Received: 31 March 2014 Accepted: 25 April 2014 Published online: 15 June 2014
Available from www.defenceandstrategy.eu doi: 10.3849/1802-7199.14.2014.01.029-038

Jak citovat tento příspěvek / How to Cite this Contribution

SCHMIDT, Nikola. Kritické poznámky k současné výzkumné agendě kybernetické bezpečnosti. *Obrana a strategie*. 2014, roč. 14, č. 1, s. 29–38. ISSN 1802-7199. DOI: 10.3849/1802-7199.14.2014.01.029-038

Kritické poznámky k současné výzkumné agendě kybernetické bezpečnosti

Critical Comments on Current Research Agenda in Cyber Security

Nikola Schmidt

Abstrakt

Následující článek předkládá alternativní kritický pohled na současný výzkum v oboru kybernetické bezpečnosti. Článek v úvodu kriticky analyzuje současný sekuritizační diskurz, používající analogii významných historických událostí vůči událostem dějícím se v kyberprostoru. Autor ve své argumentaci kritizuje takovýto přístup jako nevhodný s tím, že obdobné události nastanou jen velmi nepravděpodobně. Události, které do jisté míry již ovlivnily naše vnímaní – jako například estonské kybernetické útoky – sice způsobily významné škody, nicméně v současnosti by nezpůsobily již téměř nic díky výrazné obměně kritické infrastruktury Estonska. Jiný příklad, Stuxnet, je též sice útok s citelným dopadem, ale s nízkou pravděpodobností opakování v budoucnosti. V důsledku vysoké míry komplexity celé podpůrné operace tohoto útoku je velmi nepravděpodobné, že by mohl vést k tzv. kybernetické světové válce. Budoucnost přinese více komplexní, méně viditelné, kompletně skryté a precizní operace, které přinesou útočníkovi významnou strategickou výhodu vyplývající ze všech charakteristik kyberprostoru, spíše než že by přinesla scénáře kybernetického armageddonu porovnatelného s některými historickými událostmi nebo nukleárními scénáři. Autor v závěru článku navrhuje tři základní směry výzkumu v oboru kybernetické bezpečnosti. Za prvé, výzkum normativních rámců zaměřený na lepší porozumění kybernetickým událostem. Za druhé, důkladný výzkum kybernetického prostoru za účelem lépe aplikovatelné konceptualizace. Za třetí, přehodnocení konceptu kybernetické války v duchu konzervativního myšlení v koncept, který bude lépe reflektovat novost kybernetického prostoru.

Abstract

The following article presents an alternative critical perspective of the cyber security research agenda. The article opens with criticism of the securitization discourse that uses analogies of historical events with events in cyber space. The author argues that such an approach is inappropriate, and that events of such impact are very unlikely to take place. The events that have already shaped our way of thinking – such as the Estonian attacks – caused significant damage to the respective country; nevertheless, the very same attack today would not do the same harm, thanks to the different level of critical infrastructure in Estonia. Another example, Stuxnet, is also an event of high impact, but with a low probability of happening in the future. Due to the complexity of the supporting operation of the attack, it would not lead to a cyber world war. The future will bring more complex, less visible, completely covered and precise operations that will take advantage of all cyber space features, rather than a cybergeddon comparable to some historical event or a nuclear scenario. The author proposes three directions of desired research agenda in the cyber security field. Firstly, the development of normative framework aimed at a better understanding of cyber events; secondly, a thorough research of cyber space leading to appropriate space conceptualization; and thirdly, the reevaluation of cyber warfare concept in the light of the cyber space novelty.

Poděkování

Tento článek vznikl v rámci projektu Specifického vysokoškolského výzkumu SVV 2014 260 111.

Klíčová slova

Kybernetická bezpečnost; sekuritizace; kritická analýza; kybernetická válka; konceptualizace kyberprostoru; analýza hrozeb.

Keywords

Cyber security; securitization; critical analysis; cyber war; conceptualization of cyberspace; threat analysis.

INTRODUCTION

"In the practical art of war, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to capture an army entire than to destroy it, to capture a regiment, a detachment or a company entire than to destroy them."

Sun Tzu, The Art of War, 6th – 5th Century B.C.

The following article is aimed at drawing several dilemmas that have risen along with the debate over emerging cyber security threats. Since the end of World War II, the strategic studies have developed a broad theoretic framework based on newly developed technology of nuclear weapons, communication technologies and industrialization. There is no ambition to update the strategic studies in this article, but to debate some of the dilemmas of cyber threats emanating from cyberspace that would significantly influence the strategy of state defense and international stability, and in the end to propose the needed agenda in cyber security research according to a realistic evaluation of the current state of the international security in cyberspace.

At the beginning the article introduces the securitization debate challenged by the realistic analysis of the Stuxnet incident that has served as a peon to the securitization ambitions of some scholars, especially policy makers. Then the article offers another perception of cyber space that is different from other military domains and explains why such a new domain is viable for military operations, explaining reasons why it has to be treated differently. The third part discusses some security discourses in cyber space and their impact on strategic thinking. The article concludes with ideas for further academic focus, based on previous argumentation, which would be valuable for further cyber security research instead of banal threatening securitization based on historical analogies.

SECURITIZATION OF THE CYBERSPACE AND THE NATURE OF CYBER WEAPONS

Plenty of scholars have been recently pointing relentlessly to cyber threats as something that would trigger another world war and view the topic from the national perspective;[1] Russia already mentioned that a reaction to information warfare would have nuclear dimension;[2] USA stipulates that reaction to a cyber attack does not have to be limited to cyber means, because cyber attack would be evaluated as any other hostile activity.[3] Others who call for measures to face cyber threats immediately, or say "we may miss the train", are usually policy makers that have such securitization discourse as a vital

[1] CLARKE, R.A. and KNAKE, R. *Cyber War: The Next Threat to National Security and What to Do About It*. HarperCollins, 2012. ISBN 9780061962240.
[2] HILDRETH, Steven A. *Cyberwarfare*. 2001. *CRS Report for Congress*.
[3] THEWHITEHOUSE. *International Strategy for Cyberspace* [cit. 2014-03-31]. 2011. Retrieved from: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

component of their job.[4] Other proposals emphasize development of cyber defense measures to avoid cyber war,[5] but few scholars focus on critical analysis of concepts such as cyber space, cyber war, cyber attack and related strategy development or conceptualization debate. The over-securitization tendency, or one may say exaggeration of cyber threats, is prevalently produced by application of traditional military thinking to something extraordinary new. Vigilance on security novelty of emerging cyber threats is *in situ* in the current academic debate, but it lacks a strong critical feedback.

The sources of the securitization discourse are similar in nature with those treating cyberspace as a domain comparable to other warring domains; it is not comparable, as will be discussed later. The securitization discourse adopts cyberspace as a warring domain and applies the military perspective to the analysis of threats emanating from cyber space, so those scholars use the same logic as the one developed by strategic studies during the Cold War for other domains, which is the crucial problem. The evaluation of a threat is not based on critical analysis of cyber attack impacts, technology development, possible defensive measures, but on the contrary, on creative imagination of "what may happen if we are not prepared", just as we were not prepared for 9/11 or Pearl Harbor.[6] These doomy scenarios do not provide us with a critical sight of the novelty of current security issues, but focus on threatening others with the objective of supporting unidentified interests. Application of these scenarios analogously with historical events is not suitable for cyberspace. Such analysis tends to be shortsighted. Cyberspace as a warring domain would have, and ultimately has, different dynamics than the other domains. If something related to national security already happened, it does not mean we would face a tragedy comparable to the nuclear Mutual Assured Destruction scenarios. We live in a world extraordinarily interconnected by reciprocal economic dependency that has never been so developed in the human history; in the age of exceptional world peace among democratic countries that underlined the theory of democratic peace; in a world of widely developed normative framework that has led to a normative climate of nuclear taboo and also of international law protected by semi-working but existing international organizations. Hence, we should expect different approach in strategies of states willing to influence the political world order rather than a significant cyber attack with tremendous physical, violent, lethal or publicly visible catastrophic impacts, provided we think as realists in international relations.

In fact, there has been no single cyber attack threatening the world peace to date. The most significant one has been mentioned repeatedly. In 2010, Stuxnet[7] attacked nuclear centrifuges and disrupted Iranian nuclear program, returning it a couple of years back.[8] The attack seemed to be a pure sabotage operation or a stealthy intelligence cover action and it would be extremely difficult to replicate or conduct again. Despite the fact that the systems attacked had not been repaired for years and are very likely to still have the same vulnerabilities,[9] there has been no other significant attack on similar systems reported to date. Nevertheless, some US senators assert that if Stuxnet was used against the United States, it would have a monstrous impact on disrupting the whole electrical

[4] ALEXANDER, Keith B., GOLDMAN, Emily and WARNER, Michael. Defending America in Cyberspace. *National Interest*. 2013, pp. 18–24. ISSN 08849382. or SHEA, Jamie. NEW SECURITY CHALLENGES AND NATO'S FUTURE. *Turkish Policy Quarterly*. 2011, vol. 10, pp. 53–59. ISSN 13035754.

[5] MCGRAW, Gary. Cyber War is Inevitable (Unless We Build Security In). *Journal of Strategic Studies*. 2013, vol. 36, pp. 109–119. ISSN 0140-2390.

[6] LAWSON, S. BEYOND CYBER-DOOM: Cyberattack Scenarios and the Evidence of History. *Mercatus Center George Mason University Working*. 2011, no. 11 [cit. 2014-03-28]. Retrieved from: http://www.voafanti.com/gate/big5/mercatus.org/sites/default/files/publication/beyond-cyber-doom-cyber-attack-scenarios-evidence-history_1.pdf

[7] FARWELL, James P. and Rafal ROHOZINSKI. Stuxnet and the Future of Cyber War. *Survival*. 2011, vol. 53, pp. 23–40. ISSN 00396338.

[8] NICOLL, Alexander. Stuxnet: targeting Iran's nuclear programme. *Strategic Comments*. 2011, vol. 17, pp. 1–3. ISSN 1356-7888.

[9] PETERSON, Dale. Offensive Cyber Weapons: Construction, Development, and Employment. *Journal of Strategic Studies*. 2013, vol. 36, pp. 120–124. ISSN 0140-2390.

power grid,[10] but this never happened. One may argue that the other side does not possess the same state-of-the-art cyber weapons and capabilities, but precisely such presumption is wrong.

Stuxnet attack was a part of the operation called Olympic Games. To conduct such an extremely precise and stealthy operation requires a preceding intelligence operation to guarantee the success; especially when any cyber weapon is a double-edged sword that may be used against the attacker in retaliation. Hungarian cyber security and cryptography research institute CrySys Lab., established at the Budapest University, revealed that a worm called Flame would be such a predecessor collecting a vast amount of intelligence information to support the Stuxnet attack.[11] Flame or some selective part of the code was very likely used again during the attack against Saudi Aramco.[12] However, if we look at those two incidents, they do not seem to have the same origin as we may deduce from the current international relations dynamics. Iran is an eyesore to the international community and especially to the U.S. or West that are willing to put diplomatic pressure on Iran in the name of international security. The attack used a sophisticated irreversible method to ensure Saudi Aramco immediate shutdown. Saudi Aramco is a long-lasting ally to the U.S.; hence, it does not make sense for the U.S. or West to destabilize world oil production by deleting fifty thousand computers in Saudi Aramco while seeking for stabilization by undermining Iranian nuclear program. Thus, the interpretation is that a cyber weapon was highly probably used in retaliation against Saudi Aramco in Saudi Arabia by Iran or by a non-state actor. Who in fact was behind the attack is not clear due to the well-known attribution problem in cyberspace that significantly and maybe ultimately hides the attacker's origin.[13] One may argue that the high level of Stuxnet sophistication would serve as a clue to attribute it to a developed country such as the U.S. or Israel;[14] or the "logic of threatened others" in the nexus of international security would serve as another hint.[15] Sanger attributed the attack to the U.S. and Israel openly.[16] However, the Crimea experience showed that such deduced evidence of attribution without certainty (Russian soldiers without flags) does not push others to act in the name of international norms or law (!) even in a conventional conflict where the evidence of use of force is without doubt; of course, because it does not violate international law in the first place – there is no confirmed state behind the attack. Above all, a cyber attack could be conducted in order to inform the enemy that one has the capability to use the opponents' weapons in retaliation, and stay in the shadow by precisely securing strategic advantage exploiting the attribution problem. That would be the core message, something completely incomparable to the pre-cyber age; today cyber threats cannot be treated from the same perspective.

The conclusion of the first part of this paper consists of the following findings. First, the application of conservative perspective developed during the pre-cyber age is not an appropriate approach. Our enemies would retaliate by our own means, with our own weapons, and at the same time they would do their best to stay uncovered. Hence, the principal of deterrence by retaliation may not stop the attacks, but may rather escalate them in the form of extremely precise sabotage cover actions that undermine some competitive or threatening components of the enemy's highly developed society. One

[10] COLLINS, Sean and Stephen MCCOMBIE. Stuxnet: the emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence and Counter Terrorism*. 2012, vol. 7, pp. 80–91. ISSN 1833-5330.

[11] DEMIDOV, Oleg and Maxim SIMONENKO. FLAME IN CYBERSPACE. *Security Index: A Russian Journal on International Security*. 2013, vol. 19, pp. 69–72. ISSN 1993-4270.

[12] BRONK, Christopher and Eneken TIKK-RINGAS. The Cyber Attack on Saudi Aramco. *Survival*. 2013, vol. 55, pp. 81–96. ISSN 0039-6338.

[13] MUDRINICH, Erik M. Cyber 3.0: The department of defense strategy for operating in cyberspace and the attribution problem. *Air Force Law Review*. 2012, vol. 68, pp. 167–206. ISSN 00948381.

[14] GUITTON, Clement and Elaine KORZAK. The Sophistication Criterion for Attribution. *The RUSI Journal*. 2013, vol. 158, pp. 62–68. ISSN 0307-1847.

[15] GLASER, Charles L. *Deterrence of Cyber Attacks and U.S. National Security*. 2011. *Report GW-CSPRI-2011-5*.

[16] SANGER, D E. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. B.m.: Crown Publishing Group, 2012. ISBN 9780307718044.

may argue that the development of international norms in cyberspace would serve as a deterrent,[17] while others oppose the idea and support the above argumentation of conflict escalation.[18]

Second, cyber weapons are not conventional or nuclear weapons. They are novel in nature and should be treated with such novel strategic approach. The escalation in that sense does not mean that its result would eradicate people with bloody cruel lethality or turn the whole country into dust in a couple of minutes; on the contrary, the existence of a cyber weapon and its possible successful use may e.g. significantly influence the direction of a particular political representation. Nonetheless, the research should focus on the dynamics of such novelty rather than on the development of insane doomy scenarios.

Thirdly, for some reason critical infrastructures in all developed countries still do work and do not face any major state backed attacks. The DDoS (Distributed Denial of Service) attacks on Estonia in 2007[19] were treated as a new kind of war[20] that should be somehow deterred, and scholars began working on research on how a comparable cyber war would be deterred. In fact, the same attack would cause no harm today due to technical measures adopted in the network architecture and well-configured systems.[21]

CYBERSPACE CONCEPTUALIZATION AS A FLUID AND UNSTABLE DOMAIN

Most cyber security strategies tend to treat cyberspace as a solid, measurable, securable, spatial space dependent on technology with only few newly emerged characteristics, such as borderless space of ultimate freedom with solvable attribution problem. I deem that this approach is still limited. Treating cyberspace just as another domain as stipulated particularly in the US Department of Defense Strategy for Operating in Cyberspace[22] is not a definition of cyberspace; the strategy more precisely encourages the U.S. security community with Pentagon in the lead to *"organize, train, and equip"* with the objective to *"take full advantage of cyberspace's potential."* The mystification between definitions or knowledge that may be used as an epistemology of cyberspace for theory development or action and the governmental appeal to *"organize, train, and equip"* is a common mistake found in the literature treating cyberspace. The domain simply does not exist in the same form as all the other four domains including land, sea, air and space. All those four domains ontologically exist and a human is challenged to gain the strategic advantage by adopting a particular technology. However, one apparent characteristics changes everything. Cyber space as a fifth domain is a man-made domain.

Plenty of definitions can be found across national strategies. The following short examination is not comprehensive, but stresses several particular points. Martin Libicki probably is not the first one, but he is definitely the most visible one who emphasized the three-layer (with additional fourth layer) perspective and came up with a very valuable contribution of possible conquests at all respective layers. He divides cyberspace into three layers where the first physical layer consists of the physical infrastructure of hardware, cables, routers, satellites on orbit, etc.; the second syntactic layer consists of principles on which the physical systems are working, such as communication protocols; the third semantic layer consists of data flowing in the systems or saved on hard drives.[23] The first layer is easy to conquest by securing physical space or by taking over servers by law enforcement institutions

[17] STEVENS, Tim. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*. 2012, vol. 33, no. 1, pp. 148–170. ISSN 13523260.

[18] STŘÍTECKÝ, Vít. *Deterrence through Norms in Cyberspace: Critical Appraisal*. Toronto, Canada: Paper presented at the 55th ISA Annual Conference. 2014

[19] KAMPMARK, Binoy. CYBER WARFARE BETWEEN ESTONIA AND RUSSIA. *Contemporary Review*. 2007, vol. 289, pp. 288–293. ISSN 00107565.

[20] BEIDLEMAN, Scott W. *Defining and Deterring Cyber War*. USAWC. 2009

[21] Based on a personal discussion with officials at the Estonia Ministry of Defense.

[22] US-DOD. *DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE*. 2011 [cit. 2014-03-31]. Retrieved from: http://www.defense.gov/news/d20110714cyber.pdf

[23] LIBICKI, M.C. *Conquest in Cyberspace: National Security and Information Warfare*. Cambridge University Press, 2007. ISBN 9781139464659.

or simply by destruction with kinetic means. The second layer is much more sophisticated. The way to conquest the second layer lies in the ability to let the machines do what you want by injecting a specific code to their controllers. The first attack aimed at the syntactic level was probably the sabotage of Urengoy-Surgut-Chelyabinsk natural gas pipeline in 1982. The attack manipulated pressure valves and led to the biggest non-nuclear explosion ever.[24] It happened seven years before the emergence of the World Wide Web – the most important technology that has increased significance of the semantic layer by filling the Internet with freely available information. Conquering the third level in a sense of Libicki's approach means manipulating the information available to the public, but it also means blinding air defenses during a military operation such as the attack in Syrian region Deir ez-Zor in 2007 aimed at a deemed nuclear facility.[25]

Libicki evaluated possible "conquest" strategies of respective layers while adding a fourth layer as well, a pragmatic layer that lies behind the *"speech acts"*, which would be hard to define and hard to conquest. In 1998, Edward Waltz divides cyberspace into three layers: physical, information infrastructure and pragmatic,[26] putting emphasis on the importance of the content and its possible manipulation. Some of the definitions seem to be quite limited, consisting of infrastructure only: *"Cyberspace is the information space consisting of the sum total of all computer networks."*[27] In contrast, Kuehl offers definition where all the infrastructures are shaped *by the use* of them: *"Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interconnected information-communication technology (ICT) based systems and their associated infrastructures."*[28] Kuehl's definition is valuable in combining the following components of the definition. All the systems on the physical layer provide connectivity on the global scale between computer systems as well as between people, as they are sharing, adding, exploiting, downloading, modifying the content that can be moved immediately around the globe to anyone. The addition *"by the use"* is valuable in adding a cognitive or let say pragmatic layer that influences people's decision-making and that makes the space unstable and indefinitely fluid in its nature. Such fluidity is caused by the human behavior, habits and decisions.

Albert-László Barabási has developed an inspiring theory of networking more than a decade ago.[29] The important finding in his thoughts is the tendency of each network to create important nodes – centers. These nodes are also created by human habits, by preferring specific services while ignoring alternatives due to routines that in our minds secure the fulfillment of desired goals. Therefore, the way we use the technology intentionally by routines significantly shapes the cyberspace at the strategic level as well. It shapes the cognitive layer and defines the center when we prefer Google and the services the corporation provides. Cyberspace, thus, is not just a mess of cables around the world, but it also reflects our habits that may sink society into Durkheim's *anomie* if challenged. Hence, it is not only about infrastructure, systems, content, but also about the way we use it and shape it constantly. Development of appropriate conceptualization and consequent strategy for such a space is a challenging, but essential task.

[24] BETZ, D.J. and T. STEVENS. Cyberspace and the State: Toward a Strategy for Cyber-power. 2011

[25] CZOSSECK, C. and K. GEERS. *The Virtual Battlefield: Perspectives on Cyber Warfare*. Ios Press, 2009. ISBN 9781607500605.

[26] WALTZ, Edward. *Information warfare principles and operations*. Boston, London: Artech House, 1998, p. 150. ISBN 089006511X.

[27] DENNING, Dorothy E. *Information Warfare and Security [Paperback]*. B.m.: Addison-Wesley Professional; 1st edition, 1998, p. 22. ISBN 0201433036.

[28] KUEHL, Daniel. From cyberspace to cyberpower: Defining the Problem. In: Franklin D. KRAMER, Stuart H. STARR and Larry K. WENTZ, eds. *Cyberpower and National Security*. B.m.: Potomac Books, 2013, p. 24–42. ISBN 1597974234.
Many other definitions could be found in this book chapter as well.

[29] BARABÁSI, A L. *Linked: the new science of networks*. B.m.: Perseus Pub., 2002. ISBN 9780738206677.

HOW A SPECIFIC DISCOURSE SHAPES OUR PERSPECTIVE AND THUS STRATEGIC THINKING

As mentioned in the first section, the current debate is quite over-securitized especially due to using inappropriate analogies with key historical events. Jason Healey with Gregory Rattray developed a framework valuable in assessing particular scenarios based on such historical events.[30] The framework uses a traditional military perception to evaluate analogies such as Cyber Battle of Great Britain, Cyber 9/11, Cyber Pearl Harbor, etc. Despite their undoubted contribution in assessing possible events in cyberspace, the paper creates exactly the improper securitization discourse that simply may never emerge. Although, Healey is discreet in over-estimation in his other paper;[31] in this paper, Rattray and Healey first explore some characteristics of cyberspace,[32] though they do not assess appropriately the probability of their analogies in the end; their contribution lies in the military-influenced methodology they wittingly applied in the light of the proposed cyberspace's characteristics. Myriam Dunn Cavelty reacts to such academic work with a strong criticism saying that majority of the policy recommendations and developments strictly focus on military or civil aspects of cyber threats analogous to the conventional and conservative military security frameworks.[33] Cavelty in the mentioned paper divides the securitization discourse of cyber security into three currents: technical, crime/espionage and military/civil defense, as shown in the table 1.

[30] RATTRAY, Gregory and Jason HEALEY. Categorizing and Understanding Offensive Cyber Capabilities and Their Use. In: John D. STEINBRUNER, ed. *Proceedings of a Workshop on Deterring CyberAttacks : Informing Strategies and Developing Options for U. S. Policy*. Washington, DC, USA: National Academies Press, 2010. ISBN 9780309160865.

[31] HEALEY, Jason. Five Futures of Cyber Conflict and Cooperation, The. *Geo. J. Int'l Aff.* 2010

[32] *„1. Logical but physical; 2. Usually used, owned, and controlled predominantly by the private sector; 3. Tactically fast but operationally slow; 4. A domain in which the offense generally dominates the defense; and 5. Fraught with uncertainty." Cited from:* RATTRAY, Gregory and Jason HEALEY. Categorizing and Understanding Offensive Cyber Capabilities and Their Use. In: John D. STEINBRUNER, ed. *Proceedings of a Workshop on Deterring CyberAttacks : Informing Strategies and Developing Options for U. S. Policy*. Washington, DC, USA: National Academies Press, 2010. ISBN 9780309160865.

[33] CAVELTY, Myriam Dunn. The Militarisation of Cyberspace: Why Less May Be Better. Tallin: NATO CCD COE, 2012.

Table 1. Three alternative cyber discourses by Miriam Dunn Cavelty

	Technical	Crime / Espionage	Military / Civil defence
Main actors	Computer experts Anti-virus industry	Law enforcement Intelligence community	National security experts Military Civil defence establishment / Homeland security
Main referent object	Computer networks	Private sector (business networks) Classified information (government networks)	Networked armed forces (military networks) Critical (information) infrastructures
Main threat	Malware Network disruptions Hackers (all kinds)	Advanced persistent threats Cyber criminals, cyber mercenaries States (foreign intelligence)	Catastrophic attacks on critical infrastructures Cyber terrorists States (cyber commands)

Source: CAVELTY, Myriam Dunn. The Militarisation of Cyberspace: Why Less May Be Better. Tallin: NATO CCD COE, 2012.

Cavelty reveals an immensely valuable analysis of cyber security thinking. Her critical approach sees Stuxnet as an intelligence driven operation that is not a sign of cyber war. Based on such a meaning, she criticizes especially the military current of the securitization due to an inappropriate evaluation of the contemporary situation, real threat and available counter-measures, as shown on the Estonian example. Cyber war in the shape of the Battle of Britain is very unlikely at least. In contrast, other kinds of operations, such as less important but precise attacks would multiply. She concluded her article saying: *"Using too many resources for high impact, low probability events – and therefore having less resources for the low to middle impact and high probability events – does not make sense, neither politically, nor strategically, and certainly not when applying a cost-benefit logic."*[34]

Using Cavelty's contribution as an addition to the above drafted logic of securitization thinking reveals the following. The real tendency of conservative and rigid military thinking would cost huge money, threaten people and would not address and successfully cope with emerging cyber security threats. However, the real interest of such behavior can be found if we perceive the analysis differently. The threatening situation and the will to be defended in advance may force some states to obtain a specific defensive technology and to refrain from another. The securitization discourse may serve some particular interests rather than defensive objectives; it may be a part of a discursive strategic influence. Critical geopolitician Simon Dalby came up with the idea of the constructed concept "global threat" that knows no boundaries.[35] The idea is about a social construction of a threat, such as the result of 9/11 events, that has global potential impact; therefore no state is excluded and it is required to cooperate. As a consequence, such discourse legitimizes surpassing the borders representing division

[34] Ibid.

[35] DALBY, Simon. Political Space: Autonomy, Liberalism, and Empire. *Alternatives: Global, Local, Political*. 2005, vol. 30, no. 4, pp. 415–441. ISSN 03043754.

of states' "sovereignties" by enforced discourse seeking for measures adoption that cannot be simply ignored if we are willing to stay within the "group".

Promising academic research has been conducted, for example, by Thomas Rid in his article Cyber War Will Not Take Place[36] that precedes his book in which he applied the introduced arguments on particular events.[37] Rid infers that cyber war will be prevalently filled with operations such as propaganda, sabotage and espionage. The key argument why the contemporary cyber security situation is not a war is based on Clausewitz theory. In spite of some disputable assertions that an act of war must be with no doubt lethal, instrumental and political, cyber war, in Rid's argumentation, apparently bears none of those features. However, his approach is a great contribution for ongoing critical analysis. Constructive critical thinking is a promising way to reflect the reality of cyber war better than adoption of inappropriate historical analogies.

Nevertheless, conquests of territories in future may be devoted to highly precise and perfectly prepared complex operations including discourse pressure, propaganda and a bit of sabotage by novel cyber means with the aim to compel states to fulfill our means. The future will bring non-violent weapons, extremely sophisticated and successful propaganda that crosses borders in milliseconds, and attribution problem not viewed as a problem, but rather as an inseparable component of any future strategy. Territories do not need to be conquered only physically; critical geopolitics has shown us that a forceful pressure may lie in discourse as a power rather than a power in conventional war while trying to achieve strategic objectives. The academic analysis would further focus on such critical approach when dealing with cyber security.

CONCLUSION

In this article, I intended to critically assess the current academic approach to cyber security. I did not aim at a thorough analysis of the over-securitized flow of academic articles and their critics, but to demonstrate that the research agenda in cyber security needs to focus more on constructive critical analysis, rather than on the application of conservative military perspective. Critical views in a wide variety of academic fields proved that such an epistemological approach would contribute to academic research with immensely valuable thoughts. On the contrary, over-securitization and uncreative application of tremendous and threatening historical events to cyber realm may seem to be a tangible approach, but such events are highly improbable in cyberspace, and thus the investment into defensive counter-measures does not solve the problem. Espionage, subversion or sabotage cyber operations are in their possible extreme complexity – and as a part of broader strategic approach – highly probable, and already tacitly taking place. The perception that scholars would adopt depends on their capability to accept the novelty of cyber threat in its extraordinariness and complexity, and the need for appropriate research agenda.

There are three important research areas in cyber security strategy that should be studied. The first one is the creation of an appropriate normative framework for the world community. NATO CCD COE is working on such a project and the outcome is expected by the end of 2014. The novelty of cyber space lies in the widely known "space of freedom" where the organization of people is close to anarchy. Since the "space of freedom" has provided a wide range of cyber crime in global measure, the adoption of new norms is awaited. Software piracy is a perfect example of how a prohibitive and widely accepted norm that prevents stealing another one's property has become completely ignored and unaccepted in cyber space. Norms should regulate not only behavior of individuals, but of states as well.[38] However, these norms have to be developed from scratch rather than adopted from the perspective of the Cold War era and the nuclear war threat. In cyberspace, military operations may

[36] RID, Thomas. Cyber War Will Not Take Place. *Journal of Strategic Studies*. 2013, vol. 35, pp. 5–32. ISSN 0140-2390.

[37] RID, Thomas. *Cyber War Will Not Take Place*. London: Oxford University Press, 2013. ISBN 0199330638.

[38] LEWIS, James A. Sovereignty and the Role of Government in Cyberspace. *Brown Journal of World Affairs*. 2010, vol. 16, pp. 55–65. ISSN 10800786.

occur by which states seek advantage in international relations. Nonetheless, I argue that they will seek the advantage tacitly in complex espionage and sabotage operations, rather than in visible ones as we had experienced during the Cold War. Hence, we should not follow norms like nuclear taboo, because the ones for cyberspace will be completely different and novel to the established international regime.

The second research area is the incorporation of cyberspace conceptualization into strategic analysis. Mere application of historical thinking will not suffice, and a completely new perspective has to be developed. Cyberspace as a military domain is truly different because of one characteristics – it is a domain created by man. Therefore, its shape is changing constantly while being used by individuals, states or other actors, and influenced by their habits. Nuclear warheads mounted to ICBMs (Inter-Continental Ballistic Missile) changed geopolitical distance especially by the capability of warhead delivery in terms of minutes, but cyberspace completely dissolves the geopolitical distance between states. Hence, the defensive reaction to an attack should be focused more on system resilience – as all the major strategies already emphasize[39] – but that does not lower the importance of necessary strategic analysis. Critical geopolitics taught us that geopolitical influence is not limited to physical distance, since the influence is not necessarily demonstrated by military power. This does not mean that the power of discourse as introduced by Michel Foucault[40] replaces military power in geopolitical influence. Nonetheless, we should consider that the power of discourse in achieving strategic objectives in cyberspace has such an important role as it never had before, and is much more important here than in other military domains, especially when defending state against propaganda operations. Cyberspace has to be conceptualized precisely and from a broad perspective, rather than treated in the same way as other domains.

The third area of study should focus on new forms of warfare as a means of gaining advantage over our enemy. Debates discussing whether we are standing in front of a World War III are extremely reductionist and exaggerated. Warfare has always depended on both human strategic thinking and the technology used, and does not necessarily have to involve violence and lethality to compel the enemy to fulfill our conditions. The discussed example of the Estonian "cyber war" is completely inadequate, especially because using the same means would cause no harm today.

Remembering Sun Tzu at the beginning, we should close with his thoughts. The ideal way to conquer the enemy is to take his country completely intact. A more likely scenario than the nuclear type of cybergeddon is a strategy combining cyber methods with psychological warfare, propaganda and extremely precise disruptive sabotage operations with threat of conventional force, but not violating the international law while being focused on state destabilization induced by undermining the trust of citizens in their government.

[39] EU. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*. 2013 [cit. 2014-03-31]. Retrieved from: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

[40] ELDEN, Stuart and Jeremy w. CRAMPTON. *Space, Knowledge and Power: Foucault and Geography*. Abingdon, Oxon, GBR: Ashgate Publishing Group, 2007. ISBN 9780754684589.