Received: 15 October 2014 Accepted: 25 October 2014 Published online: 15 December 2014
Available from www.defenceandstrategy.eu doi: 10.3849/1802-7199.14.2014.02.073-086

Jak citovat tento příspěvek / How to Cite this Contribution

SCHMIDT, Nikola. Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War. *Obrana a strategie.* 2014, roč. 14, č. 2, s. 73-86. ISSN 1802-7199. DOI: 10.3849/1802-7199.14.2014.02.073-086

Nikoli konvenční nebo kybernetická, ale dlouhodobá a nenápadná hybridní válka

Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War

Nikola Schmidt

Abstrakt

Následující článek přistupuje k vybraným konfliktům z perspektivy tzv. hybridní války s akcentem na její komponentu informačních operací a analyzuje související důsledky na mezinárodní bezpečnost. Na jednu stranu jsme svědky zvyšujícího se počtu kybernetických incidentů a s nimi související debaty o kybernetické válce v duchu katastrofických scénářů. Na stranu druhou politici ani národní bezpečnostní strategie viditelně neadresují problém tzv. síťové války (net war), ačkoliv byla odlišena od kybernetické války již v roce 1993. V síťové válce je cílem manipulace s informacemi z decentralizovaných zdrojů, které jsou volně dostupné veřejnosti i elitě. Čína i Rusko mají ale informační operace jako jednoznačný komponent svých vojenských doktrín a jejich vysoce efektivních důsledků jsme viditelně svědky až nyní i díky prudké decentralizaci informačních zdrojů. Hybridní kampaně navíc mohou být snadno proveditelné obejitím současného mezinárodního práva zneužitím tzv. problému přisouzení za využití moderních komunikačních technologií. Bez obranných opatření, jako je např. „mentální odolnost", můžeme čelit rostoucí, tiché, ale vysoce efektivní hybridní válce, aniž bychom si toho byli vědomi, což ve svém důsledku může podkopat kredibilitu, nebo i legitimitu západních demokratických vlád nejen v očích jejich vlastních občanů.

Abstract

The following article perceives selected conflicts from the perspective of hybrid warfare and its component of information operations and analyzes consequent impacts on international security. We are witnessing rising number of cyber incidents and related discussion over a cyber war under the light of doom scenarios without taking into consideration the term "net war" despite the fact it was discerned from "cyber war" in 1993. In net war information manipulation emanating from decentralized sources matters, however, we are still living in a situation where a strategy of influencing minds of public or elite are neither appropriately addressed by politicians, nor by national security strategies. Nevertheless, China and Russia are having information operations as a military component included in their doctrines and their highly effective consequences are evidently visible as late as today. The hybrid campaigns might be easily conducted by circumventing international law through attribution problem in cyberspace through current modern communication technologies. We would face a rising, silent, but highly effective hybrid warfare if any defensive measures such as "mental resilience" are not adopted. We would face it preferably without being aware of it. Finally, the result would undermine credibility, or legitimacy, of the Western democratic governments not only in the eyes of their own citizens.

Poděkování

Text vznikl v rámci projektu PRVOUK č. P17 Vědy o společnosti, politice a médiích ve výzvách doby na UK, FSV, IPS a za podpory projektu grantové agentury Univerzity Karlovy, projekt č. 538213.

Klíčová slova

Kybernetická válka; hybridní válka; informační operace; strategie; současné bezpečnostní hrozby; mezinárodní právo; suverenita státu.

Keywords

Cyber war; hybrid war; information operations; strategy; current security threats; international law; state sovereignty.

INTRODUCTION

The aim of this article is to argue that the future conflict will not be a large-scale conventional war, nuclear armageddon nor a complete chaos caused by large-scale doomy cyber attacks against critical infrastructure. The future conflict will have a hybrid shape in a sense that the conflict will be conducted in several battle-spaces, by several means and will pretend to be isolated as different actions with no relation to each other in a military campaign, but will still be driven by a collective idea without the need of a central command and control. These operations will strictly and precisely circumvent international law through the attribution problem either by denying the physical presence of soldiers violating territorial integrity of an occupied country, denying participation in a cyber attack disrupting critical infrastructure or influencing minds of people that are supposed to stay loyal to their authorities in order to preserve the integrity of the state. All three situations have one characteristic in common – to circumvent the international law by exploiting the attribution problem in its ultimate expectation – to prove the identity behind an attack on 100%. Moreover, the conflict will incorporate as many decentralized components of war as possible that are not and will not be understood as traditional components of war, but will provide a strategic advantage over an unprepared enemy in unprecedented ways by unanticipated means with unpredictable impacts. When information operations (IOps) or cyber attacks are conducted as a part of conventional warfare, they are understood as a military campaign according to international law. However, when these operations are silently conducted in cyberspace with focus on citizens of a particular country (chosen language might be enough to geographically limit the impact) and with the objective to change their minds whether to follow or to oppose their government by indoctrinating lies, or just by a specific interpretation of that government's positions and decisions (calling fascism what is in fact democratically elected government), it cannot be simply evaluated as a military operation, yet in fact it certainly is - as it is linked to military strategic objectives.

Hybrid warfare can be extremely effective; it lacks decisive conventional victory by a lethal force, but its components such as the mentioned IOps may influence minds of a targeted society to the extent that no decisive conventional victory is needed; the objective may be just to relativize key milestones in the history of the affected nation to undermine their current believes or by alternative explanation of current decisions made by the government to undermine its credibility even in the context of already relativized history. Moreover, to reach a decisive conventional victory, it has to be backed by a legal support of e.g. a resolution released by the Security Council or be based on article 51 of UN Charter dealing with the right of self-defense or be widely accepted as a legitimate outcome of a campaign against evident evil as the one against ISIL (Islamic State of Iraq and Levant, or just IS) in Syria and Iraq; if it is not backed, it would never lead to a sustainable victory. However, in hybrid warfare – as already mentioned - there is no need of a decisive victory as no such an outcome is possible, and that is what makes a hybrid strategy one of the most threatening strategic approaches of our enemies in the near future. Some components of hybrid wars might be ongoing for a long-time without our recognition or our first lines of defense and precede a conventional decisive victory that may follow as it has been shown recently in Ukraine.

The following article does not focus on hybrid warfare from the whole perspective as, unfortunately, the term hybrid warfare is not used consistently in the literature[1] and is quite broad in its meaning. The following analysis concentrates at the information operations component of hybrid warfare, the analysis of their strategic layer and the consequent possible impacts to national security.

PRECONDITIONS TO THE HYBRID WARFARE

John Arquilla and David Ronfeldt discerned between "cyber war" and "net war" in 1993; where the former relates to a one-click cyber attack disrupting critical infrastructure in a wide campaign of today's meaning and the latter points to the manipulation of information from decentralized sources aiming to undermine public or elite opinion; net war, quoting Arquilla and Ronfeld *"means trying to disrupt, damage, or modify what a target population 'knows' or thinks it knows about itself and the world around it"* (referring to information operations).[2] The debate over a cyber war, what it means and whether it may ever emerge, is currently a very hot topic in academic journals.[3] In this debate, authors discuss whether a chain of consecutive cyber attacks can be called a war, how such a war is close in its meaning to any conventional war or war on cancer, whether violence needs to be included and what is violence, what is the distinction between force, violence and power, and whether a non-lethal violence should be understood similarly as violence in a conventional war.[4] Hybrid war is not only an asymmetric conflict where the enemy possesses only a different amount of firepower, but a more complex conflict consisting of wide variety of components where the components themselves and their offensive or defensive power are hard to predict, estimate or evaluate; on the other hand they may have a significant impact to the overall military strategy. Currently the most visible scholar dealing with hybrid wars is Frank Hoffman who argues that the distinction between the state and non-state actors and indeed their influence on national security, is blurred as the irregular strategy is used by both of them.[5]

His namesake Bruce Hoffman predicted that the combination of propaganda and information operations effectively conducted by our enemy with our incapability to beat them will lead to their later emergence in alternative battle spaces, with more lethal skills and deeper credibility, as they are toughly

[1] Some available military oriented literature review in detail can be found in FLEMING, Maj Brian P. *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art* [online]. Fort Leavenworth: School of Advanced Military Studies. United States Army Command and General Staff College, 2011 [cit. 2014-12-04]. Available from: https://www.hsdl.org/?view&did=700828

[2] ARQUILLA, John and David RONFELDT. Cyberwar is coming! *Comparative Strategy*. 1993, vol. 12, pp. 141-165.

[3] For a current debate refer to RID, Thomas. Cyber War Will Not Take Place. *Journal of Strategic Studies*. 2012, vol. 35, no. 1, pp. 5-32. ISSN 0140-2390.; STONE, John. Cyber War Will Take Place! *Journal of Strategic Studies*. 2013, vol. 36, no. 1, pp. 101-108. ISSN 0140-2390; GARTZKE, Erik. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security* [online]. 2013, vol. 38, no. 2, pp. 41-73 [cit. 2014-12-04]. Available from: http://belfercenter.ksg.harvard.edu/files/IS3802_pp041-073.pdf; LIFF, Adam P. Cyberwar: A New "Absolute Weapon"? The Proliferation of Cyberwarfare Capabilities and Interstate War. *Journal of Strategic Studies*. 2012, vol. 35, no. 3, pp. 401-428. ISSN 0140-2390; JUNIO, TJ. How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate. *Journal of Strategic Studies*. 2013, vol. 36, no. April, pp. 125-133.

[4] The author of this article contributed to the debate arguing that non-lethal violence in cyberspace is still violence according to Clausewitzian theorization of war. The argument is mainly based on a conviction that such violence is about power as Hannah Arendt explains in her master piece On Violence and power of a man over a man matters when one follows his/her objectives to coerce the adversary to follow his/her will. For more refer to SCHMIDT, Nikola. Super-empowering of non-state actors in cyberspace. In: World International Studies Committee 2014. Frankfurt: Goethe Universitat, 2014.

[5] HOFFMAN, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars* [online]. Arlington, Virginia, USA: Potomac Institute for Policy Studies, 2007 [cit. 2014-12-04]. Available from: http://www.projectwhitehorse.com/pdfs/HybridWar_0108.pdf

defeasible by conventional means.[6] Recently, in October 2014, USA, France, Denmark, Netherlands, United Kingdom, Canada together with some Arabic allies have started with airstrikes against Islamic State in Syria and Iraq. The terrorist threat has not been beaten by any conventional war or sophisticated counter-terrorism efforts, but arose in an unimaginable genocidal shape. The spark that ignited the West's asymmetrical reaction of airstrikes was the beheading of several journalists and humanitarian workers in front of a camera crowned by uploading the video to youtube.com, making it available to the world public with no constrains and causing a deep shock in the whole world population. Cyberspace is not only a proper space for conduction of huge disruptive attacks against critical infrastructure; it is much more about spreading messages with speed and effectiveness never seen before. The beheading of Western civilians has given legitimacy to the airstrikes as the Western public generally agrees with them; hence it seemed to be a nearsighted strategy of ISIL. However, those acts very probably have not been meant to threaten the West and influence decisions of Western leaders, but to tighten the determination between the radicals,[7] to provoke an asymmetric response from the West, and to ground the legitimacy of Islamic State in the minds of their ideological supporters. The propaganda that gives their radicalized supporters blood to the veins is professionally prepared[8] and full of alleged humanitarian activities of ISIL.[9] Indeed, the air strikes cannot stop their propaganda campaign and are very likely to lead to a protracted campaign of hybrid war on different battle spaces as the ground in Syria and Iraq will be much more scorched by war and ISIL will be stronger and more cohesive and radical. They may be weakened conventionally, but certainly not for long, and they will arise again like the ancient hydra conducting various hybrid operations; predictably under a different flag and name, especially because such a cycle has been already seen. This is a hybrid strategy against which no decisive victory is achievable.

ISIL has shown its real face, hence there is a concrete identity behind the atrocities; they masked their faces, but the acts are certainly attributable to ISIL.[10] However, the situation in Ukraine is significantly different, it shows us a strategy focused on delegitimizing any kind of proper reaction of the Ukrainian government against hybrid operations of separatists. The alleged humanitarian convoy and the incapability of the Ukrainian government to stop it or to check it would serve as an example of an intentional act focused on lowering the credibility of the Ukrainian government. Any forceful suspension of the convoy would be understood not only as an act lowering any credibility, but as an illegitimate prevention of the access to humanitarian support. The enemy (or enemies) of Ukraine uses hybrid kind of tactics crowned with the impossibility of a clear attribution process[11] due to its precise deception in order to delegitimize the official government bylowering its credit in the

[6] HOFFMAN, Bruce. *Combating Al Qaeda and the Militant Islamic Threat* [online]. Santa Monica, California, USA: RAND Corporation. 2006 [cit. 2014-12-04]. Available from: http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT255.pdf

[7] PAPE, Robert A. and Michael ROWLEY. Why ISIL Beheads Its Victims. *Politico Magazine* [online]. Washington, 2014 [cit. 2014-10-08]. Available from: http://www.politico.com/magazine/story/2014/10/why-isil-beheads-its-victims-111684.html#.VDVaU5OSzbk

[8] The official website is on the domain www.takvahaber.net, but the server is unavailable most of the time, probably due to ongoing cyber attacks, because the site is time to time reachable.

[9] KAYA, Karen. ISIS's Information Operations: Analyzing their Themes and Messages. *Foreign Military Studies Office (FMSO)*. 2014, vol. 4, no. 10, p. 63.

[10] Here, we have to take into consideration the legal perspective of international law, because we can attribute an attack to ISIL only if we recognize the terrorist group as a state. Before such recognition, the analysis has to be limited to individuals; thus we can approach the situation as a criminal behavior and as such it can be treated in front of International Criminal Court of Justice. I am not making a difference here as it is not so important to explain the wider argument.

[11] Sanctions are imposed against Russia, because the West views some decisions and progress of the conflict as a violation of international law; however, the case of „a little green man" is what is meant here.

minds of the locals, making their own activities as legitimate as possible[12] to increase their own credibility. The result is a direct laugh at the international security regime that seems to be completely toothless in stopping the Russian progress, because the conflict is not about a decisive victory but rather about the deconstruction of the credibility of an enemy's democratic government that may descend into chaos under a pressure of public criticism, and as a result it paves the way for a conventional campaign to be accepted as legitimate in the eyes of the locals, because it reputedly saves them from the ill depicted Ukrainian government. It allegedly solves the problem of chaos caused by the Ukrainian government as we used to hear from locals during the illegal elections in the affected regions. Both examples have one component in common - an impugnment of legitimacy of the enemy by hybrid operations (or its IOps component) in the minds of inhabitants of the targeted territory before a conventional attack; hence it is noticeably the act of aggression or at least it precedes the act of aggression.

Since the end of the Cold War, the military society has been analyzing a revolution in military affairs;[13] however the tactics of information warfare within the scope of the revolution in military affairs has been focused on information used for high-precision weapons or for disruptive information warfare capabilities focused on weapons depending on or controlled by information systems.[14] Both accented problems and the role of information are still a part of a conventional strategic thinking. The whole development of cyber security or the cyber defense agenda in academia, but in policy world as well, is poisoned by such a straight-lined conventional thinking threatening society with doom scenarios[15] that are very unlikely to happen[16], and has been already criticized as a wrong way of cyber security research agenda.[17] Cyber security debate omits or does not put a deserved emphasis on the component of information operations or warfare in favor of threatening politics of doom scenarios concerning cyber attacks on critical infrastructure.[18] I argue that it is happening due to the consistent conventional strategic thinking and, as will be shown further, the national strategies still focus on such kind of catastrophic threats and are silent about hybrid conflicts, especially about their information operations component. Here, it fits to think about the national strategy in cyberspace of a superpower and its coverage of cyber related threats. When the United States presented its approach to face cyber threats by declaring cyberspace as the fifth domain,[19] it did not address its potential use for conducting information operations; the whole declaration was only about the information infrastructure, societal

[12] Russia's new tactics of war shouldn't fool anyone. *The Washington Post* [online]. 2014 [cit. 2014-10-09]. Available from: http://www.washingtonpost.com/opinions/russias-new-tactics-of-war-shouldnt-fool-anyone/2014/08/27/0cb73b3a-2e21-11e4-9b98-848790384093_story.html

[13] A comprehensive study of RMA in available literature can be found in FRIDMAN, Ofer. "Are We Ready for the Revolution of Nonlethal Weapons?": Using a Comprehensive RMA Model to Examine the Current Strategic Situation. *Comparative Strategy* [online]. 2013, vol. 32, no. 3, pp. 192-206 [cit. 2014-12-04]. ISSN 0149-5933. Available from: doi:10.1080/01495933.2013.805993

[14] METZ, Steven and James KIEVIT. *Strategy and the Revolution in Military Affairs: From Theory to Policy*. DIANE Publishing, 1995. ISBN 1428914641.

[15] CLARKE, R.A. and Robert KNAKE. *Cyber War: The Next Threat to National Security and What to Do About It*. New York: HarperCollins, 2012. ISBN 9780061962240.

[16] RID, Thomas. Cyber War Will Not Take Place. *Journal of Strategic Studies*. 2012, vol. 35, no. 1, pp. 5-32. ISSN 0140-2390.

[17] SCHMIDT, Nikola. Critical Comments on Current Research Agenda in Cyber Security. *Obrana a strategie*. 2014, no. April, pp. 29-38.

[18] CAVELTY, Myriam Dunn. The Militarisation of Cyberspace: Why Less May Be Better. In: Christian CZOSSECK, Rain OTTIS and Katharina ZIOLKOWSKI, eds. 4th International Conference on Cyber Conflict. Tallin: NATO CCD COE, 2012, pp. 141-153.; *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London and New York: Taylor & Francis, 2007. ISBN 9780203937419; Cyber-terror - looming threat or phantom menace? The framing of the US cyber-threat debate. *Journal of Information Technology & Politics*. 2008, vol. 4, pp. 19-36. ISSN 19331681.

[19] LYNN III, William J. Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*. 2010, vol. 89, pp. 97-108. ISSN 00157120.

or military dependence on information technologies and about determination of a hundred intelligence agencies to break through or disrupt such infrastructure. Not a single word about information operations was mentioned. On the other side of the globe, Russia has as its top priorities the security of information, information as the battle space and its manipulation as a weapon.[20]

UNDERSTANDING INFORMATION COMPONENT OF HYBRID WARFARE IN THE CONTEXT OF CURRENT TECHNOLOGICAL SITUATION

There are several problems of conventional strategic thinking that have to be unlocked in the minds of military staff, but probably even more in the minds of policy makers. The foremost is the fact that the conventional strategy does not apply to cyberspace and thus that neither similar conflict to conventional war will spark in cyberspace, nor doom scenarios are coming.[21] Debate over a territory in cyberspace in which a state wields traditional sovereignty[22] is a non-sense based on the technological principles of cyberspace (borders exist if respected); even though the debate over sovereignty in cyberspace is completely valid as security issues caused by cyberspace have implications to states' security. All the already analyzed characteristics of cyberspace such as transformation of temporality to near instantaneity, transcendence of geographical physicality, permeation of boundaries and jurisdictions, fluidity of rules and configurations, open and available participation of a free choice, attribution problem and lack of accountability[23] directly deconstruct the conventional thinking of territory in cyberspace and should be precisely reflected in the further strategy development; moreover, a related debate should be opened again to reconsider a violation of state sovereignty by attributable propaganda. If the deliberate and precisely targeted flow of disinformation effectively influences minds of people within a certain territory using cyberspace, the debate over a violation of sovereignty is on place, but will rise questionable positions.

This debate is not completely new. It was for the first time on the table of the League of Nations in 1936 discussing huge propaganda conducted by Nazi German over radio frequencies.[24] The debate had progressed during the following decades and created two different schools of law: the broad responsibility school and the narrow responsibility school;[25] where the former explanation understands responsibility of an individual as a responsibility of the state whereas the latter understands the state responsibility unaffected by actions of individuals. However, the author evolves the topic in the following chapter into a term "war-mongering propaganda by a state" based on the mentioned discussion in the League of Nations.[26] He analyzes that any activity that encourages population of a foreign country or the state itself to make the first step towards war declaration, invasion, naval blockade or assistance to armed bands organized on the territory of a sovereign state are considered as an act of war.[27] The case when United States supported Nicaragua rebels has been used as an

[20] MCDERMOTT, Roger. Russia's Information-Centric Warfare Strategy: Re-defining the Battlespace. *Eurasia Daily Monitor*, The Jamestown Foundation [online]. 2014, vol. 11, no. 123 [cit. 2014-11-18]. Available from: http://goo.gl/QaiEe3

[21] GARTZKE, Erik. The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security* [online]. 2013, vol. 38, no. 2, pp. 41-73 [cit. 2014-12-04]. Available from: http://belfercenter.ksg.harvard.edu/files/IS3802_pp041-073.pdf

[22] CCDCOE. *Tallinn Manual on the International Law Applicable to Cyber Warfare*. New York: Cambridge University Press, 2013. ISBN 978-1-107-02443-4.

[23] CHOUCRI, N. *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press, 2012, p. 4. ISBN 9780262517690.

[24] ANDROUNAS, Elena and Yassen ZASSOURSKY. Protecting the Sovereignty of Information. *Journal of Communication*. 1979, vol. 29, no. 2, pp. 186-192. ISSN 0021-9916.

[25] WHITTON, John Boardman and Arthur LARSON. *Propaganda towards disarmament in the war of words*. New York: Oceana Publications, 1963, pp. 133-139.

[26] Ibid., p. 62.

[27] Ibid., p. 63.

example that training a cyber rebel units to fight their government in cyberspace is understood similarly.[28] However, such conclusion applies very conservatively and does not easily include information operations especially because they are hardly attributable in general as they are conducted carefully, wisely, silently and patiently for a long time. It must be attributed to a state and to its military authorities to be understood as an act of war even though the "troll armies" seems to be exactly such an exposure of military capability when organized so precisely, however, the wide distribution of each unit, decentralized leadership, unprovable involvement of state or military authorities, but high effectiveness is a toughly defendable hybrid strategy.

Also spreading a resentment that a nation faces a threat (that is evidently unconfirmed) and pressing on a response that has a shape of a preventive war, or an operation to secure allegedly oppressed people, is considered as a violation of state sovereignty and might be considered as an act of war. In that perspective, Russia definitely violates international customary law just by the way how the information over Ukraine in 2014 was interpreted and precisely what interests such activity follows. However, the attribution problem and the consequent processes toward confirmation of the particular state involvement are denying using such jurisdictional perspective and thus remain toughly enforceable by law.

However, access and free flow of information is the core value of Western societies; hence any kind of regulation to preserve and defend sovereignty against such deliberate spreading of disinformation is unbearable (narrow responsibility school). In that perspective, information operations using current communication systems, social networks or deliberately created propaganda portals conducted to undermine a state sovereignty by spreading hatred, fear, resentment and bad blood are an immense power that is indefensible under a current legal as well as security international regime. The problem is not new, the technology is new, the access to social networks in our pockets and thus a shift of prime information flow from professional journalism to peppery social sharing susceptible to prefer controversial, conspiratorial and shocking news is completely new and has these explained consequences. The defensive measures have to be identified and trained - professionals already call such measure a *mental resilience*.[29] The ability to critically assess controversial information and withstand intended mental influence of our minds, of our interpretation of historical consequences and all other deliberate influence to undermine our beliefs into our value structures.

The debate whether the mentioned "troll armies" should be engaged and fought in cyberspace by governments, whether their disinformation campaigns should be hacked-backed or somehow confronted has been already opened. The idea would be to distinguish between general public and troll armies with the latter not being given (e.g.) the rights of free speech.[30] It is certainly highly questionable. However, the debate whether information can be weaponized is under huge analytical efforts[31], especially, after the events following the "Maidan revolution" in Ukraine preferable under a lead of the Russian Federation. In the cited analysis produced by the Institute of Modern Russia, the authors mentioned that Kremlin *"exploits the idea of freedom of information to inject disinformation into society. The effect is not to persuade (as in classic public diplomacy) or earn credibility but to sow confusion via conspiracy theories and proliferate falsehoods"* and they continue asserting that *"the aim is to exacerbate divides and create an echo chamber of Kremlin support."* The injection of divide into democratic societies using lies is focused on *"using local rivalries and*

[28] The original case can be found at I.C.J. *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Merits*. 1986. *I.C.J. reports*. Analysis of relations in cyberspace according to the case can be found in HEINEGG, Wolff Heintschel von. Legal Implications of Territorial Sovereignty in Cyberspace. In: R. Ottis C. CZOSSECK, ed. Tallinn: NATO CCD COE Publications, 2012.

[29] Mentioned in a presentation of Jarno Limnéll from McAfee during his presentation on CyCon Conference 2014 organized by CCD COE in Tallinn Estonia.

[30] Applebaum, Anne. Svobodu projevu. Ale ne pro trolly. *Ihned.cz* [online]. HN: 2014 [cit. 2014-12-2]. Available from: http://archiv.ihned.cz/c1-63199160-svobodu-projevu-ale-ne-pro-trolly

[31] POMERANTSEV, Peter and Michael WEISS. The Menace of Unreality : How the Kremlin Weaponizes Information , Culture and Money. 2014.

resentments to divide and conquer."[32] Such a strong accusation of Russia is certainly serious, however, it nicely fits into our assertion that the hybrid warfare could be conducted completely without the victim being aware of it. The same analysis puts an emphasis on Central European countries as they in many cases tend to accept the conspiracy explanation of current events in Ukraine even though they have suffered decades long oppression from Russia. Such a situation is certainly a moment in a divided society that is not capable to recognize a deliberate bending of historical events focused on relativization of its principal context that led to current values and structures; on the contrary it does not even lead to a loss of faith in current political representatives, but it leads into a loss of faith into the whole political system of liberal democracy. The next step is usually an increased support of the radical parties prepared to support Kremlin politics as we have witnessed in France, but in Hungary as well, or for apolitical messiahs with a populist program of saving miraculously the society like in the Czech Republic. This deliberate division of society is a part of a wider strategy as well and should not be disregarded in its context. Especially because it leads into a loss of faith into the basic democratic institutions and thus the whole system of liberal democracy.

SPACE, TERRITORY AND BATTLE-FIELD. THE STRATEGIC INSIGHT

Cyberspace as a space or territory is just a specific interactive component upgrading possibilities in a complex hybrid warfare strategy. Calling for sovereignty in cyberspace over cyber installations in particular states does not solve the problem; from the strategic perspective it is a non-sense without the desirable strategic effect; especially because all the actors, including states, do not respect it. Rid's prophetic prediction about rising number of less violent but more numerous cyber attacks[33] are not based only on his feelings, but empirical background.[34] Pronouncing sovereignty cannot serve as a defensive or deterrence strategy - rules neither apply in cyber space, nor in hybrid warfare;[35] enemy does not have motivation to obey them when conducting operations silently and under cover of the attribution problem; neither states, nor non-state actors. Enemy does not respect "boundaries" when attacking a particular server to influence the information saved. If the attribution problem helps and thus causes states to play a role of non-state actors in cyberspace[36] (from a legal perspective), and even the sophistication criterion cannot be used to attribute particular attack to a state,[37] then we need to perceive states in cyberspace as any other non-state actors. In that perspective, there is no way how to enforce states to play a fair game of traditional conventional war where e.g. war declaration makes difference between two bodies of international law - *ius ad bellum* and *ius in bello* - and thus gives defenders juridical framework for an appropriate defensive behavior. The silence of both information and conventional component of hybrid wars, along with the problematic application and prevalent circumvention of international law not only in cyberspace, plays into the cards of those willing to use their power today.

[32] Ibid.
[33] RID, Thomas. More Attacks, Less Violence. *Journal of Strategic Studies* [online]. 2013, vol. 36, no. 1, pp. 139-142. ISSN 0140-2390.
[34] Difference between the number of attacks in 2010 and 2011 is an increase of 83% according to EGAN, Gerry, Kevin HALEY, David MCKINNEY, Tony MILLINGTON, Joanne MULCAHY, Thomas PARSONS, Andrew WATSON, Mathew NISBET, Nicholas JOHNSTON and Sean HITTEL. *Internet Security Threat Report*. Symantec, 2012 [cit. 2014-12-04]. Available from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf
[35] HOFFMAN, Frank G. *Conflict in the 21st Century: The Rise of Hybrid Wars* [online]. Arlington, Virginia, USA: Potomac Institute for Policy Studies, 2007, p. 16 [cit. 2014-12-04]. Available from: http://www.projectwhitehorse.com/pdfs/HybridWar_0108.pdf
[36] SCHMIDT, Nikola. Super-empowering of non-state actors in cyberspace. In: *World International Studies Committee 2014*. Frankfurt: Goethe Universitat, 2014.
[37] GUITTON, Clement and Elaine KORZAK. The Sophistication Criterion for Attribution. *The RUSI Journal*. 2013, vol. 158, pp. 62-68. ISSN 0307-1847.

The silent information operations in combination with the attacker's patience would lead into effective mind disruptions and can be used as a preparatory operation in advance to a conventional one. Operations aimed to dishonor, delegitimize and accuse the government based on mendacious propaganda and diffusion of conspiratorial theories are barely defensible. If there is a strategic relation to a planned conventional mission, the patience would be stronger, more serious, better prepared and planned and would last longer than comparable disinformation mess before election campaigns; hence the implication would be much more serious to the national security as the game ends here. Therefore, if there were a strategic consequence the effectiveness would be multiplied.

Frank Hoffman thinks that we are going to experience a decentralized hybrid warfare in the near future that *"incorporates a range of different modes of warfare, including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder."*[38] Battlefield does not need to be limited to a sovereign physical territory on which huge conventional armies have to be supported by logistics, but would be more about spreading ideas and moving digitized money as theorists behind the fourth generation warfare (4GW) predict.[39] They also point very providently that the main purpose of a war is still 4GW oriented and focused on changing minds of *"our opponents to force them to fulfill our will."*[40] It is about non-lethal power that is still violent as Hannah Arendt analyzed: *"A power of a man over a man"*[41] is by her words a violent activity as it leads to a deliberate and enforced compellation of our will. No lethal force is needed. The message sent to the decision makers and to the population is what makes difference in forthcoming strategic intentions rather then a disruption of military assets by cyber means that are much more useful during an active conventional operation. Changing minds in psychological operations[42] has an irreplaceable position in military doctrine as anticipating the enemy's intentions is shaped by the "firing" side; hence, it helps the following conventional operations to be successful and the actions of the enemy foreseeable. I argue, that the same applies to the whole society within particular states and does not need to be limited to isolated military operations. Long-lasting, silent, undetectable and soft diffusion of disinformation dividing the targeted society is in that perspective a substantial threat. If Russia and China oppose the paradigm of "cyber security" and promote "information security" instead during debates at OSCE and anywhere else, it is supposed to be understood as an emphasis to not only a different defensive strategy, but a different offensive strategy as well.

Therefore, we should not be limited to information operations as a single-shot act seeking a desired objective.[43] We would rather understand information operations as a part of a wider national security strategy of states that still think in the framework of *"stronger survives"* or as a part of an *unrestricted warfare* where no rules apply as the prevalent part of the operations are silent, secret and long-lasting. Unrestricted warfare from the Chinese military doctrine is based on three principles: an omni-directionality, synchrony and asymmetry.[44] First, omni-directionality says that the fight is conducted on

[38] HOFFMAN, ref. 35

[39] HAMMES, TX. War evolves into the fourth generation. *Contemporary Security Policy*. 2005, vol. 26, no. 2, pp. 189-221.

[40] Common clausewitzian perspective. CLAUSEWITZ, C, M. HOWARD, P. PARET and B. HEUSER. *On War*. Oxford: Oxford University Press, 2007. ISBN 9780192807168.

[41] ARENDT, Hannah. On Violence. In: *Crises of the Republic*. San Diego, New York, London: Harcourt Brace Jovanovich, 1972, p. 105-198. ISBN 0156232006.

[42] YAWORSKY, William. Target Analysis of Shining Path Insurgents in Peru: An Example of US Army Psychological Operations. *Journal of Strategic Studies*. 2009, vol. 32, no. 4, pp. 651-666. ISSN 0140-2390.

[43] Compare a well prepared monograph on information operations, which is prevalently perceived from a military perspective WALTZ, Edward. *Information warfare principles and operations* [online]. Boston, London: Artech House, 1998. ISBN 089006511X with contemporary concerns regarding information operations from Russia in HEICKERÖ, Roland. *Emerging Cyber Threats and Russian Views on Information Warfare and Information Operations*. Stockholm: Swedish Defence Research Agency. 2010.

[44] LIANG, Qiao and Wang XIANGSUI. *Unrestricted warfare*. Beijing: PLA Literature and Arts Publishing House, 1999.

various battlefields, so we should not be limited to a spreading of messages between military armies, but would switch to thinking that the battlefield is everything around us (information warfare using media, financial/economic warfare using critical supplies such as oil or gas, etc.).

Second, the principle of synchrony says that all the actions can be conducted at the same time on different battlefields. Cyber attacks in Georgia as a part of a conventional Russian campaign were not limited to the territory of Georgia as some servers were attacked in Azerbaijan as well.[45] They were not attacked by DDoS to only make them unavailable, but they were defaced as the information on the servers was changed and plenty of mendacious articles were published to shape minds of the Georgian population to spark a debate whether the whole situation is not just an infantile fail of their own government even though the conventional bloody campaign was ongoing in the name of the allegedly oppressed Russian population. Exactly the same hybrid strategy was used in Ukraine during the Crimea annexation and occupation of Donbas and Luhansk territories of the sovereign state. The principle of synchrony exactly emphasizes the wideness of hybrid warfare based on a possibility of perfectly synchronized operations without capacity of the enemy to recognize them at the same time. The information shaping and denial in Georgia was assessed as a part of the Russian tactics - hence can be attributed to Russia - as it evidently was a part of the wider conventional campaign conducted by Russia on a physical territory; however, such an operation approached separately, or non-attributable to a visible conventional campaign, would be usually assessed neither as a military act, nor as a use of force even though it may have comparable strategic consequences. The delegitimizing campaign against Georgia and the converse campaign to make the Russian practice legitimate, even though the international law says exactly the opposite (a case of war-mongering propaganda by a state), is a component of the hybrid warfare strategy. Hence the conclusion here is that hybrid operations would have strategic critical impacts on conventional ones and that conventional operations would be critically dependent on the apparently legal hybrid operations. I would like to add here that the operations would not need to be separated in time even by months or years to be perfectly synchronized in the wider strategy. The principle of synchronization would last in synchronization of operations following one objective in different time as well (the opposite kind of synchronization than defined in unrestricted warfare); thus, it is a tough task to perceive them in different time as threatening operations preceding something bigger in synchrony. If this is the case, the current international law is completely toothless; an information operation enabling use of force is not use of force.

Third, the principle of asymmetry says that overlooking rules gives power to the weaker and circumventing international law by the powerful nation empowers it even more. However, non-state actors such as terrorist groups, robbers, bandits and their organizations existing more on the line of charisma instead of institutions and driven by radical thinking instead of professionalism are becoming relevant actors rising their hands against states, quoting van Creveld.[46] These organizations are not limited to terrorists only, but also include idealistic, libertarian and anarchic decentralized hacker communities developing their own digital currencies and calling for a total deconstruction of a state as a meaningless entity.[47] These organizations can play a significant role in a step-by-step process of delegitimizing the state by forming, and spreading out conspiracy theories, but effectively developing alternative interaction cyber spaces for radicals to share knowledge and stay organized. Such environment would be capable to enable wider strategic and political objectives of a superpower using information operations to divide the society and take over the power. That applies to Al Qaeda, much more to ISIL seeking for its legitimacy between radicalized people around the whole world,

[45] DEIBERT, R. J., Rafal ROHOZINSKI and M. CRETE-NISHIHATA. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. *Security Dialogue*. 2012, vol. 43, pp. 3-24. ISSN 0967-0106 1460-3640.

[46] VAN CREVELD, Martin. *Transformation of war*. New York: Simon and Schuster, 1991, p. 359. ISBN 1439188890.

[47] An example would be a newly established association called “Paralelní polis” in the Czech Republic which is openly focused on an ultimate deconstruction of state in favor of auto regulated society using digital currency bitcoin that is completely independent on state regulation.

however, above all, it applies to separatists playing the role of proxies of higher and wider political objectives of much more powerful countries like Russia. The environment, available equipment and battlefield have changed significantly, but the strategy in national security documents surprisingly has not changed significantly.

A SELECTION OF NATIONAL STRATEGIES AND HYBRID WARS

In the perspective sketched above, the pure distinction between combatants and non-combatants is blurred and becomes irrelevant. The US administration[48] put an emphasis on new forms of warfare in 2005 in the National Defense Strategy and divided them into traditional, irregular, catastrophic and disruptive,[49] but it lacks a word about hybrid warfare using a combination of all available means to gain strategic advantage. The security advisory community in 2009 is certainly aware of the above-mentioned characteristics of hybrid warfare and accentuated the consequences very precisely.[50] However, in National Security Strategy published in 2010, threats within the cyber domain are still perceived preliminary as a threat to physical networks or as a possible large-scale cyber attack. The whole document lacks a word about hybrid conflict or information operations as well.[51] Albeit the strategy marked cyber threats as the most threatening threat to the national security, the counter-measures are still focused only on activities such as to *"deter, prevent, detect, defend against, and quickly recover from cyber intrusions and attacks by* (…) *investing in people and technology"* and *"strengthening partnerships,"*[52] which are measures against cyber war, not a net war.

Hence, the strategy still thinks in the light of catastrophic singular doomy events such as 9/11 that could happen in cyber space;[53] not in the light of protracted long-lasting silent hybrid warfare exploiting cyberspace. Moreover, the National Security Strategy final draft document from 2013 (20 years later after the article of Arquilla and Ronfeldt discerning between cyber war and net war was published) is still explaining the cyber related threats in the conventional perspective of a clash between offensive and defensive capabilities that have to be strengthened to face future cyber threats with no reference to information operations, net war or threat of systematic propaganda. There is neither a measurable power in the perspective of the theory offense defense balance[54] in cyber war, nor in the net war, however, these policy makers surely think it is. The reason probably lies in the way of traditional thinking. Concretely said, Western society is extremely sensitive to the topic of information consistency, integrity or in recognizing manipulation; hence any "demanipulation" processes as a defensive measure would be understood as a violation of a fundamental right - freedom of speech. Nevertheless, China openly develops its information capabilities as a response to the US technological

[48] Used here for the analysis, because it is understood as one of the most important security insurance in the Atlantic community.
[49] RUMSFELD, Donald H. The national defense strategy of the United States of America. *Washington, DC*. 2005, pp. 2-4.
[50] United States Government Accountability Office. *Hybrid Warfare* [online]. 2009 [cit. 2014-12-04]. Available from: http://digital.library.unt.edu/ark:/67531/metadc295393/
[51] *National Security Strategy*. Washington: White House. 2010
[52] Ibid.
[53] Interesting comparison of possible cyber events based on historical conventional events can be found in 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.
[54] GLASER, Charles L. and Chaim KAUFMANN. What is the Offense-Defense Balance and Can We Measure it? *International Security*. 1998, vol. 22, pp. 44-82. ISSN 0162-2889.

advantage[55] and has a strong capacity in the research of so-called unrestricted warfare, integrated network electronic warfare and information confrontation.[56]

Core national security strategies simply omit the information component of modern hybrid warfare even though the military community is completely aware of the problem and has been working on counter strategies of such threat,[57] and the policy environment reflects the situation as well.[58] Above all, the world has witnessed hybrid warfare conducted by Russia in more than one occasion just in the last decade (2007 DDoS in Estonia,[59] 2008 attack of media in Georgia and Azerbaijan,[60] 2014 Ukraine); hence the appropriate national security positions are more then required.

However, the debate is quite chaotic in the sense of what is cyber war, information operations, information war, net war or hybrid war. Some authors discussed the events in Estonia as information war[61] even though the same act is in strategies and other articles rather called cyber attack or cyber war[62] due to its nature in DDoS - denial of service attacks. Such inconsistency in the whole debate is precarious for appropriate study and policy reflections. However, all those terms are supposed to be studied as components of a new phenomenon in the international security environment - the silent hybrid warfare.

CONCLUSION

This article argued that the contemporary security environment is moving toward rather complex and silent hybrid warfare than toward visible one-shot catastrophic doomy cyber attacks. Hybrid warfare should be deconstructed into several components and the article focused prevalently on the component of information operations. The complex of components represents separate types of incidents or campaigns that should not be approached in isolation even though occurring in different time. Moreover, when analyzed in context it would refer to a wider campaign where international law is circumvented, attribution problem is exploited by states and involvement is consistently denied. Several examples were shown in which different shapes of hybrid warfare have been used. In the case of ISIL the attribution to a higher entity has been admitted while the tactics have been used to radicalize other Sunnis. In the case of Ukraine a combination of information operations and conventional attack was aimed on a territorial conquest, but also to undermine the Ukrainian government and its legitimacy in

[55] BARRETT, Barrington M. Information Warfare: China's Response to U.S. Technological Advantages. *International Journal of Intelligence and CounterIntelligence*. 2005, vol. 18, no. 4, pp. 682-706. ISSN 0885-0607.
[56] WORTZEL, Larry M. *The Chinese People's Liberation Army and Information Warfare* [online]. Carlisle: U.S. Army War College, 2014 [cit. 2014-12-04]. ISBN 1584876085. Available from: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA596797
[57] FLEMING, Maj Brian P. *The Hybrid Threat Concept: Contemporary War, Military Planning and the Advent of Unrestricted Operational Art*. Fort Leavenworth, Kansas: School of Advanced Military Studies. United States Army Command and General Staff College, 2011; LASICA, Col Lt Daniel T. *Strategic Implications of Hybrid War: A Theory of Victory* [online]. Fort Leavenworth, Kansas: United States Air Force, School of Advanced Military Studies, 2009 [cit. 2014-12-04]. Available from: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA513663
[58] WILSON, Clay. *Information Operations, Electronic Warfare, and Cyberwar* [online]. 2007 [cit. 2014-12-04]. Available from: http://www.dtic.mil/dtic/tr/fulltext/u2/a466599.pdf
[59] KAMPMARK, Binoy. CYBER WARFARE BETWEEN ESTONIA AND RUSSIA. *Contemporary Review*. 2007, vol. 289, pp. 288-293. ISSN 00107565.
[60] DEIBERT, R. J., Rafal ROHOZINSKI and M. CRETE-NISHIHATA. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. *Security Dialogue*. 2012, vol. 43, pp. 3-24. ISSN 0967-0106 1460-3640.
[61] BLANK, Stephen. Web War I: Is Europe's First Information War a New Kind of War? *Comparative Strategy*. 2008, vol. 27, no. 3, pp. 227-247. ISSN 0149-5933.
[62] KAMPMARK, Binoy. CYBER WARFARE BETWEEN ESTONIA AND RUSSIA. *Contemporary Review*. 2007, vol. 289, pp. 288-293. ISSN 00107565.

the eyes of Ukrainian nation in order to ease the conventional advancement and to complicate any operations conducted by the Ukrainian army. However, similar activity was discussed already in 1936 within the international body of League of Nations after the Nazi exploitation of radio frequencies to spread their propaganda throughout Europe with the aim to delegitimize Western governments, strengthen legitimacy of the Nazi government and to portray their intentions as legitimate. The subsequent juridical research thoroughly analyzed similar activities and reached a consensus that when conducted by a state it is to be approached as a violation of state's sovereignty. However, the related consequences are usually hard to attribute and thus hard to defend by international pressure based on international law; especially when the current "troll armies" operating in cyberspace of social networks seem to be a "voice of public". Such covert strategy dissolves and questions defensive arguments of the affected governments; complicate attribution processes of the adversary and serves as a self-activating mind bomb of indoctrinated self-fulfilling prophecies within conspiracy theories presented as an objective reality. If this process is enough long-lasting and patient it does not need to reach tangible strategic objectives in the shape of people's trust in something desirable by the adversary, but may very easily reach an objective to delegitimize the affected country and its government, by e.g. relativizing the importance of key historical events and thus milestones of general values structure development. In a reaction to this new situation the concept of mental resilience has been introduced as a piece of possible wider defense strategy against an information component of hybrid operations. Mental resilience is a crucial defensive capability against deliberate intrusions into minds of civilians aiming to divide them on the line of alternative interpretation of current or historical events that constitute a consistent and shared awareness of their identity; a strategy that seeks the objective to "divide and govern." The brief analysis of several U.S. national security and defense strategies unveils non-addressing this component of information operations or hybrid warfare itself. On the other hand, general awareness - as a defensive measure - of cyber security threats are included in every recent strategy. Moreover, it was argued that the battle space should be understood as a wide variety of battle spaces that links each other into one complex; our minds and beliefs in a particular explication of our history including. No information operation campaign is conducted without deeper strategic intentions; hence every such campaign should be understood from a wider perspective and in the context, even though it is legal as an isolated act. The hybrid warfare is a topic that has been studied and on which scholars have been putting some emphasis. It is a part of military doctrines, but surprisingly, it is not included in national security strategies as an alarming new threat due to the society interconnectedness. And even though hybrid warfare seems to be one of the most threatening and effective strategic approaches that could undermine Western democracies in the near future, politicians keep silent over it.