to various forms of cyber threats, while providing technical solutions and services for the military, possessing and supervising sensitive data and telecommunications infrastructure (for which the state more and more often usurps the ultimate poverty right), and all this in the face of the need to maintain the confidence of individual consumers and respect their right to privacy. Academic traditions of contestation dating back to the counterculture movement in the USA, when the idea of ARPANET was being developed, the theory of virtual reality appeared and Silicon Valley was created, have been and will remain in the future very

[3] B. Buzan, O.Wæver, J. De Wilde, Security: A New Framework for Analysis, Boulder 1998, p. 40, cited after: Ł. Fijałkowski, Teoria sekurytyzacji i konstruowanie bezpieczeństwa, [in:] "Przegląd Strategiczny" 2012 No. 1, p. 154 [online]. Available on the Internet: http://studiastrategiczne.amu.edu.pl/wp-content/uploads/2013/03/12.FIJALKOWSKI.pdf.

[4] R. Wellen, Cyber war and Nuclear War: the Most Dangerous of All Conflations, [online]. Available on the Internet: http://fpif.org/ cyber war-and-nuclear-war-the-most-dangerous-of-all-conflations/ [accessed on: 15.01.2015].

[5] D. S. Alberts, Information Age Transformation: Getting to a 21st Century Military, Washington 1996, p. 7-8 [online]. Available on the Internet: http://www.dodccrp.org/files/Alberts_IAT.pdf.

strong in the global dimension. In 1997 James Boyle introduced the term of *digital libertarianism*, mentioning at the same time the fact that the proponents of this approach ignore methods enabling governments to fulfil their governance functions on the Internet. There was the general opinion that the state was too inept to pose a threat to the freedom on the net[6]. In 1998, John P. Barlow published *Declaration of the Independence of Cyber space* in which he stated: "Governments of the Industrial World (...) I have come from Cyber space, the new home of Mind (...) You are not welcome among us. You do not have sovereignty where we gather. (...) You have no moral right to rule us[7]"; in another text he said that "information wants to be free[8]".

After nearly two decades that have elapsed since then, the situation is somewhat different. Cyber space as an area subject to dynamic changes resulting from globalization and the growing economic interdependence of states and connecting more and more new users, operating oftentimes several access devices, currently generates a wide range of security-related threats. They are situated at all levels related to the use of teleinformation means: technological, political, economic, social, educational, psychological, military etc., simultaneously revealing the multidimensional nature of the information society. They give rise for making more and more frequent attempts to increase the supervision of the medium. It is pointed out as necessary to implement indirect regulations concerning the activities of actors in cyber space, demanding changes to the code itself and forcing the need for the content self-censorship on the side of both by a provider and a recipient[9]. Mechanisms shaping the modern electronic information space in the context of human security are widely used in this process. A user's consent to the selective reduction of sources of information may be obtained by the skillful management of the subjective sense of security and extending it to the areas important for the entity. Technical solutions with software integrated with web browsers constitute a particular example, as many restrictions on network traffic occur beyond the control of the concerned parties - their role is limited to the installation of a service pack, which filters out websites using predefined lists or keywords contained in the header.

The late 1990s brought to the American ground the government regulations concerning cyber space related to, among others, protection of minors against obscene materi-

---

6 J. Boyle, Foucault in cyberspace: surveillance, sovereignty, and hardwired censors, "University of Cincinnati Law Review" 1997 vol. 66, p. 201 [online]. Available on the Internet: http://scholarship.law.duke.edu/cgi/ viewcontent.cgi? article=1552&context=faculty_scholarship.

7 J. P. Barlow, A Declaration of the Independence of Cyberspace, [online]. Available on the Internet: https://projects.eff.org/ ~barlow/Declaration-Final.html [accessed on: 13.01.2015].

8 Ibidem, Selling Wine Wirhout Bottles: The Economy of Mind on the Global Net, [online]. Available on the Internet: https://w2.eff.org/Misc/Publications/John_Perry_Barlow/HTML/idea_economy_article.html [accessed on: 16.01.2015].

9 L. Lessig, The constitution of code: limitations on choicebased critiques of cyberspace regulation, in: „Commlaw Conspectus: Journal of Communications Law and Technology Policy", vol. 5, 1997 [online]. Available on the Internet: http://scholarship.law.edu/cgi/viewcontent.cgi?article=1119&context=commlaw.

al (*Communications Decency Act*[10]) and copyright protection (*Digital Millennium Copyright Act*). It is pointed out, however, that as a result of similar records, the Internet service providers (ISPs), who for obvious reasons allow to store and transfer contents covered by the laws, will censor themselves the flow of data in order to avoid criminal liability. This leads eventually to a bizarre situation, where in accordance with the law regulations the private correspondence containing non-censural expressions or private photos and videos may be liable to a penalty or may be locked. What matters is not so much the question of the obvious need to set the filters in the browsers used by children, but the mechanism itself and its features revealed eventually in the context of socio-technique. Removing contents poorly perceived by governments could soon be completely automated, forming the desired image of the world and users' behaviors without their knowledge. Based on the argument about the inability to stop people from posting dissident materials and potential exposure of minors, there are introduced regulations on the network architecture, while postulating its permanent monitoring and appointing areas subject to restrictive (often personalized) forms of access. The situation is similar in the case of algorithms of major search engines and positioning services, which direct a group of ordinary Internet users to a relatively stable set of websites.

Therefore, the digital division begins to refer not so much to access to the network, but to the rights to the content, bearing in mind not only the flagship issue of sex and violence (by the way, TV provides similar and easily accessible dose of it). The danger consists rather in possible sectorization of information on the civilian network (e.g. disaggregation of information sets available for specific social groups prior authorization) or taking arbitrary decisions on its removal. The growing tendency to keep citizens in the dark about the world around them manifests itself, for example, in the warnings of the British government concerning the materials of the James Foley's execution performed by the so-called Islamic state (even watching it can be punished with arrest under the antiterrorism law - *Terrorism Act 2006*[11]). A similar situation may occur when creating, sharing or locking sources of information on the course of ongoing armed conflicts, methods of armed struggle, adopted policies, security strategy of states, judgments of the International Criminal Court, the technical data relating to armaments, research in the military field, the theory of a cyber war, surveys of social moods etc. Thus, the law is realized more and more frequently in the form of a computer code and selection of information, while the commercial sector becomes a tool to introduce censorship on the net.

Once the monitoring of information has been officially introduced, the governments are able to reduce political costs incurred by states, in return leaving at disposal the

[10] Finally rejected as unconstitutional (2006), similarly to the subsequent Child Online Protection Act (2009); Children's Internet Protection Act of 2000 is currently in force.

[11] J. Elgot, Islamic State Beheading Video Watchers Get Arrest Warning From Met Police, [online]. Available on the Internet: http://www.huffingtonpost.co.uk/2014/08/20/watch-james-foleys-beheading-online-and-you-could-get-arrested_n_56 94871.html [accessed on: 17.01.2015].

content classifiers and filtering software, operating on the principle of "use or risk legal consequences", which is *de facto* the imperative for self-censorship. Hence, another way to limit the freedom of access to information is the so-called website content determination (*Internet Content Rating Association*[12]) which enables the authors of www pages the classification of contents appearing on them (labeling pages) according to the PICS standard[13]. This generates two types of effects – the unmarked content can be automatically blocked, and further, unless the effective enforcement of the requirement to mark the content is possible, the system will be inefficient and selective. In addition, the content subjective assessment will be made under the pressure of potential legal consequences. All this may be reflected on the military grounds, including the quality of analyzes carried out on the basis of "open source intelligence", potential removal of blogs run by veterans, countering opposition activity by military juntas[14], establishment of military monitoring centers, consolidation of gateways, deleting online data potentially prejudicial to the state defense system[15].

The cooperation on the state and private grounds in the context of censoring the Internet content when both a recipient (identification system) and a supplier (selection of content, also as a paid service) of information are interested in using the software to shape social attitudes is part of a broader issue. A separate matter is the growing pressure on commercial entities towards making their data relevant for ensuring cyber security of the country more widely accessible, which was reflected even at the summit in Silicon Valley (13 February 2015), where B. Obama said: "We need to work together as we have never before[16]". This has received their different responses, as evidenced by the absence of the highest executive authorities of giants such as Google, Yahoo and Facebook. Despite this, the US President expressed his support for the creation of analytical centers (*Information Sharing and Analysis Organisations*, ISAOs) - platforms of cooperation and exchange of information on cyber threats, and he announced the establishment of a new intelligence unit to coordinate data analyzes as well. Such actions taken by the most networked countries of the world set the standards in the field of cyber security, which are often replicated in countries interested in the development in this area. In this context it is interesting to note that during the February summit there

[12] What is ICRA®?, [online]. Available on the Internet: https://www.fosi.org/icra/ [accessed on: 13.01.2015].

[13] Platform for Internet Content Selection, [online]. Available on the Internet: http://www.w3.org/PICS/ [accessed on: 13.01.2015], followed by Protocol for Web Description Resources (POWDER), [online]. Available on the Internet: http://www.w3.org/2007/powder/ [accessed on: 13.01. 2015].

[14] Thai military seeks Facebook, Google cooperation with censorship, [online]. Available on the Internet: http://www.reuters.com/article/2014/05/29/thailand-politics-censorship-idUSL3N0OF26B20140529 [accessed on:23.01.2015].

[15] S. Krupsky, Israel's military censor to monitor Facebook, Twitter, blogs, [online]. Available on the Internet: http://www.haaretz.com/news/diplomacy-defense/israel-s-military-censor-to-monitor-facebook-twitter-blogs-1.427769 [accessed on:23.01.2015].

[16] Cybersecurity: Tech firms urged to share data with US, [online]. Available on the Internet: http://www.bbc.com/news/ technology-314409 78 [accessed on: 15.02.2015].

was underlined the leading role of the government as an entity possessing the latest data on cyber threats.

2. A CYBER WAR

The implementation of technical solutions using the moral (auto)censorship is an excellent starting point to lock the broadly understood military content, as well as a useful tool in the information war (filtering of online forums, or the refusal of access implemented without the users' knowledge, e.g. by updating the browser). As the indirect result of the lock of contents related to nudity and sex is to limit the access to educational sites relating to this aspect of humanity, the lock using tags concerning violence prevents from displaying information on war crimes committed in the area of ongoing armed conflicts, or relations from the course of events. It is similarly, when it comes to the access to the statements of soldiers, containing offensive words used e.g. in relation to other countries and ethnic groups, educational materials concerning the functioning of the armed forces of countries in the world and the ways of fighting, controversial reports and documents disclosed by *hacktivists* (e.g. WikiLeaks[17]), etc.

The excessive emphasis on cyber threats results in shaping the fragmented reality, closing citizens in a secure capsule of a world without disturbing data and depriving them of situational awareness, and thus ultimately delegating the responsibility for their own perception of reality to third parties, and also gaining incomplete knowledge from the homogeneous medium under the control of corporations and governments; it can also generate a false feeling of danger or instrumentally escalate insignificant concerns. With the use of the software (code), Internet Service Providers as "the private police" help to avoid potential problems arising from legal restrictions, while creating the communication channel: a content provider – a network provider - the state. In this case, the Internet begins to resemble television, where there is an almost complete control over programs presented. When the law becomes a code there is no space for civil disobedience - in the face of the technology of the justice systems, an average web user remains powerless.

The implementation of new military strategies and technologies shapes hitherto unknown forms of threats, including these related to the future direction of development of telecommunications and ICT. In the face of the anticipated increase in the number of the Internet users and the number of access devices, almost unlimited possibilities appear to intervene in the system of military security, and the evolution of its forms (e.g. *Internet of Things*). It seems that the main factor influencing the scale of risk generated by the military activity in cyber space is the fact that international actors perceive this area differently - from the strictly technical recognition as the transmission infrastructure composed of nodes to the virtual psychological space, where the human needs of creativity and belonging are met and the impact on the awareness is particu-

[17] Bradley Manning given 35-year prison term for passing files to WikiLeaks, [online]. Available on the Internet: http://www. theguardian.com/world/2013/aug/21/bradley-manning-35-years-prison-wikileaks-sentence [accessed on: 23.01.2015].

larly suggestive. These issues have become extremely important in case of possible legal consequences of citizens' activities related to operations carried out by the armed forces in the face of an international conflict. The Lithuanian authorities included the provision on the desired participation of citizens in a cyber war in the event of an attack from another state and the subsequent occupation of their country in the document entitled "*What should we know about preparations for crisis situations and a war*" issued by the Ministry of Defense in 2014[18]. According to the guide, in the case of the above-mentioned situation, the inhabitants are advised to conduct offensive operations in cyber space, including information warfare with the use of the social media, like Facebook and Twitter. Therefore, the question reappears about the blurred boundaries between the civil and military spheres in cyber space and the legal consequences of this situation in the real world (*ius ad bellum, ius in bello,* the international humanitarian law, the right to use force in international relations). *Tallinn Manual on the International Law Applicable to Cyber warfare*[19] endeavours to answer many of these questions. As a pilot project, it puts the issue of a cyber war in the context of the existing legal provisions on armed conflicts, and bearing in mind the nineteenth-century origin of some of them one would rather expect a modern, dedicated code.

Meanwhile, the adequacy and legitimacy of some paragraphs of this non-paper are still to be discussed, for instance exceptional circumstances of the war time, justifying the enforcement of the rights to physical elimination of a hacker conducting military operations in cyber space in favour of the state[20], especially in view of still existing lack of technical possbilities to quickly and unambiguously confirm the involvement of particular persons. At the same time the document is proof that the militarization of cyber space and a cyber war has become a reality, and any attempt to stop this process may prove to be ineffective. The world confronted a similar situation in 1139, when the Lateran Council II unsuccessfully tried to ban the use of propelling weapons and crossbows in hostilities conducted between Christians[21]; the then feudal world did not respond to earlier condemnations of these practices by Pope Urban II during the Lateran Synod in 1097. Having regard to the then status and influence of the Church, one can identify the importance of the challenge posed by eliminating effective, though not always "humanitarian" weapons.

---

18 K. Aleksa (ed.), Ką turime žinoti apie pasirengimą ekstremaliosioms situacijoms ir karo metui, Vilnius 2014, p. 70 [online]. Available on the Internet: www.kam.lt/download/46229/ka%20turime%20zinoti%20(knyga%202014)%20sk. pdf.

19 M. N. Schmitt (red.),Tallinn Manual on the International Law Applicable to Cyber warfare, New York 2013 [online]. Available on the Internet: https://ccdcoe.org/tallinn-manual.html.

20 K. J. Heller, Does the Tallinn Manual Allow States to Kill Hackers? Not Really, [online]. Available on the Internet: http://opiniojurisorg/2013/03/25/does-the-tallin-manual-allow-states-to-kill-hackers-not-really/ [accessed on: 21.01.2015].

21 S. Hongsheng, The Evolution of Law of War, w: „Chinese Journal of International Politics" 2006 1(2), p. 272; Medieval Sourcebook: Tenth Ecumenical Council: Lateran II 1139, kanon 29., [online]. Available on the Internet: http://legacy. fordham.edu/halsall/basis/lateran2.asp [accessed on: 23.01.2015].

Thus, in the subjective dimension, the issue of a cyber war in the context of human security ought to be considered at least at three main levels. The first one concerns the safety of the population at risk of a cyber attack on the critical infrastructure of a state – the issues raised here include mainly the physical (original) and psychological (secondary) effects of the breach of its integrity. The interference within the elements essential for the functioning of a state (communication, energy, supply chains and other systems, for which the ICT network remains a common feature and a guarantee of effective action) results in the destabilization of individuals' psychic structures. The next level includes security of resources and information awareness (awareness of information technology) of soldiers - especially officers - allowing, based on government documents (programs, policies and cyber war security strategies), to perceive their own information resources (including private ones) as means of strategic importance. The last plane relates to guarantees of security of civilian involved in military activities in cyber space (e.g. coders, hackers). A particular challenge in this field is the legal classification of the effects of the use of a computer taken over remotely, functioning in bot networks[22] without the knowledge of its owner.

The involvement of commercial sector entities in the process of constructing military cyber security, including cooperation with the military sector within the knowledge-based economy is now becoming more and more apparent. Suffice it to mention the realization of civil orders on behalf of or in cooperation with the defense industry, the generated demand for ICT professionals (especially in the field of cryptology), or the sponsorship of events related to military cyber security (e.g. the international conference on cyber conflicts which took place in the NATO's Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) in Tallinn was sponsored by companies such as Microsoft, Verint, Intel, Cisco, Lanscope, Ixia, and IBM). However, one should not forget that in addition to the element of lobbying it is based on pragmatic prerequisites. In this case, the situation in the ICT market defines the current and future threats concerning not only the material layers of cyber space (infrastructure, *hardware*), but also its logical layer and software. The US defense industry calls for increased spendings on a cyber war[23], while the flagship companies from the military sector, like General Dynamics and Lockheed Martin, also produce devices provided for cyber forces of countries concerned. This results in a constantly expanding catalog of dual-use technology and increasing budgetary expenditures on armaments, as the prices of high-end devices reach millions of dollars (e.g. the training simulator of network traffic PerfectStorm ONE Californian Ixia costs approx. $ 1 million). In addition, the question remains, *de facto* rhetorical one, about the access to the most advanced technologies, even within the NATO alliance - here comes to the fore the realistic school of international relations.

[22] Botnet - a network of computers infected with software running in the background, communicating with each other in order to carry out the specified tasks.

[23] N. Farrell, US defence industry calls for more spending on cyber-warfare, [online]. Available on the Internet: http://www.theinquirer.net/inquirer/news/1592237/us-defence-industry-calls-spending-cyber-warfare [accessed on: 12.01.2015].

Also the ongoing efforts of lobbyists associated with cyber space are a considerable factor of an impact on the state of military security of a country and development of the theory of a cyber war. Such a wave took place in 2012, when, according to the Center for Responsive Politics almost two thousand reports used the term "cyber security[24]" (compared to 990 in 2011). After the attack on the giant of multimedia market and electronic equipment *Sony*[25] (November 2014), another wave of documents highlighting the importance of this issue may be expected. There will therefore be no exaggeration to say that today we are witnessing the cyber arms race; moreover, representatives of the governments have acknowledged that. The US Admiral Samuel Cox expressed such an opinion: "What we observe is the global cyber arms race. It does not proceed slowly or even linearly, but actually accelerates[26]". At the same time, the growing military activity in the digital sphere forms - along with the active participation of the industrial lobby - the conglomerate aiming towards gradual restriction of freedom on the civil network, which affects indirectly the soldiers themselves, to mention just a common practice of surveillance by the intelligence services and the military counterintelligence, as well as the real threat posed by the acquisition of cyber identity by unauthorized persons in order to discredit the command staff members or to conduct active disinformation. Seemingly reliable data once recorded in the public space is extremely difficult to be corrected even in a longer time perspective.

It seems that the existing legislative solutions are no longer adequate to the hybrid nature of a war in cyber space and lag behind technological changes, and, what is more, their indiscriminate use might generate significant legal problems. The lack of wider cooperation between states in this field seems rather remarkable, partly due to the quiet acceptance of those practices in the absence of the possibility of effective enforcement of the regulations. Cyber attacks have become an informal practice in international relations, contributing to the destabilization of relations in the political arena, and consequently also on social and military grounds. As mentioned above, an important aspect is the process of involving citizens in the offensive / defensive activities carried out by states in the framework of a cyber war and a net war. The first one is defined as "information-based comprehensive approach to a fight[27]", while the other as a "information-based comprehensive approach to a social conflict". In turn, Richard A. Clarke entered both of the above approaches to his definition of a cyber war: "the

[24] After attacks against NBC, LinkedIn and Global Payments, see: Cybersecurity lobbying doubled in 2012, [online]. Available on the Internet: http://money.cnn.com/2013/04/08/technology/security /cybersecurity-lobbying/ [accessed on: 12.01.2015].

[25] There was taken over a hundred terabytes of data and Sony's systems were infected by malware named Wiper canceling data on disks, See: What caused Sony hack: What we know now, [online]. Available on the Internet: http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/ [accessed on: 31.01.2015].

[26] U.S. Officials Warn of Global Cyber Arms Race, [online]. Available on the Internet: http://www.ciozone.com/index.php/ Security/U.S.-Officials-Warn-of-Global-Cyber-Arms-Race.html [accessed on: 23.01.2015].

[27] S. J. Cimbala, Nuclear Weapons in the Information Age, London & New York 2012, p. 46-47.

action taken by the nation-state to penetrate computers or networks of another nation with the aim to cause damage or disturbance[28]".

The dependence of modern warfare devices on computers and networks creates for potential aggressors the convenient opportunities to influence defense capabilities of a state. However, due to, among others, the high degree of safety of military systems, currently "experts disagree on the importance of a cyber war as an actual military threat[29]". A key element of this dispute is also the perception of a cyber war as a form requiring attributes typical for an interstate conflict, or at least the demand for accompanying a formally ongoing kinetic war. Therefore, some digital security experts use the concept of *a cyber arms race* instead of *a cyber war* claiming that today the latter does not exist[30]. Professor Terry D. Gill, a specialist in military law at the University of Amsterdam and in international public law at the University of Utrecht, a legal expert in the process of the development of the *Tallinn Manual on the International Law Applicable to Cyber warfare* prepared by the NATO's Cooperative Cyber Defense Centre of Excellence (NATO CCD COE) in Tallinn thinks alike.

In his view, the issue of a cyber war is not yet a priority in the field of cyber security and international relations, but today the most important issue, which demands active states' cooperation is the phenomenon of cyber crime and challenges associated with it[31]. Professor Thomas Rid of the King's College in London, involved in the field of security studies, explicitly says: "a cyber war did not happen in the past, it does not occur today and it is very unlikely to cause disturbances in the future[32]". Other authors consider the effects of the progressive militarization of cyber space as factors destabilizing the international environment[33]. The use of the military terminology (a cyber attack, cyber defense, etc.) is to lead to the conclusion that cyber space 'can and should be recognized as the military-strategic domain (...) This assumption is problematic and misleading (...) it suggests that countries can establish control over cyber space. It may result in the harmful atmosphere of insecurity and tension at the international level[34].

---

[28] R. A. Clarke, R. Knake, Cyber war: The Next Threat to National Security and What to Do About It, New York 2010, p. 6.

[29] S. J. Cimbala, Nuclear weapons and strategy. U.S. nuclear policy for the twenty-first century, London & New York 2005, p. 16.

[30] Mikko Hypponen - The Cyber Arms Race, [online]. Available on the Internet: https://www.youtube.com/watch?v=UUoi5-otFBE [accessed on: 31.01.2015].

[31] Professor T. D. Gill expressed the opinion 20 November 2014 during the meeting with the author of the article.

[32] T. Rid, Cyber war and Peace. Hacking Can Reduce Real-World Violence, [online]. Available on the Internet: http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace [accessed on: 31.01.2015].

[33] M. D. Cavelty, The militarisation of cyber security as a source of global tension, in: D. Möckli (ed.), Strategic trends 2012. Key Developments in Global Affairs, [online]. Available on the Internet: http://www.css.ethz.ch/ publications/pdfs/ Strategic-Trends-2012-Cyber.pdf [accessed on: 13.01.2015].

[34] M. D. Cavelty, O. Rolofs, Cyber war hype, [online]. Available on the Internet: http://www.the-atlantic-times.com/ index.php?option=com_ content&view=article&id=485:cyber-war-hype-&catid=25:politics&Itemid=2 [accessed on: 13.01.2015].

Since complex organizations, including the US Armed Forces, "are cross-linked and publicized, are model –making[35]" and military operations and a battlefield are becoming more and more saturated with network technology, which is vulnerable to attacks, such as the augmented reality[36], the issue of a cyber war is constantly evolving.

Thus, the term "cyber war" is often abused and related to each type of a cyber conflict on the international arena, and "from a military point of view, it should be considered as a part of the information war[37]". In the above context it can be noted that the hybrid and asymmetric nature of a cyber war does not require any formal declaration by a state. And if a cyber war actually cannot be spoken about with full conviction, there is nothing to prevent the actions of modern states in cyber space from being given the status of a low intensity conflict. Thus, in view of the above, the militarization of cyber space is a logical continuation of the construction of digital security in the national security system. However, it should be noted that when using the sectoral recognition and separating the military area out of the whole system, the picture of the entire issue is ignored and essential elements are underestimated, such as the right of higher rank commanders to the protection of privacy on the network, or the local safety (e.g. computer skills and the information awareness of public administration employees), which were aforementioned as regards human security, because information security and human security overlap.

The issue of a cyber war is now new and the key elements are still being discussed: the actual costs of its conducting, its impact on the global economy and political systems, operational and strategic dimensions of a cyber attack, the issue of classification of IT equipment as weapons and civilian infrastructure as a target. The very possibility of a precise cyber attack is disputable, as well as the low costs of its conducting are undermined, suggesting at the same time that the cyber arms race should be stopped. The literature on this subject allows assuming that a cyber war will not make it possible to avoid fatalities: "When countries combine cyber attacks with conventional operations, these can be paid for with human lives[38]". However, at this point, the rectification is necessary: in order to obtain fatalities it seems sufficient to carry out "pure" cyber attacks affecting critical infrastructure components via SCADA (*Supervisory Control and Data Acquisition*[39]) and PLCs (*Programmable Logic Controller*). Similarly, refer-

[35] E. Skrzypek, Wiedza i praktyka, in: A. Szewczyk, Dylematy cywilizacji informatycznej, Warszawa 2004, p. 116.

[36] M. Prigg, Google glass for war: The US military funded smart helmet that can beam information to soldiers on the battlefield, [online]. Available on the Internet: http://www.dailymail.co.uk /sciencetech/article-2640869/ Google-glass-war-US-military-reveals-augmented-reality-soldiers.html [accessed on: 31.01.2015].

[37] M. D. Cavelty, Cyber war: concept, status quo, and limitations, „CSS Analysis in Security Policy" 2010 no. 71(4), [online]. Available on the Internet: http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-71.pdf [accessed on: 31.01.2015].

[38] W. Goodman, Cyber Deterrence Tougher in Theory than in Practice?, „Strategic Studies Quarterly" 2010 vol. 4(3), [online]. Available on the Internet: http://www.au.af.mil/au/ssq/2010/fall/goodman.pdf.

[39] G. Brönnimann et al., CRN REPORT Focal Report 6. Assessing Threats in Cyberspace: Interrogating

ring to the strategy of nuclear deterrence, the effectiveness of this scheme in cyber space is taken into consideration and therefore there are forecasted high expenditures on security systems and military infrastructure not only against a cyber war, but cyber crime and cyber espionage as well; especially when cooperating with the ICT commercial sector and its supervision of military resources through outsourcing or intensive cooperation at an international level. Furthermore, it should be stressed that due to the scope and scale of destruction in case of a potential cyber war, a state-aggressor may face a nuclear response[40].

CONCLUSION

The militarization of cyber space seems to be another step on the way to the appropriation of this area by a state, regardless of whether the ontological status of a cyber war will be confirmed. The level of control over this process influences not only its effectiveness on the international arena, but also the rationality of state actors operating during today's armed conflicts. This requires the limitation of military expansion in cyber space since "the fight against cyber threats has become a highly politicized issue[41]". Furthermore, the excessive militarization of cyber space abolishes the customary law prevailing in it and appropriates this area by introducing regulations and restrictions applicable not only during a conflict, but in peacetime as well. Cyber deterrence and a cyber war are justified only in a situation when the opponents have the technology to allow such activities. However, it is a bit too early to talk about a war only limited to cyber space. This does not change the fact that with the development of global ICT structures such a war will become increasingly realistic, heading towards realizing the vision of fighting cyber armies. The most important issues are forms and the range of the legislative influence of the military sphere and the industrial sector, including the role of securitization actors, as well as prerequisites accompanying the creation of adequate regulations at the national and international levels. It is not surprising that the information society supported by the services of information and telecommunications technologies, which perceives information as a key product and knowledge as wealth, is aware of their military applications. It is evident that a citizen begins to play the role of civilian support to military operations in this field and, consequently, also a prisoner-of-war and a victim.

Therefore, the current situation is the result of many factors, including the historical and geopolitical ones (e.g. regionalization of cyber security in the case of the Baltic states). Due to the non-linear nature of a cyber war, all the projections are temporary

methodological approaches & the challenges of today's complex risk environment, Zurich 2011, 16 [online]. Available on the Internet: http://www.css.ethz.ch/publications/ pdfs/Focal-Report-6-Cyber-Security.pdf.

40 E. Colby, Cyber war and the Nuclear Option, [online]. Available on the Internet: http://nationalinterest.org /commentary/ cyberwar-the-nuclear-option-8638 [accessed on: 17.01.2015].

41 M. D. Cavelty, The Militarisation of Cyberspace: Why Less May Be Better, in: C. Czosseck, R. Ottis, K. Ziolkowski (ed.), 2012 4th International Conference on Cyber Conflict, Tallin 2012, p. 149 [online]. Available on the Internet: http://www.css.ethz.ch/publications/pdfs/Militarization-Cyberspace.pdf.

and require constant updating with taking account of the complex relationships of political and technological impact, as well as the sequence: national security, local security, human security. Threats mainly include hidden legislative measures, which are beyond the social control, such as the *Cyber Intelligence Sharing and Protection Act* (CISPA) and *Anti-Counterfeiting Trade Agreement* (ACTA). Attempts to monopolization of cyberspace by state and deprivation / regulation citizens' access to information stored in the network, which currently is met in the countries considered by the West as totalitarian or semi-totalitarian (North Korea, China), confirm the strategic importance of information and the universality of similar procedures. The information awareness of political elites is not without significance, as its deficiency promotes thoughtless adopting regulations affecting the interests of their own. In resolving the dilemma of "freedom and security" it should be noted that in the face of a war in cyber space freedom in the network is becoming increasingly crucial. It leaves a margin for citizens to ultimately support the military activity of the state in case of a possible cyber war - acquiring information and the accumulation of knowledge.

REFERENCES

1. Alberts D. S., *Information Age Transformation: Getting to a 21st Century Military*, CCRP: Washington 1996.
2. Aleksa K. (red.), *Ką turime žinoti apie pasirengimą ekstremaliosioms situacijoms ir karo metui*, Krašto apsaugos ministerija, Vilnius 2014.
3. Barlow J. P., *A Declaration of the Independence of Cyberspace*, [online]. Available on the Internet: https://projects.eff.org/~barlow/Declaration-Final.html, [available: 13.01.2015].
4. Barlow J. P., *Selling Wine Wirhout Bottles: The Economy of Mind on the Global Net*, [online]. Available on the Internet: https://w2.eff.org/Misc/Publi cations/John_Perry_ Barlow/HTML/idea_economy_article.html. [available: 16.01.2015].
5. Boyle J., *Foucault in cyberspace: surveillance, sovereignty, and hardwired censors*, [in:] University of Cincinnati Law Review, vol. 66 (1997), p. 177-205.
6. Brönnimann G. i in., *CRN REPORT Focal Report 6. Assessing Threats in Cyberspace: Interrogating methodological approaches & the challenges of today's complex risk environment*, Center for Security Studies (CSS), ETH Zurich, Zurich 2011, [online]. Available on the Internet: http://www.css.ethz.ch/ publications/pdfs/Focal-Report-6-Cyber-Security.pdf. [available: 13.01.2015].
7. Buzan B., Wæver O., De Wilde J., *Security: A New Framework for Analysis*, Rienner, Boulder 1998.
8. Cavelty M. D., *Cyber war: concept, status quo, and limitations*, [in:] CSS Analysis in Security Policy, no. 71(4), 2010, p. 1-3, [online]. Available on the Internet: http://www.css.ethz.ch/publications/pdfs/CSS-Analyses-71.pdf, [available: 31.01.2015]
9. Cavelty M. D., *The militarisation of cyber security as a source of global tension*, [in:] Möckli D. (ed.), *Strategic trends 2012. Key Developments in Global Affairs*, Center for

Security Studies ETH Zurich, Zurich 2012, p. 103-124.

10. Cavelty M. D., *The Militarisation of Cyberspace: Why Less May Be Better*, [in:] Czosseck C., Ottis R., Ziolkowski K. (ed.), *2012 4th International Conference on Cyber Conflict*, CCDCOE, Tallin 2012, p. 141-153.
11. Cavelty M. D., Rolofs O., *Cyber war hype*, [online]. Available on the Internet: http://www.the-atlantic-times.com/index.php?option=com_content&view=article&id=485:cyber-war-hype-&catid=25:politics&Itemid=2, [available: 13.01.2015]
12. Cimbala S. J., *Nuclear Weapons in the Information Age*, Continuum International Pub. Group, London & New York 2012.
13. Clarke R. A., Knake R., *Cyber war: The Next Threat to National Security and What to Do About It*, Ecco, New York 2010.
14. Colby E., *Cyber war and the Nuclear Option*, [in:] The National Interest, June 24, 2013 [online]. Available on the Internet: http://nationalinterest.org/commentary/cyber war-the-nuclear-option-8638, [available: 17.01.2015].
15. *Cybersecurity lobbying doubled in 2012*, [online]. Available on the Internet: http://money.cnn.com/2013/04/08/technology/security/cybersecurity-lobbying/, [available: 12.01.2015].
16. Denett S., Feinler E. J., Perillo F. (ed.), *Arpanet information brochure*, DDN Network Information Center, SRI International, Menlo Park 1985.
17. Elgot J., *Islamic State Beheading Video Watchers Get Arrest Warning From Met Police*, [in:] The Huffington Post, 21 August 2014, [online]. Available on the Internet: http://www.huffingtonpost.co.uk/2014/08/20/watch-james-foleys-beheading-online-and-you-could-get-arrested_n_5694871.html, [available: 17.01.2015]
18. Farrell N., *US defence industry calls for more spending on cyber-warfare*, [in:] The Inquirer, 17 February 2010, [online]. Available on the Internet: http://www.theinquirer.net/inquirer/news/1592237/us-defence-industry-calls-spending-cyber-warfare, [available: 12.01.2015].
19. Fijałkowski Ł, *Teoria sekurytyzacji i konstruowanie bezpieczeństwa*, [in:] "Przegląd Strategiczny", no. 1 (2012), p. 149-161.
20. Goodman W., *Cyber Deterrence Tougher in Theory than in Practice?*, [in:] Strategic Studies Quarterly, vol. 4(3) 2010, p. 102-135.
21. Heller K. J., *Does the Tallinn Manual Allow States to Kill Hackers? Not Really*, [online]. Available on the Internet: http://opiniojuris.org/2013/03/25/does-the-tallin-manual-allow-states-to-kill-hackers-not-really/, [available: 21.01.2015].
22. Hongsheng S., *The Evolution of Law of War*, [in:] Chinese Journal of International Politics" vol. 1(2), 2006, p. 267-301.
23. Krupsky S., *Israel's military censor to monitor Facebook, Twitter, blogs*, [in:] Haaretz, 2 May 2012, [online]. Available on the Internet: http://www.haaretz.com/news/diplomacy-defense/israel-s-military-censor-to-monitor-facebook-twitter-blogs-

1.427769, [available: 23.01.2015].

24. Lessig L., *The constitution of code: limitations on choicebased critiques of cyberspace regulation*, Commlaw Conspectus: Journal of Communications Law and Technology Policy, vol.5, 1997, p. 181-191.
25. Prigg M., *Google glass for war: The US military funded smart helmet that can beam information to soldiers on the battlefield*, [in:] Daily Mail, 27 May 2014, [online]. Available on the Internet: http://www.dailymail.co.uk/ sciencetech/article-2640869/ Google-glass-war-US-military-reveals-augmented-reality-soldiers.html, [available: 31.01.2015].
26. Rid T., *Cyber war and Peace. Hacking Can Reduce Real-World Violence*, [in:] Foreign Affairs, November/December 2013, [online]. Available on the Internet: http://www.foreignaffairs.com/articles/140160/thomas-rid/cyberwar-and-peace, [available: 31.01.2015].
27. Schmitt M. N. (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, New York 2013.
28. Skrzypek E., *Wiedza i praktyka*, [in:] A. Szewczyk, *Dylematy cywilizacji informatycznej*, PWE, Warszawa 2004, p. 97-135.
29. Wellen R., *Cyber war and Nuclear War: the Most Dangerous of All Conflations*, [online]. Available on the Internet: http://fpif.org/cyber war-and-nuclear-war-the-most-dangerous-of-all-conflations/, [available: 15.01.2015].
30. *Platform for Internet Content Selection*, [online]. Available on the Internet: http://www.w3.org/PICS/, [available: 13.01.2015].
31. *Protocol for Web Description Resources (POWDER) Working Group*, [online]. Available on the Internet: http://www.w3.org/2007/powder/, [available: 13.01.2015].
32. *Thai military seeks Facebook, Google cooperation with censorship*, [online]. Available on the Internet: http://www.reuters.com/article/2014/05/29/thailand-politics-censorship-idUSL3N0OF26B20140529, [available: 23.01.2015].
33. *Bradley Manning given 35-year prison term for passing files to WikiLeaks*, [online]. Available on the Internet: http://www.theguardian.com/world/2013/aug/21/ bradley-manning-35-years-prison-wikileaks-sentence, [available: 23.01.2015].
34. *Cybersecurity: Tech firms urged to share data with US*, [online]. Available on the Internet: http://www.bbc.com/news/technology-31440978, [available: 15.02.2015].
35. *DARPA Goal for Cybersecurity: Change the Game*, [online]. Available on the Internet: https://www.dvidshub.net/news/62356/darpa-goal-cybersecurity-change-game#.VONd3dpK_Wk, [available: 15.01.2015].
36. *Medieval Sourcebook: Tenth Ecumenical Council: Lateran II 1139*, kanon 29., [online]. Available on the Internet: http://legacy.fordham.edu/halsall/basis /later an2.asp, [available: 23.01.2015].
37. *Mikko Hypponen - The Cyber Arms Race*, [online]. Available on the Internet:

https://www.youtube.com/watch?v=UUoi5-otFBE, [available: 31.01.2011].

38. *U.S. Officials Warn of Global Cyber Arms Race*, [online]. Available on the Internet: http://www.ciozone.com/index.php/Security/U.S.-Officials-Warn-of-Global-Cyber-Arms-Race.html, [available: 23.01.2015].

39. *What caused Sony hack: What we know now*, [online]. Available on the Internet: http://money.cnn.com/2014/12/24/technology/security/sony-hack-facts/, [available: 31.01.2015].

40. *What is ICRA®?*, [online]. Available on the Internet: https://www.fosi.org/icra/, [available: 13.01.2015].

BIOGRAPHICAL NOTE

Boguslaw OLSZEWSKI, MA – a doctoral student in the Center for Eastern Studies at the Institute of International Studies, the University of Wrocław. His areas of research interests include: cyber security, crime in Central and Eastern Europe, the Baltic region geopolitics, ethnic conflicts. The author of articles and chapters in journals and monographs, as well as publications in thematic online portals. The participant of the Polish nationwide project NCN on ethnic policy, conducted by the University in Lublin. The manager and executor of internal research projects performed in his home scientific unit, related to the military dimension of cyber security: *The evolution of the law of armed conflicts vs. international security* and *International law aspects of the militarization of cyber space.*

HOW TO CITE THIS PAPER

Olszewski B., (2016). Militarization Of Cyber Space And Multidimensionality Of Security. *Zeszyty Naukowe Wyższa Szkoła Oficerska Wojsk Lądowych im. gen. Tadeusza Kościuszki Journal of Science of the gen. Tadeusz Kosciuszko Military Academy of Land Forces*, 48 (2), p.104-120. http://dx.doi.org/10.5604/17318157.1216083