



Ad Securitatem

The best essays written by students at the
Baltic Defence College during 2015/16



Contents

Foreword

4

Joint Command and General Staff Course (JCGSC) 2015/16

How can NATO as a collective alliance effectively counter the threat of Russia's hybrid warfare?

MAJ Priit Heinloo

6

What is the significance of the emergence of the Wider North to Estonia?

MAJ Indrek Sarap

22

Given the strong Russian and Soviet heritage for use of air power in directly subordinated support of land operations, how would a near-future contest between NATO and Russian forces match this against NATO's air doctrine of independent, deep air operations?

MAJ Steven Grimshaw

45

Does globalisation cause asymmetric conflicts? Is it part of the solution or problem?

CPT Ale Prosic

65

Is network theory the most suitable for understanding terrorist radicalisation?

MAJ Mari Cecilie Tølfesen Reinskou

79

The Russian A2/AD capabilities in Baltic Sea region: are they existential threat to the defence of Baltic countries, or another buzzword?

MAJ Klaus-Jürgen Kaivo

91

Was Stuxnet an Act of War?

MAJ Janis Jansons

103

The Implications of Russian Federation Security Strategy for the Baltic States' military security.

MAJ Andrius Jagminas

121

Is Russia a strong or a weak power?

MAJ Davit Aghabekyan

140

Given the nature and understanding of what is being called Hybrid Warfare today, how can NATO, as a collective alliance, effectively counter hybrid threats? What would an Alliance Counter-Hybrid Warfare Operating Concept look like? What would be some of the challenges associated with such a concept?

MAJ Darius Meilunas 157

Is Russia's hybrid war contagious? Has the world just witnessed the outbreak of a new age of 'peaceful war'?

MAJ Kaspars Miežitis 176

Higher Command Studies Course (HCSC) 2016

Can small- and medium-sized states have grand strategies?

LTC Armin Wagner 191

Can it ever be ethical to deliberately kill enemy non-combatants during an armed conflict?

LTC Michael Christensen 209

Can the forward deployment of armed forces extend and entrench regional security?

Mr Karolis Aleksa 224

Foreword

Welcome to the second edition of *Ad Securitatem*, a collection of the best essays produced by students at the Baltic Defence College during the 2015/16 academic year.

Academic writing continues to play a key part in the educational process at the Baltic Defence College. Throughout the 2015/16 academic year, the students of the Joint Command and General Staff Course (JCGSC) 2015/16 and the Higher Command Studies Course (HCSC) 2016 have engaged in research and writing in areas related to operations, leadership, political and strategic studies, and beyond.

With the encouragement and support of Baltic Defence College faculty acting as supervisors, students have produced perceptive writings which demonstrate their determination and inquisitiveness. As with the previous edition of *Ad Securitatem* the booklet could easily have been double the length, such is the quality of work produced by this year's cadre. As such, I hope the essays present provide at least an illustration of the aptitude of the students of the 2015/16 JCGSC and 2016 HCSC from their time at the Baltic Defence College.

Dr Ashley Roden-Bow
Lecturer, Critical Thinking and Communication
Acting Director, Department of Leadership

Joint Command and General Staff Course (JCGSC)

How can NATO as a collective alliance effectively counter the threat of Russia's hybrid warfare?

MAJ Priit Heinloo

Introduction

Now we have reached the hour when we can no longer ignore this problem, which, in the interest of national defense, we should face squarely (Douhet, 1921, p. 31).

Almost a century ago Giulio Douhet foresaw a dominant role of air power in warfighting. Although a large part of his vision proved to be untrue, producing opposite effects to what he imagined (most notoriously, carpet bombings in World War II), some of his ideas are still highly regarded – a sentence resembling his ‘To conquer the command of the air means victory; to be beaten in the air means defeat and acceptance of whatever terms the enemy may be pleased to impose’ (Douhet, 1921, p. 28) are probably voiced in most of modern military educational institutions. Today, some have argued, we are facing a comparable change in the character of warfighting – the emergence of hybrid warfare. This evolution has been rapid enough to raise concerns about the security of even the strongest contemporary military alliance, evoking questions of NATO's ability to cope with the alleged transformation (Berzins, 2014, pp. 8–9; Vandiver, 2014). Amongst myriads of articles published after Russia's surprising aggression in Crimea in 2014, that brought the term *hybrid warfare* to widespread use, several publications mention specific NATO members as the next possible targets of similar belligerent actions (Stoicescu, 2015; Colby and Solomon, 2015, pp. 22–24). On the other hand, counterarguments rejecting any relevance of ‘hybrid element of Russia's operation in Ukraine’ to NATO (Charap, 2015, p. 52) have also been presented. This essay positions somewhere in-between of these opposing opinions and argues that the hybrid warfare concept used by Russia cannot be applied universally; therefore NATO can devise successful preventive and counteractions by focusing its efforts to specific threatened regions. To support this argument, firstly the theoretical background of Russia's *new generation warfare concept* and its practical application will shortly be presented.

Secondly, the implications for NATO – the extent of the threat and the possibilities for countering it – will be discussed.

Russia's hybrid warfare in brief

First of all, one must consider, what is meant by *hybrid warfare*. The definition has evolved since 2002, when it was first used (Racz, 2015, p. 28), denoting different ways of waging war observed by researchers. Initially the term described the mixture of regular and irregular tactics stemming from the combination of traditional social structure and modern technology successfully employed by Chechens against Russia (Nemeth, 2002, pp. 49-54; Racz, 2015, pp. 28–29). Israeli-Hezbollah war in 2006 was also described as a hybrid war incorporating ‘a full range of different modes of warfare including conventional capabilities, irregular tactics and formations, terrorist acts including indiscriminate violence and coercion, and criminal disorder’ (Hoffman, 2007, p. 8). These two conflicts can undoubtedly be classified as wars and hence these two descriptions incorporate only the military domain – different tactics and strategy used in warfare, from conventional to different kinds of irregular methods. Considering that lately Russia has been accused of waging hybrid warfare even against European Union (Holmes, 2015; The Baltic Times, 2016), it is clear that to date this definition has evolved much further from the original.

What NATO calls *hybrid warfare* today is more accurately defined as a *full spectrum conflict*, encompassing not only military, but also political, economic, technological, informational and other domains. The conflict in Ukraine, to which NATO refers as *hybrid warfare*, has arguably been based on a concept of *new generation warfare* mostly attributed to general Gerasimov, the Chief of the General Staff of the Russian Federation (Racz, 2015, p. 36). According to this concept, open warfare is rarely thought (as events in Crimea proved) and non-military methods are preferred (*Ibid.*). As the situation in Ukraine has proved to be difficult to be indisputably defined as a *war* (at least formally and legally, which is exactly what Gerasimov's theory foresees), the term *full-spectrum conflict* proposed by Jonsson and Seely (2015, p. 2) could be used to provide more clarity. In essence all of these terms encompass the same comprehensive approach (understandably, because they are all used to describe the same events), while the latter puts more emphasis on *full-spectrum* versus the

emphasis on *warfare* in both the NATO's and Russia's definition. However, for the purposes of achieving coherence between this essay and the references herein used, only the definitions *hybrid warfare* and *new generation warfare* will be used (as synonyms).

At first glance the *new generation warfare concept* is similar to NATO's *comprehensive approach*; however there are two fundamental differences between these, which give the former an advantage over the latter. Both NATO's and Russia's concepts highlight the importance of other sources of power besides military. According to Allied Joint Doctrine (NSA, 2010, pp. 1-2–1-3) the essential instruments of NATO's strategy are military, diplomatic, economic, and information instruments, additionally it stresses the utility of states' and non-governmental organisations' civil capabilities. Russia's *new generation warfare* concept also lists almost identical domains (diplomatic, economic, political, military) (Racz, 2015, p. 36). The first thing that separates these concepts is their respective purpose. The concept of comprehensive approach arose from the experiences in the Balkans and Afghanistan and was therefore devised to contribute to the resolution of an already existing crisis (Rotmann, 2010, p. 2). The *new generation warfare concept* however aims at creating one, discussing the ways an aggressor could overcome its intended victim (Chekinov and Bogdanov, 2013, p. 13). Therefore it also includes more aggressive measures, some of which clearly cross the line between legal and illegal actions (active use of asymmetric warfare, including committing terrorist acts and employing mercenaries) (*Ibid.*, p. 20). The second major difference derives from the different command and control structures, influencing the practical application of these concepts. Due to a more streamlined and effective command and control structure of Russia, all actions between command levels, state institutions, services and armed forces' components can be effectively synchronised. Lately this capability was further enhanced by the establishment of Armed Forces Central Command Centre, which enables to coordinate the activities of not only military forces, but also other security institutions (Rogoway, 2015). NATO as a collective alliance in contrast, requires agreed consensus, and relies on cooperating and coordinating with its members and other agencies and organisations, which constrains the level of success (NSA, 2010, pp. 1-2; Rotmann, 2010, pp. 3–4).

Based on theoretical foundations and observed actions in Ukraine, Russia's *new generation warfare* can be divided into two prominent phases – preparations for and attack. Referring to the work of Chekinov and Bogdanov, Janis Berzins (2014, p. 6) divides new generation warfare into 8 phases starting with non-military asymmetric warfare and concluding with the final elimination (mopping up) of any resisting armed units. Observing the actual events during the conflict in Ukraine, Andreas Racz however divides it to 9 sections, grouped to 3 main phases: preparation, attack and stabilisation (2015, pp. 58–67). Comparing these two approaches by looking at the actions taken in each phase (Berzins) or section (Racz), one can conclude that despite the different naming and theoretical division Berzins' phases largely coincide with the preparation and attack phases of Racz. In fact, Chekinov and Bogdanov acknowledge the need for preparations (creating favourable settings) but do not clearly distinguish the line between these and the actual attack itself (2013, pp. 19–23). The stabilisation phase however is altogether excluded in the work of Chekinov and Bogdanov. Similarly, the latter will not be discussed in this essay, since it only follows the successful completion of previous phases and therefore commences only if countering hybrid warfare proves to be unsuccessful in the first place. The essence of and possibilities of countering the preparation and attack phases of Russia's hybrid warfare will however be further explored.

The aim of the preparation phase is to identify the vulnerabilities of a possible target country and to create conditions for effectively taking advantage of these later in the attack phase. For the most part it includes using various economic, cultural, diplomatic and informational measures that are common in international relations. But it also encompasses establishing pro-Russian non-governmental organisations and media channels that are then used to fuel dissatisfaction, and even bribing politicians, government officials and armed forces' commanders who would be used to cripple the targets ability to resist from the inside. (Racz, 2015, pp. 58–59; Sherr, 2015, p. 26; Giles, 2015, p.42) Considering that according to the “new generation warfare” concept the state of conflict is considered to be permanent, rather than restricted in time (Berzins, 2014, p. 5), it is hardly surprising that these measures are constantly used by Russia in relations with its neighbours. Moreover, detecting these actions cannot provide the intended target definite warning about a planned hybrid attack, because ‘traditional acts of Russian diplomacy may function as preparations

for future hybrid warfare action, if the Kremlin decides so, while also serving their conventional, everyday purpose' (Razc, 2015, p. 58).

The main aim of the attack phase is to expel the central government from (at least) part(s) of the target country and create alternative political power centres, while denying Russia's involvement in the conflict to avoid the intervention of international community. The start of the attack phase is distinguished from the preparatory phase by the appearance of organized, armed violence, although the direct involvement of regular military units is avoided. Unmarked troops and (often armed) demonstrators try to block security and police forces, take over administration buildings and key media and civilian infrastructure. These actions are supported by massive information campaign with the aim of portraying the attackers as local citizens and flooding the local media with own propaganda to alienate the locals from central government. The information campaign is also directed to the international media, where it is supported by Russia's top level politicians, denying any involvement. At the same time the decision making cycle of central government and security forces is further disrupted by sabotage, cyber-attacks, electronic warfare and activation of bribed officials. Finally, if the central government has lost control over the territory, the so-called *separatists* could hold referendums for independence. (Razc, 2015, pp. 60–64) To avoid the escalation of the conflict into open conventional war, especially if an attack against a NATO member is considered (i.e. evade the activation of article V of the Atlantic Treaty), concealing Russia's involvement during the attack phase is of particular importance. This is well illustrated by the fact that president Putin himself played an important part of the denial effort during the hybrid attack against Ukraine (Shuster, 2015).

It is important to notice however, that for successful accomplishment of hybrid warfare there must be several preconditions (vulnerable points to exploit) present in the target country. First of all, there should be dissatisfaction with the central government, which is persistent and preferably regionally concentrated. Secondly, there is a need for Russian-speaking minority to justify Russia's involvement in the rising conflict and provide operational advantages. Additionally, the victim's central power and its security structures must be too weak to avoid or resolve the disorder and chaos resulting from hostile demonstrations, subversions and information

warfare. (Racz, 2015, pp. 73–83) Unfortunately the presence of Russian-speaking minority does not only serve as a quasi-legitimate reason for invading its neighbours (as it was justified both in Georgia in 2008 and Crimea in 2014), but it also helps to build discontent with the central government, provided that the latter represents (or is perceived representing) different ethnic, religious or cultural group. Moreover, according to Racz's observations in Ukraine, in the absence of actual lasting disagreements this minority can be used to portray (by information operations) an internal confrontation that does not actually exist (*Ibid.*). One can conclude then, that the target country must at very least have a Russian minority and vulnerable governance and security structures to be vulnerable to a hybrid attack.

In addition to the vulnerabilities of the intended victim itself, there is also a need for further preconditions that the attacker must ensure. Firstly, Russia needs to have military superiority to deny the target's ability to conduct effective armed resistance (by concentrating regular troops near the border, thereby threatening to start also a conventional attack) against irregular attacks. Moreover, there might be the need to provide direct support to irregular fighters or even to escalate the conflict to full scale (that is, reverting to open employment of conventional forces), if previous measures proved to be unsuccessful. Secondly, there is a need for strong media presence both in the target country and international media. This enables to generate and escalate tensions between minorities and central government, as well as to provide an alternative narrative about the events to the international media. And finally, to conduct the attack phase of hybrid warfare, there must be sufficient logistical support either from already existing stockpile or via adequate supply lines from Russia to support the irregular fight. (Racz, 2015, pp. 73–83) Regarding the first two points, Russia would probably not have major difficulties to establish versus most of the countries it considers being in its sphere of influence. Ensuring logistical support however is more difficult, since it requires either already existing resources (e.g. permanent military bases) the ability to build these up during preparations (for example, some form of covert pre-stocking) or favourable conditions for establishing appropriate lines of communications (i.e. suitable geography) during the execution.

How can NATO counter the hybrid warfare threat from Russia?

Considering the prerequisites of successful hybrid warfare discussed above, one can identify that only certain NATO members – the three Baltic States – are prone to Russia's hybrid attack. First of all, only five NATO members (Norway, Estonia, Latvia, Lithuania and Poland) are neighbours to Russia, which would enable Russia to secure the necessary supply lines which are needed for the logistic support of the hybrid warfare's attack phase. Out of these five, the Baltic States are militarily the weakest, not reaching the military capabilities of Poland or Norway (not to mention Russia) even with their armed forces combined. Moreover, only the Baltic States have a substantial Russian minority, which could be used to heighten domestic tensions and justify Russia's intervention. Therefore, NATO's efforts to counter Russia's possibilities to employ its *new generation warfare* can be focused to a specific region. As a consequence, this essay will further explore this issue solely from the perspective of defending the Baltic States.

Resulting from the nature of hybrid warfare's preconditions, some of them (dissatisfaction with the central government, weak governance and Russian minority) must be addressed by the threatened countries themselves. Resolving any domestic dispute is clearly a national responsibility; interference with these matters falls not only outside the provisions of the Atlantic Treaty, but also violates the sovereignty of the respective nations. Similarly, strengthening governance and security institutions is up to nations themselves, although NATO can assist by providing military assistance. Nevertheless, this support is limited primarily to the military domain and does not cover legislative, anti-corruption, policing, integration or other issues. Finally, the presence of Russian minority is a fact that is not going to change in the foreseeable timeframe. While there are ways to mitigate the possibility for them to be used in a hybrid warfare campaign (for example, better integration to the local society, economic and social development to minimize dissatisfaction with central government), these measures are also up to the countries themselves to carry out.

Taking into account that the weak spots of NATO identified earlier are confined to a specific region, some of the Russia's hybrid warfare's prerequisites – namely military superiority and presence in international media – can and should be addressed by

NATO. Although military power is difficult to measure accurately, there is no question about the superiority of NATO's combined military might over Russia's (Bender, 2015; Karlin, 2015). Looking at the Baltic region however, the situation is radically different with Russia's unchallenged position of advantageous military presence. The only way for this to change (without reducing Russia's capabilities) would be to enhance NATO forces' presence or at least to develop the capability to increase this presence rapidly once the situation requires it¹. Similarly, the three Baltic states on their own cannot afford to counter Russia's capabilities in the international media. Considering the massive and so far also largely successful efforts of Russia's state-run media apparatus (Jonsson and Seely, 2015, p. 12; Freedom House, 2016), it would be a challenge even for larger states. Here the application of NATO's comprehensive approach, mobilising the full potential of its members' information operations capabilities, is needed to counter hostile messages and portray the victim's side of the story.

Considering the nature of Russia's tools used in the preparatory phase of hybrid warfare, the primary responsibility to counter these lies within national level. First of all, the obvious reason for this is that the article 3 of the North Atlantic Treaty explicitly requires nations to prepare for their own defence (NATO, 1949). Secondly, given the fact that NATO is a military alliance, all its members are free to exercise their independent economic, foreign and domestic policies. The latter includes also the crucial subjects of integration, anti-corruption and internal security, which not only fall out of the scope of NATO but are also considered strictly sovereign matters. Although the concept of comprehensive approach also includes diplomatic, economic, and information instruments, the coordinated employment of NATO members' respective instruments is only possible after a collective decision has been reached (NSA, 2010, pp. 1-2). That implies that for such a decision sufficient threat has to be recognised in the first place, both by the target nation itself and the other allies. And even when this happens, any countermeasures implemented within the

¹ That is, before the attack phase of hybrid warfare commences or at least in time to prevent an intervention by regular troops.

target country must be led by that nation's government to avoid (actual or perceived) violation of its sovereignty.

Looking at the attack phase of Russia's hybrid warfare, especially its underpinning conventional military threat, it is evident that the help of NATO allies is needed to defend the Baltic countries. The Baltic countries could probably be able to deal with the "local militia" and even a moderate number of special forces troops with the employment of police and voluntary military organisations. The territorial defence forces have similar roles in all of the three countries, encompassing also crisis response and cooperation with other internal security forces (Szymański, 2015). If needed, even regular troops could be employed in a state of emergency. However, once Russia's conventional military is concentrated to the border areas, or in the worst case used to intervene inside national borders of target countries as it was done in Eastern Ukraine, the victims' ability to resist will be severely restricted. In this regard, the author of this essay agrees with Samuel Charap's otherwise incomplete² understanding of Russia's hybrid warfare: '...it could not sustain such an operation without employing its regular military...' (Charap, 2015, p. 55). Therefore, the primary purpose of NATO's assistance would be to deny Russia's ability to fix the defenders' freedom of action by (threatening of) employing its regular troops. Arguably, even the stationing of a small number of allied troops (as it is today) would effectively serve as a *tripwire*, initiating allied response if these were to be attacked (Kacprzyk, 2014, p. 7; Rogers and Martinescu, 2015, p. 19). Following the concept of new generation warfare however, the first targets would be the governmental institutions and internal security forces, while direct and overt fighting with regular units is avoided. Stepping on the *tripwire* would most likely be avoided by refraining from kinetic attacks.

² Charap (2015, pp. 54–55) considers only the employment of special forces, "rebels", propaganda, cyber warfare etc. as part of *hybrid tactics*, and detaches the usage of conventional military capabilities from the concept. Although the theoretical backgrounds used in this essay include the latter as well, the notion of the significance of conventional military power is agreed on the both sides of this argument.

Therefore it can be stated that to diminish Russia's ability to conduct hybrid warfare in the Baltic countries, NATO needs to establish a (clever) balance of military power in the region, thus removing a major precondition for successful *new generation warfare*. Although it is not conceivable to match Russia's military presence in the Baltic region by sheer numbers of soldiers and major equipment, robust and modern capabilities are needed to complement the Baltic militaries instead of *tripwires*. NATO should consider providing prioritised critical capabilities (to minimise or protect currently existing critical vulnerabilities) to enhance the capability to conduct joint and combined operations against an aggressor. For example, the ability to achieve air superiority and sea control (or even favourable air situation and sea denial) is lacking. Some of these capabilities should be prepositioned to avoid the delay of their deployment during an emerging crisis (i.e. heavy land units, medium- or long-range air defence units, elements of command and control structure etc.), some could be stationed elsewhere (navy and air force units, information operations capabilities, etc.), provided that their deployment is assured to be timely. By selective prepositioning a heavy military build-up and thus raising tensions could be avoided or at least minimised. Alternately, providing assistance and modern equipment with affordable prices to the Baltic States themselves would also raise their initial defence capabilities, thus reducing the need for other allies to relocate their troops to the area.

The main challenge for diminishing the possibility of the Baltic states being a victim to Russia's new generation warfare is finding the reasonable balance between (combined) national capabilities, mere *tripwires* and more substantial (and costly) military build-up, keeping in mind that future employment of hybrid warfare is likely to be different from previous ones. As a starting point, the Baltic militaries need to work more effectively together and create a common vision of their role in NATO's framework, followed by practical cooperation to enable this vision to realise. The response to a possible conflict must be discussed and coordinated starting from the political level to avoid creating confusion among the rest of the allies. Also, the vision of NATO's peacetime presence and employment during emerging crisis should be uniformly understood, enabling fair share of the burdens resulting from growing host nation responsibilities. Will the former be achieved at any satisfactory level or not, there still remains the tortuous task to define and agree on the exact level of allied

capabilities and mode of their employment required to ensure military balance in the region. The latter presents a complex challenge, especially in the light of McDermott's (2014) assertion that Russia does not actually have a set of fixed rules (that is, agreed and enforced doctrine) of new generation warfare, leaving ample room for further refinement and development for future engagements.

Whatever the shape and size of allied contribution to the Baltic States might be, in any case there is a need to conduct joint training and exercises between the host nations, NATO's readiness units and command structures. Since the territory of the Baltics is small, giving little opportunity to trade space for time, NATO's collective response to one or more of the countries being attacked needs to be fast. This means that the response must be planned and rehearsed, covering different contingency plans. It also means that the Baltic militaries themselves should be ready to integrate seamlessly to NATO command structure and be ready to cooperate in a joint and multinational environment. Such cooperation needs to be thoroughly rehearsed to work effectively, thus implying the need for regular exercises. Although the major exercises conducted currently involve allied troops as well, these are usually company (land forces) and squadron (air force) level, seldom involving bigger units or higher headquarters. Even at today's scale, allied troops training in the Baltics is valuable, providing opportunities to study the terrain and local weather conditions, demonstrate allied commitment, build personal relations and practice unit deployment to the region. Still, as much as the Baltic military forces need the ability to cooperate with other NATO allies on unit level (for example, with NATO air units to be able to receive air support), they must also and foremost be able to work jointly on operational and strategic levels (to help NATO to achieve air superiority in the first place). On the other hand, NATO also needs to enhance its responsiveness and agility in transitioning from crisis response to collective defence (Lindley-French, 2015, p. 3), in which multinational exercises including also the involvement of political decision makers could prove to be a valuable tool.

Conclusion

The essence of hybrid warfare is that it uses the full spectrum of power instruments in a coordinated manner, employing not only military, but also economic, diplomatic,

informational and other tools. As a result, the preparation phase of it is hardly distinguishable from regular Russian *realpolitik*, making early reaction difficult. The attack phase however has not been always fully successful, highlighting the need for specific preconditions to be established. While some of these preconditions (i.e. existence of unsatisfied Russian-speaking minority, quality of governance) can and should be addressed on national level and require long-term efforts, others (balance of conventional military power, presence in international media) can be diminished by collective efforts of NATO members. Moreover, a closer look at these preconditions accentuates that out of the NATO members only the Baltic region is susceptible to hybrid attacks. Following this conclusion NATO should not only continue its current efforts of providing *assurance measures* to this region, but take it to the next level. A more credible balance of military power should be established in the Baltics and its near proximity, reducing the currently existing capability gaps and integrating the national headquarters to common command and control structures. To realise this, it is not enough to merely position the required capabilities to Estonia, Latvia or Lithuania, in fact, some of the capabilities probably need not be constantly deployed; of equal importance is regular training and exercises to enhance the cooperation of host nations and allied troops not only on tactical level, but also the ability to fight effectively and jointly also on the operational and strategic levels. And in the end, however successful these efforts might be, one must still bear in mind the importance of being alert and receptive in predicting the future, to avoid being surprised on yet another occasion.

Bibliography:

Bender, J., 2015. *Ranked: the world's 20 strongest militaries*. [online] Available at: <http://www.businessinsider.com/these-are-the-worlds-20-strongest-militaries-ranked-2015-9> [Accessed 09 March 2016].

Berzinš, J., 2014. *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy*. Riga: National Defence Academy of Latvia.

Charap, S., 2015. The Ghost of Hybrid War. *Survival*, 57:6, pp. 51–58.

Chekinov, S. G. and Bogdanov, S. A., 2013. The Nature and Content of a New-Generation War. *Military Thought*, No. 4, 2013, pp. 12–23. [online] Available at: http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf [Accessed 11 January 2016].

Colby, E. and Solomon, J., 2015. Facing Russia: Conventional Defence and Deterrence in Europe. *Survival*, 57:6, pp. 21–50.

Douhet, G., 1921. *Command of the Air*. London: Coward McCann & Geoghegan.

Freedom House, 2016. *Freedom of the Press 2015. Russia*. [online] Available at: <https://freedomhouse.org/report/freedom-press/2015/russia> [Accessed 09 March 2016].

Giles, K., 2015. Russia's Toolkit. In: 2015. *The Russian Challenge*. London: Chatham House.

Hoffman, F. G., 2007. *Conflict in the 21st Century: the Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.

Holmes, L., 2015. *Russia plans a 'hybrid warfare' campaign aimed at destabilising Europe, says Bulgarian President*. [online] Available at: <http://www.independent.co.uk/news/world/europe/russia-plans-a-hybrid-warfare->

campaign-aimed-at-destabalising-europe-says-bulgarian-president-a6734981.html
[Accessed 03 February 2016].

Jonsson, O., Seely, R., 2015. Russian Full-Spectrum Conflict: An Appraisal After Ukraine. *The Journal of Slavic Military Studies*, 28(1), pp. 1–22.

Kacprzyk, A., 2014. *Deterring Russia after Ukraine: CEE Divided on the Future of NATO Policy*. Policy Paper no. 13 (96), July 2014. The Polish Institute of International Affairs.

Karlin, A. 2015. *Comprehensive Military Power: World's Top 10 Militaries of 2015*. [online] Available at: <http://www.unz.com/akarlin/top-10-militaries-2015/> [Accessed 09 March 2016].

Lindley-French, J., 2015. *NATO and New Ways of Warfare: Defeating Hybrid Threats*. NDC Conference Report, No. 03/15 – May 2015. Rome: NATO Defence College.

McDermott, R., 2014. *Myth and Reality – A Net Assessment of Russia's 'Hybrid Warfare' Strategy Since the Start of 2014*. [online] Available at: [http://www.jamestown.org/single/?tx_ttnews\[tt_news\]=42972&tx_ttnews\[backPid\]=7&cHash=26ffc0672bbe5ce4582138d3d2552e70#.VucXa1Jf2UI](http://www.jamestown.org/single/?tx_ttnews[tt_news]=42972&tx_ttnews[backPid]=7&cHash=26ffc0672bbe5ce4582138d3d2552e70#.VucXa1Jf2UI) [Accessed 14 March 2016].

NATO, 1949. The North Atlantic Treaty. *NATO homepage*. [online] Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/stock_publications/20120822_nato_treaty_en_light_2009.pdf [Accessed 29 October 2015].

NATO Standardization Agency (NSA), 2010. *AJP-01(D) Allied Joint Doctrine*. Brussels: NSA.

Nemeth, W. J., 2002. *Future War and Chechnya: A Case for Hybrid Warfare*. Monterey: Naval Postgraduate School.

Rácz, A., 2015. *Russia's Hybrid War in Ukraine*. Helsinki: The Finnish Institute of International Affairs.

Rogers, J. and Martinescu, A.L., 2015. *After Crimea. Time for a New British Geostrategy for Eastern Europe?* London: The Henry Jackson Society.

Rogoway, T., 2015. *Look Inside Putin's Massive New Military Command And Control Center*. [online] Available at: <http://foxtrotalpha.jalopnik.com/look-inside-putins-massive-new-military-command-and-con-1743399678> [Accessed 09 March 2016].

Rotmann, P., 2010. *Built on Shaky Ground: The Comprehensive Approach in Practice*. Research Paper No. 63, December 2010. Rome: NATO Defense College.

Sherr, J., 2015. A War of Narratives and Arms. In: 2015. *The Russian Challenge*. London: Chatham House.

Shuster, S., 2015. *Putin's Confessions on Crimea Expose Kremlin Media*. [online] Available at: <http://time.com/3752827/putin-media-kremlin-crimea-ukraine/> [Accessed 04 February 2016].

Stoicescu, K., 2015. *The Russian Threat to Security in the Baltic Sea Region*. [online] Available at: <http://www.icds.ee/publications/article/the-russian-threat-to-security-in-the-baltic-sea-region/> [Accessed 15 March 2016].

Szymański, P., 2015. *The Baltic states' Territorial Defence Forces in the face of hybrid threats*. [online] Available at: <http://www.osw.waw.pl/en/publikacje/osw-commentary/2015-03-20/baltic-states-territorial-defence-forces-face-hybrid-threats> [Accessed 09 March 2016].

The Baltic Times, 2016. *Ukrainian NSDC Secretary: Russia waging hybrid warfare on EU*. [online] Available at: http://www.baltictimes.com/ukrainian_nsdsc_secretary__russia_waging_hybrid_on_eu [Accessed 03 February 2016].

Vandiver, J., 2014. *SACEUR: Allies must prepare for Russia 'hybrid war'*. [online] Available at: <http://www.stripes.com/news/saceur-allies-must-prepare-for-russia-hybrid-war-1.301464> [Accessed 15 March 2016].

What is the significance of the emergence of the Wider North to Estonia?

MAJ Indrek Sarap

‘Like it or not, the Arctic is open for business ...’

Dr. Scott Borgerson, an Arctic expert (Borgerson, 2013, p. 78-79)

Introduction

The term ‘Arctic’ is derived from the Greek word *arktos*, which means ‘the bear’ and refers to the northern constellation of the Bear (Dunbar, 2016). Today, there are a number of ways and terms to describe the area that constitutes the Arctic. In the most straightforward geographical manner, the term refers to the Arctic Ocean, which is centred roughly at the North Pole and is the smallest of the world’s oceans (Ostenso, 2016). It is often also defined as the Arctic Circle, a region that lies above the 66° 32" north latitude and where are six month long winter and summer solstices of long-lasting darkness and light (National Snow and Ice Data Centre, 2016); or the area that lies north of the tree-line, where the landscape is frozen and features only shrubs and lichens (National Snow and Ice Data Centre, 2016 and Dunbar, 2016). In comparison with the previously mentioned definitions, the terms ‘High North’ and ‘Wider North’ are frequently used to describe the Arctic within the context of geopolitics. High North refers to the limited space of European Arctic, which consists of those parts of Nordic countries and Russia that are situated by the Norwegian Sea, Barents Sea and the southern parts of the Polar Sea (The GeoPolitics in the High North, n.d.). The Wider North, on the other hand, is a term that includes not only the Arctic itself, but also the adjacent North-Atlantic, Northwest Pacific, Nordic and Baltic regions (Rogers, 2012, p. 42).

Without any regard to linguistics and terminology, climate change is affecting the Arctic more than any other region in the world. The sea ice and the permafrost of the world’s most northern region are melting rapidly and the area is likely to become unrecognisable in a few decades (Scudellari, 2013). What is more, changes in the Arctic are expected to have a severe impact on the rest of the world. James Holmes,

a professor at the United States Naval War College, has proposed that the opening of the Arctic will entail the most significant transformation of geopolitics since the opening of the Panama Canal and predicted the Arctic to become 'the Mediterranean of the 21st century' (Holmes, 2012). This notion follows the logic that alterations in transport routes have brought about shifts in the balance of economic and political power (Blunden, 2012, p. 117). In addition, it creates a new dimension to a historical confrontation – four out of five littoral states of the Arctic Ocean are NATO members while the fifth is Russia (Tuohy ed, 2014, p. 2). Estonia is not an Arctic country with its northernmost point, the Vaindloo Island, being about six degrees below the Arctic Circle. Yet, the opening of the region will influence the small Baltic country both directly and indirectly (Tuohy ed, 2014, p.45-53). Accordingly, this essay argues that the Arctic will attain global and regional importance in the next decades, entailing potential risks and opportunities for Estonia. It starts with a short overview of the Arctic region, a summary of the implications of climate change and an outline of the areas of regional cooperation and disagreement. The second section attempts to look into the future of the region and sketches four possible future outlooks with narratives of how the geopolitics of the Wider North might unfold. The third and the final section provides insights to the risks and the opportunities that the opening of the Arctic will have for Estonia.

Opening of the Arctic

The Arctic will attain global importance in the next decades due to melting sea ice. To understand the reasons behind this conversion, the scene of the transformation must be considered. The Arctic Circle entails more than 21 million square kilometres or about 6 percent of the Earth's surface, out of which merely a little more than 1/3 or 8 million square kilometres is onshore (United States Geological Survey, 2008, p. 1). The countries surrounding this ocean can be divided into two. Firstly, there are the littoral states Canada, Denmark (through Greenland), Norway, Russia and the United States, which all have coastlines in the Arctic Ocean. Secondly, there are the non-littoral Arctic states Finland, Sweden and Iceland, which do not have a coastline in the Arctic Ocean, but which nevertheless have territories within the Arctic Circle. During the last 100 years, the average temperature in the Arctic has raised more than

twice the global average (Tuohy ed, 2014, p. 41), making it the scene for the most rapid and severe climate change in the world (Bert, 2012, p. 6). A ground-breaking study conducted by the United States National Aeronautics and Space Administration (NASA) showed that since the late 1970s the Arctic has witnessed a roughly 1.2°C increase in temperatures and an approximately 9 percent decrease of perennial ice each decade (NASA, 2003). The melting of perennial ice deteriorates the existing state of affairs even further, since the released water absorbs the sun and accelerates the melting process (Bert, 2012, p. 6). As a consequence, it is possible that the Arctic will be seasonally ice free by the 2030s (Bert, 2012, p. 6) and the perennial ice will disappear completely during this century (NASA, 2003).

A positive outcome of climate change in the Arctic is that the region opens up for exploitation. According to a survey conducted by the scientists of the United States Geological Survey, the Arctic Circle may hold roughly 90 billion barrels of oil, 1,669 trillion cubic feet of natural gas and 44 billion barrels of natural gas liquid (United States Geological Survey, 2008, p. 4), which is estimated to amount to 15 percent of the world's undiscovered oil reserves and 30 percent of natural gas reserves (Papp, 2012, p. 2). The region also holds vast amounts of minerals such as zinc, nickel, palladium, platinum, cobalt, copper, iron ore and many others (Bert, 2012, p. 7 and Tuohy ed, 2014, p. 30-31). Apart from the energy sources and minerals, the fisheries of the Arctic Ocean are an often overlooked resource of the region (Tuohy ed, 2014, p. 28). Today, the United States' portion of the Arctic produces around 1.8 million metric tonnes of seafood annually, worth more than US \$1.3 billion (Papp, 2012); while seafood counts for 85 percent of Greenland's and 40 percent of Iceland's total exports (Tuohy ed, 2014, p. 32). However, the extracting of natural resources from the Arctic is likely to remain an expensive venture and therefore the largest benefit of the melting sea ice might be the opening of new shipping routes (Young, 2011, p. 187-188). The Northern Sea Route (NSR) (see figure 1) is a roughly 2,600 nautical mile long corridor, which could shorten the route between East Asia and Western Europe from 13,000 to 8,000 miles, cutting the travel time by 10-15 days³ (Bert,

³ In 2009, two ships traveling from Ulsan in South Korea to Rotterdam in the Netherlands by NSR cut down the distance by 3,000 nautical miles and cost by US \$300,000 (Blunden, 2012, p. 118).

2012, p. 8). Likewise, the Northwest Passage (NWP) will offer an alternative corridor to traveling from East Asia to Northern America, shortening the distance by 7,000

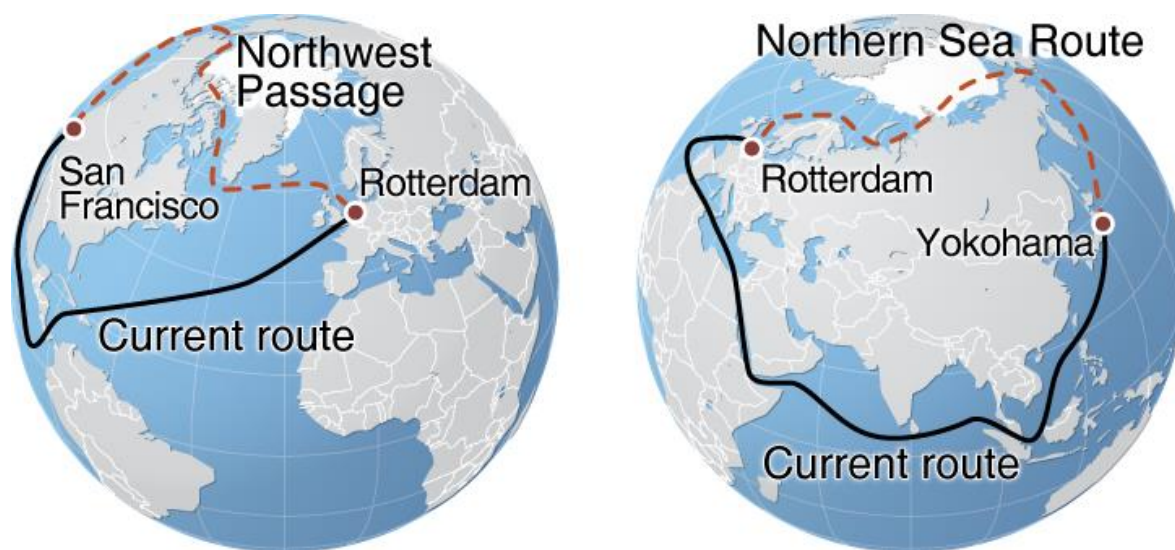


Figure 1. Northern Sea Route and the Northwest Passage compared with currently used shipping routes.

Source: (Ahlenius, 2007).

nautical miles and travel time by 14 days in comparison with the route through the Panama Canal (Robinson, 2015). Although the NSR is currently suitable for shipping only around 50 days per year and the NWP was not used for commercial purposes from 1969 to 2013, both routes are becoming more navigable every year with the rising temperatures and melting ice (Tuohy ed, 2014, p. 33-34 and Nielsen, 2014).⁴

The Arctic has been occupied in peaceful cooperation so far. First of all, this constructive cooperation has a solid foundation in the legal regime regulating the region. Since the Arctic is essentially an ocean, its utilisation is regulated in the United Nations Convention on the Law of Sea (UNCLOS),⁵ several other treaties and common maritime law. The littoral Arctic states have adopted the position that no special rule system (like one for Antarctica) is required for the region since the

⁴ In August 2008 both the NSR and the NWP were open for the first time in recorded history (Young, 2011, p. 187-188).

⁵ UNCLOS divides the Arctic Ocean into territorial sea, exclusive economic zones and high sea (United Nations (UN), 1982).

general regime for seas and oceans is sufficient. This position was put forward in 2008 in the Ilulissat Declaration by the foreign ministers of the five littoral states (Osica, 2010, p. 13-14). Secondly, the Arctic has generated a number of regional organisations and cooperation networks. The most prominent of them is the Arctic Council, which was established in 1996 by the eight littoral and non-littoral Arctic states. Today, the council has become the most important and visible international organisation dealing with the Arctic. It mostly focuses on the issues of environment, sustainable development, scientific research; but also maritime security and preparedness for emergencies, while specifically excluding from its agenda hard security matters such as border disputes and continental shelves claims. In addition to the Arctic states, the United Kingdom, France, Germany, Netherlands, Poland, Spain, Italy, China, India, Japan, South Korea and Singapore have joined the Arctic Council as permanent observers. Furthermore, the European Union as an intergovernmental organisation has also applied for permanent observer status, but its admission is on hold for now due to opposition from Canada and Russia (Tuohy ed, 2014, p. 20 and p. 25).

Nevertheless, there are some sources of tension which might lead to great power competition and confrontation (Holmes, 2012). One of the issues dividing the Arctic states is the dispute over the extended continental shelves. UNCLOS puts forward the idea of a continental shelf (United Nations (UN), 1982), which can extend a country's control well beyond the standard 200 nautical miles limit (Tuohy ed, 2014, p. 36). This is the case for the Lomonosov Ridge, which is a continental shelf that has been claimed by numerous Arctic states (Tuohy ed, 2014, p. 37-38).⁶ Another source of tension is the question whether the NSR and NWP are territorial waters or international straits.⁷ The European Union, the United States, China and many others

⁶Parts of the Lomonosov Ridge have been claimed by Russia in 2001 (Oliphant, 2014), Canada in 2013 (Government of Canada, 2013) and Denmark in 2014, while Norway is expected to submit a claim in the near future (Oliphant, 2014).

⁷ According to the UNCLOS, all ships enjoy the right of transit passage through straits which are used for international navigation even if it lies within the 12 nautical mile limit of territorial seas (UN, 1982, pp. 36-37).

consider the vessels traveling both routes to enjoy the right of transit passage, while Russia and Canada consider parts of them as their territorial waters (Blunden, 2012, p. 129).⁸ However, all the littoral Arctic states are foremost interested in protecting the sovereignty of their already existing territories and thereafter engaged in expanding their spheres of influence (Osica, 2010, p. 12). In fact, there has not been a military build-up in the Arctic, although there have been some displays of sovereignty through military presence and exercises (Bert, 2012, p. 11). For instance, Russia activated a new Arctic Joint Strategic Command in late 2014 (Jones, 2014) and conducted a relatively large exercise involving 38,000 troops, 110 aircraft, 41 ships, and 15 submarines soon after in early 2015 (McLaughlin, 2015). Yet, this should not be seen as confrontation, but rather as a measure to defend its national interests (Peters, 2015) in a region which is central to its economy (Ministry of Defence UK, 2014, p. 159 and Osica, 2010, p. 22).

Future of the Arctic

Scholars and experts have been unable to agree on what the future will bring for the Arctic. A recent study by the International Centre for Defence and Security (ICDS) in Tallinn suggests that the conflicting interests in the Arctic region greatly outnumber common interests (Tuohy ed, 2014, p. 28). In contrast to gloomy forecasts, the United Kingdom Ministry of Defence considers a large scale confrontation in the Arctic unlikely (Ministry of Defence UK, 2014, p. 155). Lack of consensus on the future of the Arctic is not surprising, since accurate point prediction in international relations is virtually impossible due to large number of different forces and variables which all interact with each other in multiple and random ways. Consequently, instead of predicting the exact future, many scholars recommend using forward reasoning to develop multiple possible futures. Based on the assumption that tomorrow is unpredictable, these outlooks map causes and trends, providing alternative views on how the future might unfold and being thereby a foundation for

⁸ Russia is already exercising *de facto* control over the NSR by demanding that all ships navigating it seek permission from Russian authorities and also utilise exclusively the Russian nuclear icebreaker services (Tuohy ed, 2014, p. 10).

policy- and decision-making (Bernstein, Lebow, Stein and Weber, 2000, pp. 48-70). Named as scenario planning, this method was developed in the 1970s (Bradwell, Johar, Maguire, and Miner, n.d., p. 14) and has been successfully used by corporations such as Royal Dutch/Shell, Xerox and American Express to name just a few (Ogilvy, 2015).

The details of scenario planning vary among different authors (Ogilvy, 2015 and Edwards, n.d., p. 2-6), but basic principles remain the same (Wilkinson and Kupers, 2013). Firstly, the focal issue that the outlooks need to address has to be defined (Ogilvy, 2015). In this study, they have to describe the Arctic in a 20-30 year perspective of long term planning, or up to the year 2045. Secondly, all the possible trends have to be considered and ranked according to their importance and uncertainty as driving forces (Edwards, n.d., p. 3-4). The most important trend for the Arctic is climate change and the most uncertain trend is geopolitical stability. Accordingly, these two driving forces can be depicted in a matrix (see figure 2) to establish the foundation of the outlooks. Thirdly, the driving forces must be explored and described, especially interaction between them and their likely resolution (Edwards, n.d., p. 4-5). The most important trend for the future of the Arctic, climate change, is difficult to predict. According to the Intergovernmental Panel on Climate Change's latest report, the Arctic ice will continue melting and it will become seasonally ice free as early as 2037 or as late as 2100 (Kirtman et al, 2013, p.995). The most uncertain trend, geopolitical stability, is even more difficult to predict. The world economy is projected to double by 2037 and nearly triple by 2050 with China, India and the United States becoming the undisputed economic giants (PricewaterhouseCoopers International Limited, 2015, p. 1-5). In terms of stability in the Arctic, Russia is likely to be both critical and a wild card (Kaljurand et al, 2012, p. 13 and Ministry of Defence UK, 2014, p. 159). With a rapidly decreasing population (UN, 2015, p. 21) and an undiversified economy (PricewaterhouseCoopers International Limited, 2015, p. 1), it is likely to find itself in a position of disadvantage compared to her Asian and European neighbours (Gould-Davies, 2016, p.23-24). Moreover, under the rule of President Vladimir Putin, Russia is increasingly confrontational with the Western states (Forbrig, 2015, p.1), which in turn might lead into a confrontation in the Arctic, where all other littoral states are members of either

the European Union or NATO. Finally, after exploring the trends, four distinct outlook stories describing the possible futures can be developed (Edwards, n.d., p. 5-6).

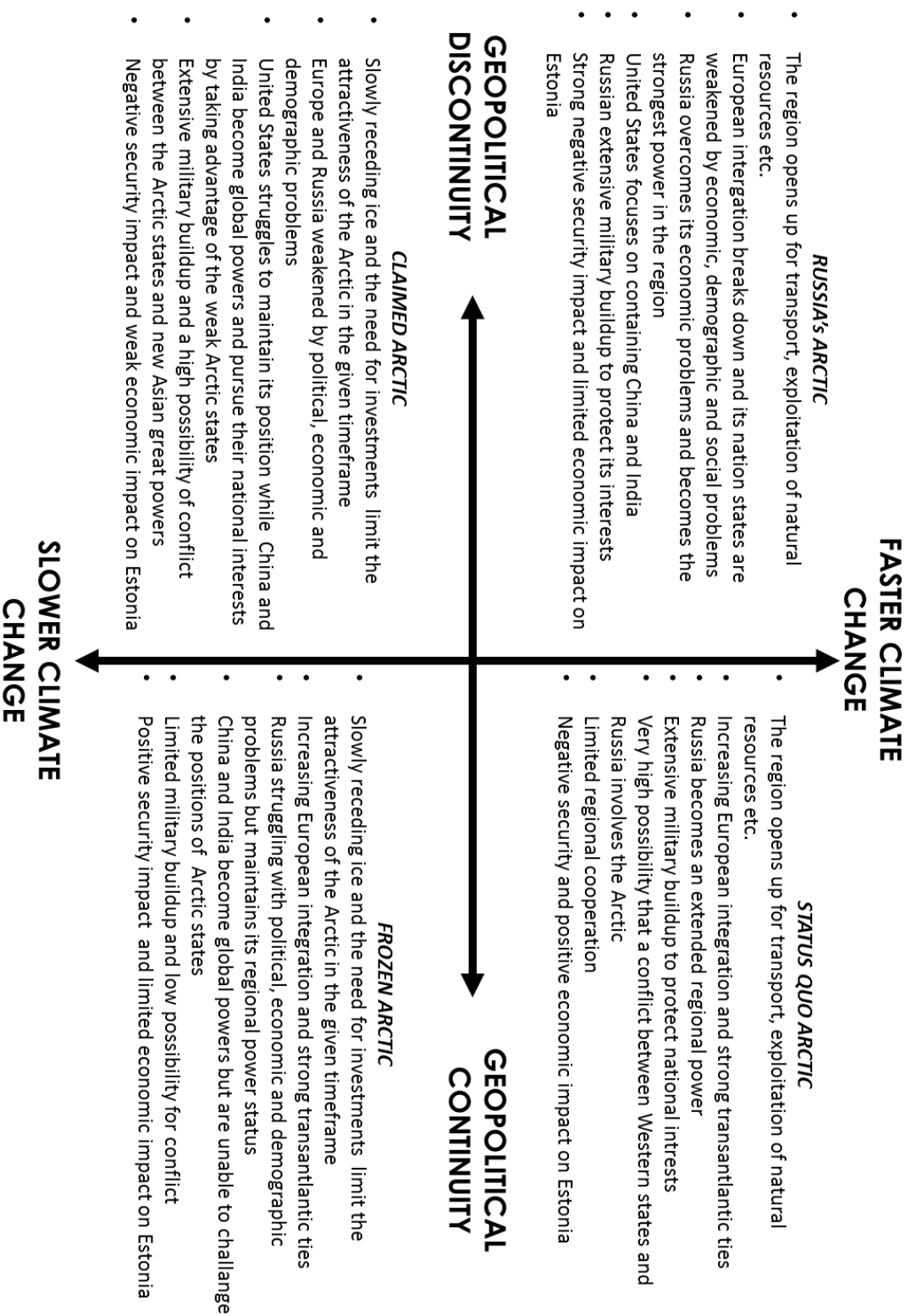


Figure 2. Possible future outlooks for the Arctic.
Source: Author's own.

Fast climate change can lead into two diverse outcomes. In the *Status Quo Arctic* outlook, the rapidly melting sea ice allows the exploitation of the region's massive natural resources while the seasonally ice free Arctic Ocean enables the establishment of new sea routes between Asia, Europe and Northern America. This greatly benefits Russia, which uses energy revenues to diversify its economy and capitalises on its relative political and military strengths to become an extended regional power. However, it is unable to compete with the vastly greater economies of China, India, United States and consolidated Europe. Realising that unity is crucial for maintaining its relative position in the twenty-first century, Europe is able to integrate into a unified entity which is further strengthened by strong transatlantic ties with the United States and Canada. The Arctic plays a significant role in the Western-Russian relations, with Russia seeing the region as its strategic resource base constantly threatened by European and North American interests. This leads into a military build-up and confrontation, while cooperation takes place only in insignificant areas like maritime security and environmental protection; and important issues like territorial disputes and control of transportation routes are solved within the framework of overall Western-Russian relations.

Conversely, in the other outlook involving rapid climate change, *Russia's Arctic*, although the region opens up for exploitation similarly, the geopolitical dynamic is different. European nation states are overwhelmed by economic, demographic and social problems after contradicting interests and competition for leadership ends the European integration project. The situation is further amplified by the loosening of transatlantic ties, after the United States focuses on the Pacific to balance the influence of China, India and Indonesia. Russia benefits from the disintegration of Europe and the American pivot; and turns into by far the strongest power in the Arctic. Due to its military and economic dominance in the region, all other Arctic states avoid any kind of confrontation and follow a policy of appeasement.

On the other hand, the future of the Arctic might evolve completely differently if climate change is less rapid. In the *Frozen Arctic* outlook, the sea ice continues to melt in slower pace so that the ocean is ice free only occasionally in the 2030s and 2040s. As a result, the Arctic remains relatively unattractive due to the cost of extracting resources and the need for extensive investments in infrastructure. This amplifies Russian economic and social problems, which seem especially severe

compared to the prosperity of the integrated Europe and Northern America. Territorial disputes are solved within the framework of UNCLOS and cooperation in the region includes fishing, tourism, environmental protection and research. Furthermore, in this outlook, there is very limited military build-up mostly focused on providing search and rescue capabilities. Finally, in the last outlook, *Claimed Arctic*, once again the region opens up slowly. European states and Russia are weak and entwined in numerous political, social and demographic problems. The United States loses its superpower status and is struggling to maintain its relative position. This opens up a window of opportunity for the new great powers China and India, which use their economic and military power to gain a foothold in the Arctic. It begins with a political initiative to create a special legal regime which allows non-Arctic states to benefit out of the vast resources of the region similarly to the littoral Arctic states. However, it soon evolves into an extensive military build-up which the feeble European states and Russia are unable to match. After a few local clashes, both Russia and the European Arctic states are forced to make concessions and allow additional states to benefit from the riches of the Arctic.

Significance to Estonia

Like the states described in the previous outlooks, the Arctic holds both risks and opportunities for Estonia as well. Estonians have been involved in the Arctic in various ways for a long time. To start with, research activities began with Baltic German explorers like Wrangell, Middendorf and Toll in the nineteenth century; reached their peak during the Soviet rule and contribute significantly today (Vaikmäe, n.d.). Just recently, Estonian universities had up to 100 people directly involved in Polar research; studying fundamentals and developing up-to-date and relevant technology (Vaikmäe, n.d.), such as a practical solution for accurate sea ice forecasting (Delfi, 2016). Secondly, since 1930, Estonia is a signatory of the Svalbard Treaty (Välisministeerium, 2015), which grants it the right to engage in economic activities in the Norwegian archipelago in the Arctic Ocean (Tuohy ed, 2014, p. 39,45). Unfortunately, the only recent Estonian economic activity in the Arctic has been ice-breaking (Kaukvere, 2014) and fishing, with mere four ships producing 6 percent of the national annual catch (Rand, 2011 and Tuohy ed, 2014, p. 47-48).

Nevertheless, Estonians are aware of their past ties with the region and have started to think systematically about strengthening the connection during the past decade. In 2012, a report by the ICDS mentioned the emergence of the High North as a trend that affects both the global and the Baltic Sea security environment (Kaljurand et al, 2012, p. 12-13 and 64). In 2014, the same think-tank published a study focusing exclusively on the Arctic and providing practical conclusions for Estonian decision-makers (Tuohy ed, 2014, p. 2-3). Among other things, the researchers recommended Estonia to develop a long-term Arctic strategy with the aim of furthering its interest in the region (Tuohy ed, 2014, p. 54-56). To understand the underpinning of this proposed strategy, it is appropriate to examine what might be the significance of the Arctic to Estonia in the next decades.

The emergence of the Wider North entails severe security risks and some political opportunities for Estonia. To start with, the security situation in the High North will influence the state of affairs in the Baltic Sea region (Osica, 2010, p. 28). All outlooks except *Russia's Arctic*, foresee Russia using the Baltic Sea Region to achieve gains in the Arctic and vice versa (see figure 3). This *modus operandi* was demonstrated last autumn, when Russia's direct involvement in the Syrian crisis served among other things the purpose of drawing attention away from the Ukrainian crisis and finding ways to relieve the Western imposed sanctions (Nye, 2016). Secondly, as most outlooks show, a military build-up in the Arctic is likely to draw away Western troops from the Baltic Sea Region, creating a security vacuum and leaving Russia with more freedom for manoeuvre (Kaljurand et al, 2012, p. 13). Finally, as is the case in the *Status Quo* outlook, a crisis in the Arctic could have a spill over effect in the Baltics (Tuohy ed, 2014, p. 49). Obviously, a large scale confrontation between Russia and NATO in the Arctic would quickly involve the latter's weakest link, the Baltic countries (Forbrig, 2015, p. 6). On the other hand, political involvement in the region entails several opportunities for Estonia. As its long time Foreign Minister, Urmas Paet, put it recently, Estonia is the closest country to the Arctic that is not a member of the Arctic Council (Kuul, 2015). Becoming actively engaged in the region would potentially enhance the bi- and multilateral relationships with the United States, the Nordic countries and maybe Russia; while supporting the European Union's aspirations towards the High North. Estonia's current government has wisely agreed to apply for the observer status in the Arctic Council during this year (Eesti

Reformierakond, Sotsiaaldemokraatlik Erakond and Erakond Isamaa ja Res Publica Liit, 2015, p. 12) and the intention has been welcomed by the High Representative of the European Union for Foreign Affairs and Security Policy (Kuul, 2015). As the two outlooks with strong European integration and transatlantic ties, *Status Quo Arctic* and *Frozen Arctic*, demonstrate, advocating enhanced EU and NATO involvement in the Wider North could further strengthen Estonia's position in the region and help support achieving its aims.

OUTLOOKS

RISKS AND OPPORTUNITIES FOR ESTONIA

	RUSSIA'S ARCTIC	STATUS QUO ARCTIC	CLAIMED ARCTIC	FROZEN ARCTIC
MILITARY	<u>Risk:</u> Russia could use its military power to influence Estonia or attack it.	<u>Risk:</u> Russia could use the Baltic Sea Region to achieve gains in the Arctic and vice versa.	No further risks or opportunities.	
		<u>Risk:</u> A conflict in the Arctic could enlarge to include the Baltic Sea Region as well.		
POLITICAL	<u>Risk:</u> Military buildup in the Arctic could draw away Western forces from the Baltic Sea Region.	<u>Opportunity:</u> Supported by its scientific interests and competence, Estonia can become actively engaged in the region through different regional cooperation frameworks and obtain political credit.		
	<u>Risk:</u> Russia could use its position of strength in the Arctic to bargain for concessions in the Baltic Sea Region.			
	<u>Risk:</u> Russia could limit the participation of non-Arctic nations in the region.	<u>Opportunity:</u> Estonia could further its interests in the Arctic by/through advocating for NATO and EU active involvement in the region.	No further risks or opportunities.	<u>Opportunity:</u> Estonia could further its interests in the Arctic by/through advocating for NATO and EU active involvement in the region.
ECONOMIC	<u>Opportunity:</u> Estonia could benefit from becoming a transit corridor both for the resources obtained from the Arctic and transported through the Arctic.		No further risks or opportunities.	
SCIENTIFIC	<u>Opportunity:</u> Estonian enterprises could become engaged in the region. The most likely sectors include shipbuilding, fishing and icebreaking; however, information technology, clean technologies and coal mining offer opportunities as well.			<u>Opportunity:</u> Estonian Polar research community could increasingly participate in the Arctic research as the region opens up and draws investments.
	<u>Opportunity:</u> Estonian Polar research community could increasingly participate in the Arctic research as the region opens up and draws investments.			

Figure 3. Risks and opportunities for Estonia.
Source: Author's own and (Tuohy ed, 2014).

Nevertheless, the most important opportunities presented by the emergence of the Wider North are scientific and economic. Estonia's small but experienced Arctic research community consists of about 45 people and 11 institutions; and has know-how comparable to the Nordic countries (Tuohy ed, 2014, p. 48). Upholding and enhancing this competency serves the interests of science⁹, while helping to validate Estonian involvement in the region. With regard to the economic dimension, the potential gains are even more significant. Firstly, as shown in *Russia's Arctic and Status Quo Arctic* outlooks, as fast climate change makes the Arctic Ocean navigable, a large portion of maritime shipping between Europe and Asia is expected to switch to the NSR (Blunden, 2012, p.115). This presents a unique opportunity for the Baltic Sea Region. Instead of sailing all the way around the Scandinavian Peninsula, cargo could be unloaded in one of the Barents Sea ports and transported to Europe either by rail or through the White Sea Canal (see figure 4). An example of this is the Finnish led Arctic Corridor project (Tuohy ed, 2014, p. 50), which aims to build a railway connection from the Norwegian port town of Kirkenes to the Finnish town of Rovaniemi and further on to Central-Europe. The project would benefit the whole region by connecting the Arctic Ocean with the Baltic Sea region and the rest of the Europe (Arctic Corridor, n.d., p. 2-7) and turn Estonia into an important transport hub. The impact of the project would be further magnified once Estonia and Finland have been connected through a proposed tunnel running beneath the Gulf of Finland (Karjus, 2015); and with Central and Western Europe by the Rail Baltic railway connection (Ministry of Economic Affairs and Communications; and Technical Regulatory Authority, 2015). Secondly, opening of the Arctic requires large investments in infrastructure and services; which could be provided by Estonian enterprises. Namely, there are currently three Estonian shipyards capable of constructing vessels suitable for the Arctic Ocean (Tuohy ed, 2014, p. 46) and able to produce to the Arctic market as successfully as their Finnish counterparts.¹⁰

⁹ For more information on Estonian Polar Research see professor Rein Vaikmäe's overview at EU-PolarNet (available at <http://www.eu-polar.net/eu/european-polar-science/europe-and-the-polar-regions/estonian-polar-research.html>).

¹⁰ Finnish shipbuilding industry has a long history of building vessels for the Arctic (Blunden, 2012, p. 122). The latest proof of their competence is the construction of



Figure 4. Possible future transportation routes connecting the Northern Sea Route with Central Europe via the Baltic Sea Region.

Source: Map courtesy of Google Maps. Graphics Author's own based on: (Northern Sea Route Information Office, n.d.; Arctic Corridor, n.d., p. 2-7; Rogers, 2012; and AECOM Limited, 2011).

Conclusion

The Arctic is witnessing the rise in temperatures twice the speed than most parts of the globe and could become seasonally ice free as early as the 2030s. The receding sea ice enables access to the vast deposits of oil, natural gas and minerals; not to mention the large fisheries of the region. Another positive outcome of the climate

the world's first icebreaker operating on liquefied natural gas and having almost a zero emission (Arola, 2015).

change is the opening of new shipping routes, namely the NSR and the NWP, which are expected to considerably shorten the travelling distance and time between East Asia and Western Europe, as well as between East Asia and Northern America. Although a sound legal regime and regional initiatives have led to constructive cooperation on the matters of environmental protection, sustainable development, scientific research and maritime security; there are still a number of unsolved disputes between the Arctic states with regards to the claims for extended continental shelves and control of sea routes. Under these circumstances, it is not surprising, that scholars and experts are unable to agree on the future of the region. Nonetheless, instead of predicting the exact future, this essay uses forward reasoning through scenario planning to shed light on the upcoming thirty years in the Wider North. Exploring the trends of climate change and political stability, the future outlooks *Status Quo Arctic*, *Russia's Arctic*, *Frozen Arctic* and *Claimed Arctic* describe distinct different dynamics that are likely to develop in the Arctic and their impact on Estonia.

Security is Estonia's most significant risk with regards to the opening of the Wider North due to the fact that the security environments of the Arctic and the Baltic Sea Region will be closely connected. It is likely that Russia will utilise the Baltics to further its interests in the Arctic and the other way around. Moreover, a confrontation in the Arctic is likely to have a spill over effect in the Baltic Sea Region. Still, there are remarkable opportunities for Estonia as well. Scientific research in the Arctic would contribute to the longstanding traditions of polar research and could be exploited for the purpose of becoming more actively involved in the region. This in turn would enhance Estonia's political credit within EU and strengthen relations with a number of Arctic and non-Arctic states. Furthermore, the opening of the Arctic also entails significant economic opportunities. Estonian enterprises could potentially profit from the investments made in the Arctic and regional infrastructure projects have the potential to turn Estonia into an important transport hub between the Arctic Ocean and Central Europe once the NSR has become regularly ice free. Nevertheless, at the moment, all of the previously mentioned considerations are merely risks and opportunities for Estonia. It will take a deliberate executive level decision to develop and implement a long-term national policy for the Arctic, thereby enabling the

mitigation of possible security risks and the transformation of different opportunities into gains achieved.

Bibliography

AECOM Limited, 2011. *Rail Baltica Final Report: Volume 1*. [online] Available at: [http://tja.ee/public/Raudtee/Rail Baltica Final Report Volume I 31 05 11 FINAL v2.pdf](http://tja.ee/public/Raudtee/Rail_Baltica_Final_Report_Volume_I_31_05_11_FINAL_v2.pdf) [Accessed 22 March 2016].

Ahlenius, H., 2007. *Northern Sea Route and the Northwest Passage compared with currently used shipping routes*. [online] Available at: http://www.grida.no/graphicslib/detail/northern-sea-route-and-the-northwest-passage-compared-with-currently-used-shipping-routes_77e3 [Accessed 1 April 2016].

Arctic Corridor, n.d. *Arctic Railway: Rovaniemi – Kirkenes*. [online] Available at: <http://arcticcorridor.fi/assets/Esitteit/JKRautatieSCR9ENG.pdf> [Accessed 16 January 2016].

Arola, H., 2015. Suomi saa pitkästä aikaa Itämerelle uuden jäänmurtaajan. *Helsingin Sanomat*. [online] Available at: <http://www.hs.fi/talous/a1449816269413> [Accessed 4 January 2016].

Bernstein, S., Lebow, R.N., Stein, J.G. and Weber, S., 2000. God Gave Physics the Easy Problems: Adapting Social Science to an Unpredictable World. *European Journal of International Relations*, Vol 6(1), pp 43-76.

Bert, M. 2012. The Arctic is Now: Economic and National Security in the Last Frontier. *American Foreign Policy Interests*, 34, pp. 5-19.

Blunden, M. 2012. Geopolitics and the Northern Sea Route. *International Affairs*, 88:1, pp. 115-129.

Borgerson, S., 2013. The Coming Arctic Boom: As the Ice Melts, the Region Heats Up. *Foreign Affairs*, 92(4), p. 76-89.

Bradwell, P., Johar, I., Maguire, C. and Miner, P., n.d. *Future Planners: Propositions for the next age of planning*. London: Demos.

Delfi, 2016. TTÜ teadlased töötavad välja meetodit laevade merejääs navigeerimise hõlbustamiseks. *Delfi*. [online] Available at: <http://www.delfi.ee/news/paevauudised/eesti/ttu-teadlased-tootavad-valja-meetodit-laevade-merejaas-navigeerimise-holbus-tamiseks?id=73867157> [Accessed 6 March 2016].

Dunbar, M., 2016. Arctic. *Encyclopædia Britannica*. [online] Available at: <http://www.britannica.com/place/Arctic> [Accessed 24 January 2016].

Edwards, C., n.d. *Futures thinking (and how to do it ...)*. London: Demos.

Eesti Reformierakond, Sotsiaaldemokraatlik Erakond and Erakond Isamaa ja Res Publica Liit, 2015. *Eesti Reformierakonna, Sotsiaaldemokraatliku Erakonna ning Erakonna Isamaa ja Res Publica Liit kokkulepe valitsuse moodustamise ja valitsusliidu tegevusprogrammi põhialuste kohta*. [online] Available at: <http://www.sotsdem.ee/wp-content/uploads/2015/04/RE-SDE-ja-IRLi-valitsusliidu-lepe.pdf> [Accessed 15 March 2016].

Forbrig, J., 2015. *What's Ahead for Russia and the West? Four Scenarios*. [online] Available at: <http://www.gmfus.org/publications/whats-ahead-russia-and-west-four-scenarios> [Accessed 21 February 2016].

Gould-Davies, N., 2016. *Russia's Sovereign Globalization: Rise, Fall and Future*. [online] Available at: <https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/20160106RussiasSovereignGlobalizationGouldDaviesFinal.pdf> [Accessed 21 February 2016].

Government of Canada, 2013. *Partial Submission of Canada to the Commission on the Limits of the Continental Shelf regarding its continental shelf in the Atlantic Ocean: Executive Summary*. [online] Available at: http://www.un.org/depts/los/clcs_new/submissions_files/submission_can_70_2013.htm [Accessed 11 January 2016].

Holmes, J., 2012. Open Seas: The Arctic is the Mediterranean of the 21st century. *Foreign Policy*. [online] Available at: <http://foreignpolicy.com/2012/10/29/open-seas/> [Accessed 2 January 2016].

Jones, B., 2014. Russia activates new Arctic Joint Strategic Command. *IHS Jane's 360*. [online] Available at: <http://www.janes.com/article/46577/russia-activates-new-arctic-joint-strategic-command> [Accessed 17 January 2016].

Kaljurand, R., Neretnieks, K., Ljung, B., Tupay, J., 2012. *Developments in the Security Environment of the Baltic Sea Region up to 2020*. Tallinn: International Centre for Defence Studies.

Karjus, J., 2015. Kas Arktika jää sulamine toob Helsingi ja Tallinna vahele tunneli? *Postimees*. [online] Available at <http://tallinncity.postimees.ee/3385377/kas-arktika-jaa-sulamaine-toob-helsingi-ja-tallinna-vahele-tunneli> [Accessed 16 January 2016].

Kaukvere, T., 2014. Eesti laev murdis Arktika naftaväljadele. *Postimees*. [online] Available at: <http://majandus24.postimees.ee/2984383/eesti-laev-murdis-arktika-naftaväljadele> [Accessed 6 March 2016].

Kirtman, B., Power, S.B., Adedoyin, J.A., Boer, G.J., Bojariu, R., Camilloni, I., Doblas-Reyes, F.J., Fiore, A.M., Kimoto, M., Meehl, G.A., Prather, M., Sarr, A., Schär, C., Sutton, R., Oldenborgh van, G.J., Vecchi, G. and Wang, H.J., 2013. Near-term Climate Change: Projections and Predictability. In: Stocker, T.F., Qin, D., Plattner, G.-K., Tignor, M., Allen, S.K., Boschung, J., Nauels, A., Xia, Y., Bex V. and Midgley, P.M. eds. 2013. *Climate Change 2013: The Physical Science Basis. Contribution of Working Group I to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change*. Cambridge and New York: Cambridge University Press. pp 953-1028.

Kuul, M., 2015. Paeti hinnangul peaks Eesti pürgima vaatlejaks Arktika Nõukokku. *Eesti Rahvusringhääling*. [online] Available at <http://uudised.err.ee/v/valismaa/7c5daa85-d400-4209-8fe6-df1978b3462e> [Accessed 5 March 2016].

McLaughlin, E.C., 2015. Amid NATO exercises, Russia puts Northern Fleet on 'full alert'. *Cable News Network*. [online] Available at <http://edition.cnn.com/2015/03/16/europe/russia-arctic-military-exercises/> [Accessed 25 March 2016].

Ministry of Defence UK, 2014. *Global Strategic Trends – Out to 2045*. [online] Available at <https://www.gov.uk/government/uploads/system/uploads/attachment>

[data/file/348164/20140821_DCDC_GST_5_Web_Secured.pdf](#) [Accessed 1 April 2016].

Ministry of Economic Affairs and Communications; and Technical Regulatory Authority, 2015. *Rail Baltic: Fast and eco-friendly rail connection to Europe*. [online] Available at <http://www.railbaltic.info/en/> [Accessed 16 January 2016].

National Aeronautics and Space Administration (NASA), 2003. *The Arctic Perennial Sea Ice Could Be Gone by End of the Century*. [online] Available at: [http://www.nasa.gov/vision/earth/environment/Perennial Sea Ice.html](http://www.nasa.gov/vision/earth/environment/Perennial_Sea_Ice.html) [Accessed 2 January 2016].

National Snow and Ice Data Centre, 2015. *What is the Arctic?* [online] Available at: <https://nsidc.org/cryosphere/arctic-meteorology/arctic.html> [Accessed 24 January 2016].

Nielsen, T., 2014. 125 days of navigable conditions by 2050. *BarentsObserver*. [online] Available at: <http://barentsobserver.com/en/business/2014/04/125-days-navigable-conditions-2050-01-04> [Accessed 24 March 2016].

Northern Sea Route Information Office, n.d. *Untitled map*. [online] Available at: http://arctic-llo.com/images/nsr/nsr_1020x631.jpg [Accessed 22 March 2016].

Nye, J.S., 2016. The Russian Connection Between Syria and Ukraine. *The National Interest*. [online] Available at: <http://nationalinterest.org/feature/the-russian-connection-between-syria-ukraine-15237> [Accessed 8 Marchy 2016].

Ogilvy, J., 2015. Scenario Planning and Strategic Forecasting. *Forbes*. [online] Available at: <http://www.forbes.com/sites/stratfor/2015/01/08/scenario-planning-and-strategic-forecasting/#2aa195196b7b> [Accessed 20 February 2016].

Oliphant, R., 2015. Russia claims resource-rich swathe of Arctic territory. *The Telegraph*. [online] Available at: <http://www.telegraph.co.uk/news/worldnews/europe/russia/11782413/Russia-claims-resource-rich-swathe-of-Arctic-territory.html> [Accessed 11 January 2016].

Osica, O., 2010. The High North as a New Area of Cooperation and Rivalry. *nowa Europa*, special Issue 1 (4)/2010. Warszawa: Centrum Europejskie Natolin.

Ostenso, N.A., 2016. Arctic Ocean. *Encyclopædia Britannica*. [online] Available at: <http://www.britannica.com/place/Arctic-Ocean> [Accessed 24 January 2016].

Papp, R.J., 2012. The Emerging Arctic Frontier. *Proceedings Magazine*, 138/2/1, 308. Available at: <http://www.usni.org/magazines/proceedings/2012-02/emerging-arctic-frontier> [Accessed 2 January 2016].

Peters, J., 2015. Russia Isn't Trying to Start a War in the Arctic — It's Just Keeping Out the Riffraff. *VICE News*. [online] Available at: <https://news.vice.com/article/russia-isnt-trying-to-start-a-war-in-the-arctic-its-just-keeping-out-the-riffraff> [Accessed 17 January 2016].

PricewaterhouseCoopers International Limited, 2015. *The World in 2050: Will the shift in global economic power continue?* [online] Available at: <https://www.pwc.com/gx/en/issues/the-economy/assets/world-in-2050-february-2015.pdf> [Accessed 21 February 2016].

Rand, E., 2011. Eesti ettevõtted on Arktikas piirdunud kalapüügiga. *Eesti Päevaleht*. [online] Available at: <http://epl.delfi.ee/news/eesti/eesti-ettevotted-on-arktikas-piirdunud-kalapuugiga?id=51290444> [Accessed 6 March 2016].

Robinson, J.L., 2015. Northwest Passage. *The Canadian Encyclopedia*. [online] Available at: <http://www.thecanadianencyclopedia.ca/en/article/northwest-passage/> [Accessed 24 January 2016].

Rogers, J., 2012. Geopolitics and the 'Wider North'. *The RUSI Journal*, 157:6, pp. 42-53.

Scudellari, M., 2013. *An unrecognizable Arctic*. [online] Available at: <http://climate.nasa.gov/news/958/> [Accessed 9 March 2016].

The GeoPolitics in the High North, n.d. *Where is the "High North"?* [online] Available at: http://www.geopoliticsnorth.org/index.php?option=com_content&view=article&id=1:an-international-research-project&catid=1:latest-news [Accessed 9 March 2016].

Tuohy, E. ed., 2014. *Cooperation and Conflict in the Arctic: A road Map for Estonia*. Tallinn: International Centre for Defence Studies.

United Nations (UN), 1982. *United Nations Convention on the Law of the Sea*. [online] Available at: http://www.un.org/depts/los/convention_agreements/texts/unclos/closindx.htm [Accessed 9 January 2016].

United Nations (UN), 2015. *World Population Prospects: The 2015 Revision, Key Findings and Advance Tables*. [online] Available at: http://esa.un.org/unpd/wpp/Publications/Files/Key_Findings_WPP_2015.pdf [Accessed 21 February 2016].

United States Geological Survey, 2008. *US Geological Survey Fact Sheet 2008-3049: Circum-Arctic Resource Appraisal: Estimates of Undiscovered Oil and Gas North of the Arctic Circle*. [online] Available at: <http://pubs.usgs.gov/fs/2008/3049/> [Accessed 2 January 2016].

Vaikmäe, R., n.d. *A glimpse on: Estonian Polar Research*. [online] Available at: <http://www.eu-polarnet.eu/european-polar-science/europe-and-the-polar-regions/estonian-polar-research.html> [Accessed 5 March 2016].

Välisministeerium, 2015. *Eesti ja Norra majandussuhted*. [online] Available at: <http://www.vm.ee/et/eesti-ja-norra-majandussuhted> [Accessed 6 March 2016].

Wilkinson, A. and Kupers, R., 2013. Living in the Futures. Harvard Business Review. [online] Available at: <https://hbr.org/2013/05/living-in-the-futures#> [Accessed 20 February 2016].

Young, O.R., 2011. The future of the Arctic: cauldron of conflict or zone of peace? *International Affairs*, 87:1 (2011), pp. 185-193.

Given the strong Russian and Soviet heritage for use of air power in directly subordinated support of land operations, how would a near-future contest between NATO and Russian forces match this against NATO's air doctrine of independent, deep air operations?

MAJ Steven Grimshaw

Russia's and NATO's use of air power in comparison: what is to be expected?

...doctrine is more than a theoretical luxury of value only in the classroom. It must instead be the binder, the adhesive, *justifying* our future technological research and development, rationalizing our planned acquisition strategy and governing our present employment of forces.

Introduction

Many questions and doubts have arisen regarding the use of air power, ever since aviation was first used in military conflicts. The reasoning behind this long-lasting discussion can be found in five aspects of air power: Firstly, air power is relatively new in armed conflicts in comparison to land and naval operations, as the first powered flight of the famous Wright Brothers dates back to 1903. Secondly, air power (comparable to naval power) is relatively expensive. Its full range of capabilities is only reserved for wealthy nations such as members of the G7 and Russia. Thirdly, due to its unique characteristics of speed, range and flexibility, projection of air power often has a decisive role in the outcome and the tendency towards a more attrition-like form of warfare, as seen in the latest in the two Gulf wars. Fourthly, and in close context to the latter, air power can achieve high effectiveness, while simultaneously avoiding high risks and casualties, especially in comparison to high intensity land warfare. Hence, air power is politically more acceptable and the threshold for its application is lower. Fifthly, air power seems to be a flexible contribution for solving regional conflicts such as Libya 2011 or the current conflict in Syria, not only for western states, but also for Russia. At least politically, the threshold of unleashing it is relatively low.

During the discussion on how to apply air power best, two tendencies have emerged. One is more in support of seeing air forces independently, directly conducting the overall military objective through deep attacks. These supporters are principally represented by major NATO members such as the United States (U.S.) or the United Kingdom (U.K.). The other favours short-range massed aviation attacks in close support to the ground forces, mainly represented by Russia. As both are very different and imply not only advantages, when thinking of possible future scenarios, the question is to be raised which “philosophy” will prevail.

Despite the recent developments and lessons learned in Russia's air forces, also taking western air power's evolution into account, this essay will argue that Russia cannot fully adapt to NATO's approach in the near future due to historical, economic, technological and geopolitical factors. This limits Russia to having a rather unbalanced air force, incapable of applying the full potential of air power. Firstly, this paper will analyse the origins of the current use of Russia's air power, by taking the mentioned factors into account. Secondly, it will discuss the Soviet heritage for use of air power against the background of recent developments in Russia's air forces. Thirdly, western and NATO's evolution of air power will be portrayed, before describing the most recent approach. On the basis of that research, the paper will describe further derivations and implications as to future developments and shed light on the subject of possible conclusions. A near future contest serves as a purely hypothetical assumption, which may or may not have been valid only in cold war times.

During the examination, this essay will focus on historical, economic, technological and geopolitical factors based on open sources. The analysis, the comparison and the contest will be limited to the European theatre and will not analyse the application of naval aviation or a potential clash between Russia and China. Ethical questions as to the use of air power will also not be addressed.

Development of Soviet air power prior and during World War II (WWII)

In order to understand the Russian perspective, it is necessary to analyse the historical developments of Russia's *Voyenno-Vozdushnye Sily* [VVS – military air forces] in combination with the exclusive impact on doctrine by specific Soviet theorists. Prior to WWII, the Soviet chief aviation editor Lapchinskii described the nature of military aviation missions as independent [*nezavisimii*], separate [*samostoiatel'nyi*] and service [*sluzhatel'nyi*]. Air forces' degree of independence was to be based on size. Despite emphasising indirectly the independent role, Lapchinskii recommended that whenever air forces were massed at a military front, they were always to be subordinated to the responsible ground forces commander. Different to the western way of thinking, total *air superiority* was not considered as achievable. In the area of ground forces' operations, air superiority was only to be seen as a temporary and tactical condition. This mindset arguably indicates that air and ground campaign were mostly to begin simultaneously. Additionally, the main tasks for the VVS resulted in conducting Close Air Support (CAS), Air Interdiction (AI) and Counter Air Operations (CAO) to a range of approximately 200 kilometres from the frontier. During the Spanish civil war from 1936-1939, faith in long-range bombing had increased, but still doubts in bombing cities or factories dominated. Soviet commanders preferred to conduct attacks against nearby enemy air bases. But again success on the ground emphasised air power's supporting role in Soviet doctrines, putting an end to tendencies towards a more independent VVS with more long-range capabilities. Because theory, main tasks and events drive doctrine and allocation of resources, this explains why a preference of subordinated tactical aviation over independent long-range aviation has been so deeply ingrained.

After a disastrous start for the VVS in 1941, due to poor readiness and training, the main ideas basically did not change. Communication and coordination problems were solved through decentralising control to units away from the front. Not only did management and logistics become more complicated, but also the ability to centralise control and concentrate the effort of air power was given up. This did not apply in total for the long-range aviation at strategic level. In order to gain the necessary decentralisation of control, strategic aviation was directed by

representatives of the Soviet High Command. Nonetheless, success of the VVS was still measured through decisive ground battles such as Stalingrad or Kursk. Despite the fact that strategic *air superiority* was achieved after these battles, the extent in which air attacks were related to major ground attacks increased from 70-75% at early stages to 90-95% in the Battle of Berlin. Partisan movements behind German lines had supported this high proportion. Instead of conducting deep air operations, long-range aviation flew approximately 71% of their sorties against troops, combat equipment and railroad targets.. Even in 1945, as the Soviets clearly had the upper-hand, CAS and Defensive Counter Air (DCA) remained the main objectives, not only because of the Allies' Strategic Attack (SA) campaigns. Again partisan's achievements covered the need for more AI-capabilities. During WWII, the successfully implemented tactics had been massing of tactical aviation, surprise and economy of force in support of ground forces' *hammer blows*. Not only did the VVS switch from centralised to decentralised control, but heavy investments in short-range capabilities and numbers, rather than in long-range aviation airplanes followed. Massed, but subordinated employment of air power in the main thrust of ground forces became the staple for later post-war thinking. The Soviet application of air power had developed in this direction because it was affordable and necessary, after being attacked in June 1941.

Economic, technological and geopolitical factors relevant until today

Close cooperation of Russian aviation and ground forces is also based on influencing factors. Since its early days, the Soviet aircraft industry was state-owned and divided into rather independent but closely interrelated sectors. Especially after aircraft became more advanced since the 1930's, technological complexity enforced an increasing specialisation on certain types of aircraft. Due to lack of competition, a missing necessity to maximise profit and as a result of the *Five-Year Plans*, the aircraft industry's drivers were high production output and spare parts supply rather than huge model variety or technological advantage. Besides operational requirements mainly technological deficits, especially in engine design, led to further specialisation on relatively simple short-range combat aircraft, such as the famous Il-

2 Sturmovik.¹¹ In comparison to the U.S. and U.K., who had an advanced technological knowledge and a higher industrial base, the Soviets could simply not afford ingenious long-range aviation. The aftermath of this development lasts until today and has a restrictive effect on the VVS's reforms and modernisation.

Furthermore, the geopolitical situation still plays an important role. Unlike the U.S. and U.K., the Russian Empire has always shared borders with potential enemies, making the land domain its main concern. The outcome of war would always be decided on the ground. This deeply different mindset contributed to a special understanding concerning the VVS's main tasks. Supporting in destroying the adversary and achieving those tasks beyond ground forces' capabilities, remained the VVS's main objective. Hence, their limitations in technology and economy forced the Soviets into focussing on less expensive tactical aviation. Nonetheless, it was the undoubted success of the VSS during WWII, and the Soviet perception of its geopolitical situation that drove Soviet doctrines. Either in self-defence or in an act of pre-emptive strike, the first and foremost task for the VVS remains ensuring the triumph of their ground forces. A more independent role with special emphasis on deep air operations was for the VVS never completely outside its specifications. For example, medium and long-range bombers such the Myasishchev M-4 (1955) or the Tupolev Tu-95 (1956) were introduced, which secondary tasks were strategic atomic bombing. But based on perception and limitations, tactical aviation in a directly subordinated role for reasons of efficiency has always been prioritised.

The Soviet heritage – how is Russian air power applied today?

Recent Soviet military participation in regional conflicts only changed the general conceptions to a limited extent. During the Soviet-Afghan war from 1979-1989, despite the major role of providing CAS, many VVS Staff Officers realised that the more independent and centrally controlled air power could be executed, the more could be achieved. But so ingrained were views that many of these opinions were

¹¹ See annex B, figure 2.

suppressed at that time . Nevertheless, the use of air power in *Desert Storm* in 1990/91 and NATO's intervention *Deliberate Force* in Bosnia in 1995 made the Russian leadership rethink the VVS's structure and role between the first and second Chechen conflict. Forming four *territorial air staffs* and executing centralised control by the various commands of the VVS became the new principle for solving conflicts. This meant a more independent 'spearhead-like' approach prior to the use of ground forces (Lefebvre, 2003, pp. 44-45; de Haas, 2004, pp. 117-122). Contributing to solving regional conflicts were considered as future tasks, so modernisation of the *Dalnyaya Aviatsiya* [DA – long-range strategic aviation] was again given the lowest priority, behind the *Frontavaya Aviatsiya* [FA – tactical air force], the *Aviatsiya Sukhoputnykh Voysk* [ASV – Army aviation] and even the *Voyenno-Transportnaya Aviatsiya* [VTA – transport aviation forces] . As a constant perception, displaying nuclear power was intended as the main task for the DA. This also explains, why the DA's 10 percent of the air forces' budget could never receive the western-style financial attention of 25-30 percent. Even though new western approaches were witnessed, a radically new approach was not achieved. An integral aspect remained the close allocation to ground forces' operations and the uppermost importance of tactical aviation for solving conflicts in Russia's periphery. From Russia's geopolitical and economic point of view, especially when taking the "price tag" of its nuclear deterrence program into account, prioritised distribution of resources to tactical aviation seems the logical approach.

The newest developments in Russia's air forces

After analysing developments mainly before the turn of the millennium, there is also recent evidence which shows that Russian aviation has partially adapted. Similar to the Chechen conflict, the war in Georgia in 2008 revealed significant deficiencies of the VVS. According to researchers Pallin & Westerlund and Cohen & Hamilton , especially the much needed Suppression of Enemy Air Defences (SEAD) against a limited enemy, the shortfalls in training, tactics and equipment and the inability to

launch precision attacks from safe distances or under the cover of night are to be mentioned. The inability to never completely establish air superiority speaks for itself. Moreover, the war had showed an inability to support the ground forces with much needed CAS. Lacking inter-service communication equipment made efficient cooperation of army and VVS impossible (Pallin & Westerlund, 2009, p. 407; de Haas, 2011, pp. 95-96). The shortcomings exposed in this conflict provided the basic motivation for a wider reaching reform, involving a smaller, but more effective performance-orientated army and a reduced, but better trained and equipped VVS. Merging of VVS and Russia's until then independent *Voiska Protivovozdushnoi Oborony* [VPVO – Air Defence Forces], reduction of bases aiming for better coordination accompanied by severe changes in personnel structure and training were the results. Furthermore, as a recent development, naval aviation was subordinated to the VVS and the general organisation was changed from previous divisional or regimental structure to an air base organisation – similar to western countries. The idea behind this allocation across the military districts is that CAS and air cover can be provided more efficiently in the army brigades' most likely area of operations (Baker, 2012, pp. 69-70; Forss, et al., 2013, pp. 67-78; Järvenpää, 2014, pp. 2-6). But above all is a shift to a belief, that quality will prevail over quantity for achieving air superiority and reaching strategic objectives .

Although the Russo-Georgian War has undoubtedly revealed the VVS's deficits, revolutionary changes in Russian doctrines have not yet taken place. What can be witnessed, is that Russia is investing much in modern technologies such as unmanned aerial vehicles (UAVs), stealth bombers and electronic warfare (EW) capabilities (Baker, 2012; IISS, 2015, pp. 159-162; Tilghman, 2015). In particular, a new strategic bomber (which is under development) could complement the approximately 140 Soviet-era medium- and long-range bombers. The very capable FA has approximately 580 aircraft at its disposal, from which 12 percent are considered as state-of-the-art and 4-5 percent being modernised annually. By 2020, Russia aims at having 1500 new or modernised aircraft, including 600 mainly tactical fighters and bombers, 1000 helicopters and 200 new air defence systems. Additionally, past command, control and communication (C3) deficits could be overcome by introducing early warning and control aircraft comparable to NATO's

AWACS planes. In comparison to the Russo-Georgian War, all of these innovations could improve the VVS's precision strike capability, the achievable sortie rate, operational tempo and inter-service integration.. Some analysts therefore believe, that all these reforms and investments, especially in drone and jamming capabilities, could abandon an almost familiar assumption of air superiority. But technological deficits, a decreasing and sanctioned economy, inter-service rivalries and a new personnel structure are still hampering these plans (Baker, 2012, pp. 75-76; de Haas, 2011, pp. 97-100; Grätz, 2014). However, more remarkable is that Russia does not seem to be able to detach itself from its old heritage of close support and subordination to ground forces' operations. Especially in the case of 2008, Russia's strategy was not to achieve decisive effects with air power, but to accomplish overwhelming superiority with land forces, having navy and VVS only in a supporting role (Pallin & Westerlund, 2009, p. 403-406; de Haas, 2011, p. 95). The VVS focussed more on degrading military equipment than destroying critical infrastructure, which led to having the DA mainly drop unguided bombs from safe altitudes rather than conducting deep and precise attacks . Even in the current conflict of Syria, the high rate of imprecise air attacks does not give evidence to an increase of Russia's precision-strike capabilities . Therefore, even though a huge modernisation and reform program was launched, full doctrinal changes seem to lag behind with the tendency of falling back to "classical habits" rather than looking ahead (Pallin & Westerlund, 2009; Cohen & Hamilton, 2011, p. 63). Last but not least, it is often the nature of conflicts that drives doctrines. Taking the past and current conflicts into account, new revolutionary changes are not to be expected soon.

Evolution and revision of air power in NATO

NATO's unified and efficient application of air power has been relatively consistent and successful, ever since military aviation has been utilised in major battles. Based mainly on the approaches of the Royal Air Force (RAF) and the later United States Air Force (USAF), three key principles are of utmost importance: *centralised control*, *decentralised execution* and *strategy-to-task* (NATO, 2009, p. 1-4). Discussions on how to employ air power best and the development of these principles go back to the days prior to WWII. According to Mets the three main theorists that led the 'early

western' mind set are: Giulio Douhet (1869-1930, Italy), Hugh Trenchard (1873-1956, U.K.) and William Mitchell (1879-1936, USA). They all came from different backgrounds, but all three supported that air power as an offensive tool would be the decisive factor. Although the effectiveness of strategic bombing during WWII is still heavily discussed, all underlined the importance of morale and the potential intimidating effects achieved by aviation deep inside enemy territory (Hallion, 2011, pp. 79-80; Mets, 1999, pp. 73-74). One of the main differences between the three is that Trenchard and Mitchell 'asserted the vulnerability of industrial and infrastructure as well as their importance to civilian morale'. Douhet on the other hand, supported more the possibility of bombing cities. All three classical theorists influenced the development of air power in western states.

Meanwhile, the classical theories have been slightly revised. First of all, their way of thinking emerged between the two Great Wars. Hence, they concentrated more on total wars between major states with totalitarian leaders. According to Mets, only Mitchell argued that even small actors could have so-called centres of gravity (COG), from which source they receive their morale or physical strength, will to fight or their freedom of action (Mets, 1999, p. 74; NATO, 2010, p. 2-C-3). Secondly, some analysts such as Futrell and Hughes indirectly support Russia's view by stressing the importance of tactical air power over strategic attacks for the success of the Allies in WWII. Thirdly, all three classical theorists could not provide sophisticated answers as to the impact of future technologies such as long-range stealth bombers or precision-guided munitions (PGM). Most of this could not be further investigated until Desert Storm. Until that time, e.g. during the Korean war, Vietnam or any of the wars in the Middle East, strategic aviation had never been applied. Most of the new technologies had neither been developed nor been utilised in mission before. Therefore, the classical theories seem to be outdated or missing the maximum effectiveness and efficiency needed in modern scenarios.

The newest approach of western air power and NATO

At the dawn of Desert Storm, John Warden's theory of air power updated the existing theories. As in most of the classical theory, he assumes that gaining and maintaining air superiority is of the uppermost importance accompanied by the importance of degrading the enemies' will to fight and favouring the offensive role of military aviation. But in contrast to the classical theories he sees air forces capable of winning certain campaigns independently of other services, not only against smaller actors but also against states (Mets, 1999, pp. 59-62; Byman & Waxman, 2000, pp. 22-25). Better intelligence, PGMs, undetectable stealth bombers, such as the B-2¹², and highly efficient command networks and information systems have made it possible to attack COGs in parallel and with greater precision. Warden's core theory is that the COGs can be arranged in five rings, with leadership targets in the middle, then production facilities, critical infrastructure, population and ground forces to the outside.¹³ The key to success is generally targeting from the centre and then moving to the outside, but targeting all the objectives in every ring in parallel rather than in sequential order is even more decisive. His theory does not exclude the possibility to prioritise CAS over SA or AI, because certain situations and a necessary direct impact can create a state of emergency. But in general, long-range application of air power is always preferable to CAS, 'because it allows more targets to be killed at less cost'. The success of the Gulf War's air campaign does support Warden's ideas, despite the undeniable demand for boots on the ground, as seen in later allied interventions.

Warden's ideas were not totally new, but did revise the classical theories. His theory adapted to new possibilities, but also to necessities resulting from new technologies and the change in conflict. However, a general preference of an independent air force has generally prevailed since WWII. The preference of long-range attacks over close allocation and tasking to ground forces, controlled from a centralised command have also dominated.

¹² See annex B, figure 4.

¹³ See figure 1.

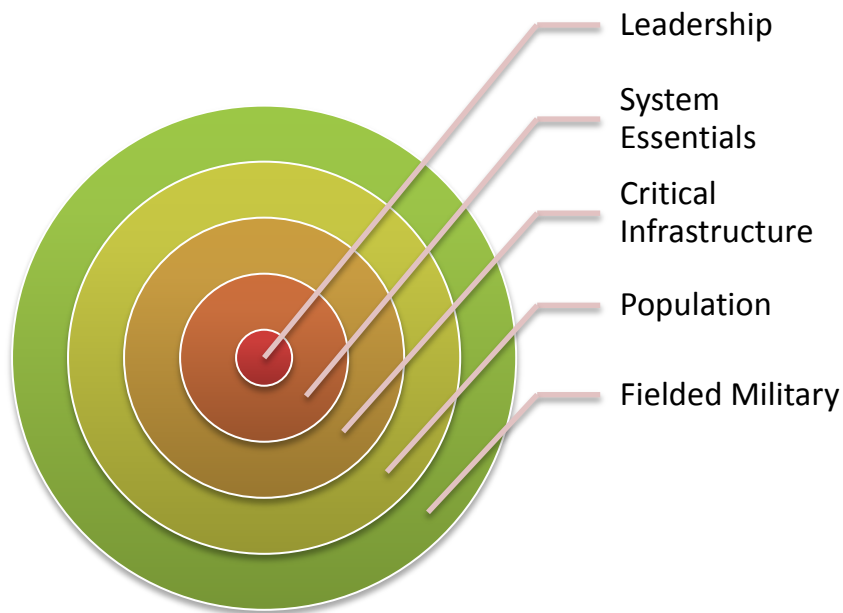


Figure 1: Warden's Five Rings (own illustration).

This explains a different prioritisation of resources and the approaches towards long-range aviation in the RAF and the USAF, but also in other NATO countries such as Germany and France. The results of this process are well-balanced but rather expensive air forces, capable of winning the contest for air superiority and precisely striking deep inside enemy territory. Technological advance, unrestricted competition and higher economical output have made this possible. These advantages have formed the basis for the success of NATO and have been proven to be successful.

Further derivations and implications for today

Russia has no further necessity to change. From a historical perspective, their strategy has always been successful. It has won the Great Patriotic War and managed to contain every regional conflict such as Chechen or Georgia, with or without the VVS. From a geopolitical point of view, Russia's "sphere of influence" may have declined in the past 10-15 years, but the strategic depth which needs to be covered basically has not changed. High penetration capabilities of conventional ground forces have always been the key to success, with the VVS in an important but only supporting role. Reliance on consistently strong land forces and heavy nuclear

capabilities, in terms of strategic missile and long-range aviation forces, have added to this way of thinking. Besides, conflicts such as Syria cannot be taken into account when comparing doctrinal changes, because an extensive use of ground forces has never been on Russia's agenda. In order to change an over 70-year-old heritage, a mixture of intrinsic motivation and more external pressure might be necessary. In the end, accepting that the VVS has not yet really fought a predominant opponent, could contribute to a different mindset.

From NATO's perspective, a necessity for change has not yet been identified. The main idea of a very independent air component focussing on deep air operations has not changed since NATO's foundation. The fundamental assumption during the Cold War has always been, that NATO would face difficulties holding off the first echelon of attacking ground forces purely with air power, at least not without suffering a decisive amount of losses. Besides triggering a nuclear response, the main task for all across Germany dispersed ground units was to stop any further penetration. The main effort for NATO's air force was to achieve and maintain air superiority, which inevitably requires deep air operations. In order to support the ground operations at best, focussing in the following on the enemies COGs and denying him the ability to introduce further echelons of attacks has always been the logical approach against an enemy of great strategic depth. This rather offensive form of air war focusses not on winning a single battle, but on achieving simultaneous, precise and lasting effects with low own casualty rates. Furthermore, the capability to achieve deep effects adds an important deterrence factor to NATO's defensive posture (Futrell, 2002, pp. 445-446; Mason, 2011, pp. 46-48). Abandoning this successful approach in the near future, seems as unlikely as Russia fully adapting to it.

But this perception may change and is very reliant on NATO-Russian relations and future missions. Indeed, since Desert Storm, the tasks of western air forces and Russia's VVS have been rather similar. Taking the recent conflicts into account, solving regional conflicts has reached a high level also in NATO's task list. From the classical perception, a relatively new and uncharted terrain. Therefore, and especially when expecting a continuing change in conflict and technology, it seems fair to

assume that further alterations could be possible. However, in a near-future contest, the Soviet heritage compared to NATO's air doctrine will not make an initial difference. As conflict develops, the analysis of this paper has shown that both sides will fall back to their peculiar approaches. In that case, NATO's well balanced but expensive mix of application offers more flexibility and the full potential of air power. Limitations of the Russian approach, would be brutally revealed against an opponent with sophisticated long-range capabilities. In fact, the question is not whether NATO's approach is better, but what can both politically and monetarily afford in the future.

Conclusion

This essay compared the Russian way of using air power with NATO's approach. Russia's "way" is based on special historical developments, but also from a geopolitical perspective it is absolutely reasonable. Due to limitations in resources and technology, it focussed more on what is required to support the ground forces. NATO took a rather different approach in utilising air forces more independently. From a generally defensive posture and for political reasons, it required to take the necessary strategic depth, necessary deterrence factors and unacceptable high losses more into consideration than Russia. In both cases, there is evidence for an adaptation to new technologies or tasks. The VVS for example, is investing in rather sophisticated technologies which will primarily increase its tactical precision strike elements, besides improving air superiority capabilities within a limited operational depth. Simultaneously, its strategic aviation will develop and may open new possibilities in the future. In case the VVS is utilised, attacks on critical infrastructure, mainly with the purpose to dismantle C3 and to deny or limit access, but also to prepare ground operations can be expected. Despite the strategic depth, an approach which is similar to NATO and feasible given the current capabilities. On the other hand, NATO has developed technologies and tactics to dismantle an opponent's C3 ability and his moral even more efficiently. Given the desired effects, it seems fair to argue that there is not so much of a difference anymore. Prioritisation and the means may be different, based on strategic depths, capabilities and doctrines, but both are very capable of reaching decisive effects in the air and on the

ground in modern conflicts. Nevertheless, in the long run both have their own way of applying air power, with NATO having an advantage over Russia.

NATO and Russia have not fought a direct confrontation in the past. Due to both sides nuclear capabilities and the devastating consequences, this will continue to apply in the near future. The described direct contest between both emerges from revisionist tendencies and a recovering Russia in terms of economic and military strength, yet does not recommend to fall back into outdated Cold War-thinking. However, a detailed study of a future scenario could contribute to improving NATO's deterrence effect. Both sides' capabilities and limitations should be analysed over time and space. Apart from that, indirect confrontation as seen in the latest in Syria will be likely. Therefore, further research underneath the level of direct confrontation between NATO and Russian forces is required, where contributing to solving crisis is considered as the major task. Additionally, this essay analysed on the basis of a predominant NATO and did not analyse the use of tactical nuclear weapons. What if this basic assumption changes or is influenced, how much are the two sides willing to jettison their relatively old perceptions? Given the current scope of functions, both sides have been relatively successful with their approach. The mentioned adaptations make it even harder to clearly divide both. In the end, it might be only size, readiness and technological advantage, not doctrine which matters – but *all* mutually condition each other.

Annex A: List of abbreviations

AI	Air interdiction
ASV	<i>Aviatsiya Sukhoputnykh Voysk</i> [army aviation]
AWACS	Airborne warning and control system
C3	Command, control and communication
CAO	Counter air operations

CAS	Close air support
COG	Centre(s) of gravity
DA	<i>Dalnyaya Aviatsiya</i> [long-range strategic aviation]
DCA	Defensive counter air
EW	Electronic warfare
FA	<i>Frontavaya Aviatsiya</i> [tactical air force]
NATO	North Atlantic Treaty Organization
PAK FA	<i>Perspektivny Aviatsionny Kompleks Frontovoy Aviatsii</i> [literally prospective airborne complex of front-line aviation]
PGM	Precision-guided munitions
RAF	Royal Air Force
SA	Strategic attack
SEAD	Suppression of enemy air defences
UAV	Unmanned aerial vehicle
U.K.	United Kingdom
U.S.	United States
USAF	U.S. Air Forces
VPVO	<i>Voiska Protivivozdushnoi Oborony</i> [air defence forces]
VTa	<i>Voyenno-Transportnaya Aviatsiya</i> [transport aviation forces]
VVS	<i>Voyenno-Vozdushnye Sily</i> [military air forces]
WWII	World War II

The pictures are provided with the intention to create a better understanding of the main topics and enhance the research in the main body of the essay.



Figure 2: Soviet Ilyushin Il-2 Sturmovik in combat, the most produced aircraft in aviation history (Picture taken from <http://www.combatreform.org/mas.htm>).



Figure 3: Russian Sukhoi T-50 (PAK FA) state-of-the-art fifth generation tactical fighter, currently only 5 prototypes were built, but introduction to service is expected for 2017 (Picture taken from <http://www.airforce-technology.com/projects/sukhoit50stealthfigh/sukhoit50stealthfigh2.html>).



Figure 4: B-2 Spirit heavy penetration strategic bomber with stealth capabilities, one of the world's most expensive aircraft to operate and only run in the USAF (Picture taken from <http://www.airpowerworld.info/bombers/northrop-b-2-spirit.htm>).

Bibliography

- Axe, D., 2016. *Russia Is Launching Twice as Many Airstrikes as the U.S. in Syria*. [online] Available at: <http://www.thedailybeast.com/articles/2016/02/23/russia-is-launching-twice-as-many-airstrikes-as-the-u-s-in-syria.html> [Accessed 24 February 2016].
- Baker, C., 2012. Gradual Reform or a Turning Point in Russian Military Transformation: How Russian Air Power has developed through Conflict and Reform from 1991 - 2012. *Air Power Review*, 15(3), pp. 59-79.
- Blechman, B., Bollfrass, A. & Heeley, L., 2015. *Reducing the Risk of Nuclear War in the Nordic/Baltic Region*, Washington, D.C.: Stimson Center & Project High Hopes Foundation.
- Byman, D. L. & Waxman, M. C., 2000. Kosovo and the Great Air Power Debate. *International Security*, 24(4), pp. 5-38.
- Cohen, A. & Hamilton, R. E., 2011. *The Russian military and the Georgia War: Lessons and Implications*, Carlisle: Strategic Studies Institute.
- Copp, T., 2015. *Russia launches second wave of airstrikes in Syria in largest show of airpower since 1980s*. [online] Available at: <http://www.stripes.com/news/russia-launches-second-wave-of-airstrikes-in-syria-in-largest-show-of-airpower-since-1980s-1.379592> [Accessed 10 January 2016].
- de Haas, M., 2004. *Russian security and air power 1992-2002*. Abingdon: Frank Cass.
- de Haas, M., 2011. Military Reform in Russia: Success or Failure?. *Security Index: A Russian Journal on International Security*, 17(1), pp. 95-102.
- Department of the Army, 1950. *Russian Combat Methods in World War II - Pamphlet 20-230*, Washington, D.C.: United States of America War Office.
- Dick, C. J., 2000. Military reform and the Russian air force 1999. *The Journal of Slavic Military Studies*, 13(1), pp. 1-12.

- Dowling, S., 2015. *Russia's Bear: The old-fashioned plane still thriving*. [online] Available at: <http://www.bbc.com/future/story/20150225-the-worlds-noisiest-spyplane> [Accessed 27 February 2016].
- Forss, S., Kiianlinna, L., Inkinen, P. & Hult, H., 2013. *The Development of Russian Military Policy and Finland*, Helsinki: National Defence University.
- Frear, T., Kulesa, L. & Kearns, I., 2014. *Dangerous Brinkmanship: Close Military Encounters between Russia and the West in 2014*, London: European Leadership Network.
- Futrell, R. F., 2002. *Ideas, Concepts, Doctrine - Basis Thinking in the United States Air Force 1907-1960*. Washington, D.C.: Government Reprints Press.
- Gibbons-Neff, T., 2015. *Mapped: Russian vs. U.S. airstrikes in Syria*. [online] Available at: <https://www.washingtonpost.com/news/checkpoint/wp/2015/10/13/mapped-russian-vs-u-s-airstrikes-in-syria/> [Accessed 14 October 2015].
- Gibbons-Neff, T., 2016. *Report: Russia flying early warning aircraft over Syria*. [online] Available at: <https://www.washingtonpost.com/news/checkpoint/wp/2016/01/12/report-russia-flying-early-warning-aircraft-over-syria/> [Accessed 13 January 2016].
- Giles, K., 2014. A New Phase in Russian Military Transformation. *The Journal of Slavic Military Studies*, 27(1), pp. 147-162.
- Gorenburg, D., 2015. *Russia's Syria operation reveals significant improvement in military capability*. [online] Available at: <http://www.lowyinterpreter.org/post/2015/11/13/Russias-Syria-operation-reveals-significant-improvement-in-military-capability.aspx> [Accessed 10 January 2016].
- Grätz, J., 2014. Russia's Military Reform: Progress and Hurdles. *CSS Analyses in Security Policy*, April, Issue 152.
- Greenwood, J. T., 1998. The Aviation Industry, 1917-97. In: R. Higham, J. T. Greenwood & V. Hardesty, eds. *Russian aviation and air power in the twentieth century*. London: Frank Cass Publishers, pp. 126-161.
- Hallion, R. P., 1987. *Doctrine, Technology, and Air Warfare – A Late Twentieth-Century Perspective*. [online] Available at: <http://www.airpower.maxwell.af.mil/airchronicles/apj/apj87/fal87/hallion.html> [Accessed 09 March 2016].
- Hallion, R. P., 2011. U.S. Air Power. In: *Global Air Power*. Dulles: Potomac Books, pp. 63-136.
- Hoyle, C., 2014. *World Air Forces 2015*, London: Flightglobal Insight.

- Hughes, T. A., 1995. *Overlord - General Pete Quesada and the Triumph of Tactical Air Power in World War II*. New York: The Free Press.
- IISS, 2015. Chapter Five: Russia and Eurasia. *The Military Balance*, 115(1), pp. 159-206.
- Järvenpää, P., 2014. *Zapad 2013 - A View From Helsinki*, Washington, DC: The Jamestown Foundation.
- Jasinski, M. & Mizin, V., 2004. Russian Strategic Aviation: In Search of Mission. *The Journal of Slavic Military Studies*, 17(2), pp. 215-235.
- Kainikara, S., 2011. Soviet-Russian Air Power. In: J. A. Olsen, ed. *Global Air Power*. Dulles: Potomac Books, pp. 179-218.
- Kalinina, N. & Kozyulin, V., 2010. Russia's Defense Industry: Feet of Clay. *Security Index: A Russian Journal on International Security*, 16(1), pp. 31-46.
- Kozhevnikov, M. N., 1977. *The Command and Staff of the Soviet Army Air Force in the Great Patriotic War 1941-1945*. Washington D.C.: Government Printing Office.
- Lefebvre, S., 2003. Difficult times for the Russian air force, 1992-2002. *The Journal of Slavic Military Studies*, 16(1), pp. 44-68.
- Locksley, C. C., 2001. Concept, algorithm, indecision: Why military reform has failed in Russia since 1992. *The Journal of Slavic Military Studies*, 14(1), pp. 1-26.
- Mason, T., 2011. British Air Power. In: J. A. Olsen, ed. *Global Air Power*. Dulles: Potomac Books, pp. 7-62.
- Mets, D. R., 1999. *The Air Campaign - John Warden and the Classical Airpower Theorists*. Maxwell Air Force Base: Air University Press.
- Mladenov, A., 2015a. The Bear gains Strength. *Air Forces Monthly*, March, Issue 324, pp. 42-49.
- Mladenov, A., 2015b. Back to the future: Red Fighters. *Air Forces Monthly*, October, Issue 331, pp. 44-59.
- NATO, 2009. *Allied Joint Doctrine for Air and Space Operations*, Brussels: NATO Standardisation Agency.
- NATO, 2010. *Terms and Definitions*, Brussels: NATO Standardisation Agency.
- O'Hanlon, M. E., 2015. *The future of land warfare*. Washington, D.C.: Brookings Institution Press.
- Pallin, C. V. & Westerlund, F., 2009. Russia's war in Georgia: lessons and consequences. *Small Wars & Insurgencies*, June, 20(2), pp. 400-424.

- Pape, R. A., 1997. The limits of precision-guided air power. *Security Studies*, 7(2), pp. 93-114.
- Pennington, R., 1998. From Chaos to the Eve of the Great Patriotic War. In: R. Higham, J. T. Greenwood & V. Hardesty, eds. *Russian aviation and air power in the twentieth century*. London: Frank Cass Publishers, pp. 37-61.
- Russel, M., 2015. *Russia's armed forces - Reforms and challenges*, Brussels: European Parliamentary Research Service.
- Segrè, C. G., 1992. Giulio Douhet: Strategist, Theorist, Prophet?. *The Journal of Strategic Studies*, September, 15(3), pp. 351-366.
- Sinovets, P. & Renz, B., 2015. *Russia's Syria operation reveals significant improvement in military capability*, Rome: DeBooks Italia.
- Sterrett, J., 2002. Learning is winning: Soviet Air Power Doctrine 1935-1941. In: S. Cox & P. Gray, eds. *Air Power History - Turning Points from Kitty Hawk to Kosovo*. London: Frank Cass Publishers, pp. 173-187.
- Sterrett, J., 2007. *Soviet Air Force Theory 1918-1945*. Abingdon: Routledge.
- Stratfor Enterprises, 2015. *Gaming a Russian Offensive*. [online] Available at: <https://www.stratfor.com/analysis/gaming-russian-offensive> [Accessed 15 January 2016].
- Stratfor Enterprises, 2015. *Russia Targets NATO With Military Exercises*. [online] Available at: <https://www.stratfor.com/analysis/russia-targets-nato-military-exercises> [Accessed 10 January 2016].
- Thornton, R., 2008. A Bear with Teeth? - The Russian Military in 2008. *The RUSI Journal*, 153(5), pp. 48-52.
- Tilghman, A., 2015. *Advanced Russian air power, jammers are focus of U.S. troops*. [online] Available at: <http://www.militarytimes.com/story/military/pentagon/2015/12/10/advanced-russian-air-power-jammers-focus-us-troops/77090544/> [Accessed 11 December 2015].
- Warden III, J. A., 2000. *The Air Campaign - Planning for combat*. Lincoln: toExcel Press.

Does globalisation cause asymmetric conflicts? Is it part of the solution or problem?

CPT Ale Prosic

Introduction

Globalisation as a fifth rider of apocalypse is a saviour for one part of the world but damnation for another. There is no place on the Earth which is not influenced by this process; negative influence has been seen especially in the Muslim's world, mainly in the Middle East and North Africa, where 'the majority of regimes, opposition movements, and intellectuals in the region are consciously anti-globalization. Moreover, there is no part of the world where violence is more often used in the anti-globalization struggle, most notably by Osama bin Laden but generally by all radical Islamist movements' (Rubin, 2003). A small group of fanatics targeting the biggest symbol of capitalism and the globalized economic world, in the middle of the day, flying through the well-defended airspace, changed the world security and sent a strong message to creators of globalization. The aim of this paper is to research the interaction of the two phenomena that shape world politics, economy, culture and security of the modern world - globalization and asymmetric conflict. It also researches the globalization effects on asymmetrical warfare and the way that globalization has greatly increased the ability of terrorists using asymmetric means and violence, in order to achieve a political, religious or ideological goal. This paper argues that globalization has caused asymmetric conflicts. This problem raises questions about what are the effects that globalization has on the world? To provide credible answer this essay will cover some of questions, e.g.: What is undesirable and dark side of globalization? How the Middle East experience globalization? Does globalization has overlapping ties with Westernisation or Americanisation, process which causes conflict between western and eastern culture? Is globalization major threat to Muslim tradition and religion? Does globalization causes and facilitate terrorism? The term globalization is very broad term, however for the purpose of this research it is viewed strictly in terms of relevant conflict generator. It focuses more specifically on the dark side of globalization that cause conflicts, both externally and internally. The thesis suggested here is that, globalization is a bleary process, as the saviour for one part of the world but damnation for another, with its negative effects

and one-way direction and global injustice, causes asymmetric conflicts, terrorism and becomes problem for the global security. The paper is structured in three sections. Firstly, it briefly defines the rather confusing and misleading concepts of globalization and asymmetric conflict. Then, the second part shows an interaction between globalisation, cultures and religion. Third part of the essay describes asymmetric opposition of 'weaker' toward 'strong' in the modern form of 'asymmetric warfare', terrorism.

A 'dark side' of globalisation

Globalization is not only a process; it is series of uneven and contradictory processes including political, economic, cultural and technological segment. It does not advocate the only ideology of the free market it strives to change our lives, culture, and tradition as well as local norms, making a global cosmopolitan society. Kirshner argues that 'the powerful and indefatigable economic, political, and cultural pressures associated with globalization give rise to new conflicts between groups' (Kirshner, 2006, 8). This process strikes social cohesion and political integration. It impacts cultural barriers that divide people. Greed, lust for power, profit and control of the rest of the world, western countries and big corporations are widening the gap between rich and poor. Furthermore, this process also called a neoliberal ideology for development, led by International Monetary Fund and World Bank, 'deepens inequality between nations on a global scale, resulting in increased global insecurity through a growing sense of injustice and grievance that may lead to rebellion and radicalisation' (Poku and Therkelsen, 2013, 231).

Defining globalisation is very challenging. This is as such notions as integration, openness, transnational, interdependence, multilateralism, closeness, interconnectedness and conflicts, and many others are echoing as globalization. So, hundred different definitions are available from many experts depending on which circumstance they were created. Academic thinkers are usually divided in the approach of defining globalisation. Interconnection and interactive dimension of inevitable and very helpful process 'can thus be defined as the intensification of worldwide social relations which link distant localities in such a way that local happenings are shaped by events occurring many miles away and vice versa'

(Giddens, 1990, 64). However, others (Lerche, 1998, Hoffman, 2002, Amin, 2003, Hanafi, 2003, Jones, 2000 and Rubin, 2003) are very critique toward this process stating that,

‘globalization has also been portrayed as having a very dark side...driven by economic power, clearly promotes the hegemony of Western culture and corporations; puts jobs and communities at risk in the rich countries and exploits cheap labour in the poorer countries; increases threats to the environment; and undermines the foundations of democracy and social stability by subjecting national political institutions to forces of economic change beyond their control’ (Lerche, 1998).

Furthermore, Hoffman argued that ‘globalization, far from spreading peace, thus seems to foster conflicts and resentments’ (Hoffman, 2002). Another points of view considers globalisation with its radical effects is ‘involving radical reorganizing and reconfiguration of the relationship between individuals, groups and organisations, so that regardless of whether or not individuals become more globally mobile, multiple distant influences affect their lives’ (Jones, 2000, p. 15). French-Egyptian economist Amin describes new globalization led by the political system in the service of global market disturbing the sense of the old process of globalization. Furthermore, he advocates an alternative humanistic project of globalization with a socialist perspective. He argued that ‘the erosion of the old system of globalization is not able to prepare its own succession and can lead only to chaos’ (Amin, 2003, p. 41). He presents evidence of two periods of globalisation. The old one which was helping undeveloped regions with a long-term of gain and the modern one, led by the World Bank and International Monetary Fund, with the short-term of gain. As a consequence, instead of creating ‘New World Order’, globalization process is creating the new form of economic, political and cultural polarization leading the World to new world disorder. This world polarization is especially expressed between industrialized centres and non-industrialized part of the world, between the North and the South.

Most of the Southern thinkers have opposing thoughts about globalization. One of them is Hanafi, he argued that ‘globalization is one of the common forms of Western hegemony, not only achieved through military action or the economy but also, the market’ (Hanafi, 2003). Professor accused several western industrialized nations of making the new age of slavery transforming the Third World into one big market

using the process of globalization as 'one of the forms of Western hegemony based on the laws of the market and military power, a concept which goes back to former imperialism.' Further on, the professor called it 'Americanization, as the United State is now the only existing block which challenges the rest of the world' (Hanafi, 2003). Another Middle Eastern thinker Barry Rubin argued that 'globalization refers to the spread throughout the globe of ideas, customs, institutions, and attitudes originated in one part of the world. At present these are usually Western in origin. Thus, it is easy to see globalization as largely equivalent to Westernization' (Rubin, 2003). The process of the world globalization is opposed to inexorably growing anti-globalization movement. This movement does not reject globalization as such. It is against weaknesses and current globalization process defects. Instead of well-being economy or 'Happiness' there is the process which is going toward economic profit and clash of civilisations. Although, there were always struggles between individuals, between small and big, rich and poor and strong and weak, globalisation made it even worst in last few decades. It created bigger inequality between the North and the South. Those differences are growing sources of tension between globalized and non-globalized, strong and weak, therefore creating conditions for the conflicts. The majority of mentioned conflict above are asymmetric in nature waged within the borders of one country among dissatisfied and government, or on the international arena among dissatisfied groups and big centres of power, conflicts between global hegemons and local forces.

There are no equal powers in the world since the fall of the Iron Curtain. So, after it fall symmetry of conflicts has lost its meaning. Rogue governments, nations and non-state actors are more relying on asymmetrical means to attack its very superior enemy. Symmetric old-fashioned warfare is replaced by 'asymmetry in armed conflict', which 'has been most often interpreted as a wide disparity between the parties, primarily in military and economic power, potential and resources' (Stepanova, 2008, p. 14). Most of the conflicts after the Cold War are seen as intra-state conflicts. In last two decades usually coalition led by strong power is fighting weaker within internal conflicts between states or government and non-state actors. Stepanova gives reliable definition of asymmetric conflict explaining role of USA as the great power in the world, where 'the absolute military–technological superiority of the USA over any other actual or potential opponent means that nearly every armed

conflict in which the USA may be engaged is by definition asymmetrical' (Stepanova, 2008, p. 15). So, following that logic, the asymmetric way of fighting is the only choice for an opponent to express their disagreement. It is not new and it has not been born with globalization but it has been intensified by globalization after transnational terrorist organisation Al Qaida attack on World Trade Centre and Pentagon in 2001. This way of fighting has been in the past and will be the biggest challenge for the countries in the future. Global battlefield, the wide spectre of weapon, unknown adversary, non-tradition methods, new technology and borderless environment will portray contemporary conflicts.

Globalization is reshaping the nature of conflict bringing it from local environment to the global stage through economic, cultural and political pressure creating violence and new vulnerabilities of global security. No doubt that globalization pressure moving toward union or uniformity is creating demand for insulation and forcing weaker for resistance. It is obvious that globalization is a destabilizing factor in individual and groups relationship. Creating 'new cultural world order' global forces are interfering into very sensitive cultural and religious domain, awakening neo-fundamentalism as a product of globalization. However, 'dark side' of globalization is driven by interaction between McWorld from one side and defenders of fundamental cultural and religious values from another side. Instead to have a 'new world order' sufficient for all, globalization aroused the holy war from local to global stage as a reaction against McDonaldization.

Globalisation, culture and religion values

The world will clash because of globalization. Huntington asserted that 'the great divisions among humankind and the dominating source of conflict will be cultural' (Huntington, 1993). He claimed that the endeavour of the Western countries promoting its democracy and liberalism as universal values, in order to maintain its military preponderance and to advance its economic interests will cause violent response from other cultures or civilizations. Globalized civilisations are promoting modern way of life and democracy forcing other to accept it without their will makes friction, even anger. Robert Wright argued that 'the modern world—featuring alcohol, satellite-beamed pornography, lapel-wearing alpha females—is an offense to traditional Islamic values. And globalization sticks modernization in the face of

Muslims, whether they like it or not' (Wright, 2002). There are less and less 'Third World's' countries with whom West share cultural and moral, social and political, - beliefs and aspirations. In essence, globalisation has made harmful consequences to the different culture around the world, especially to the Muslims world. Modernisation, integration, openness, transnational, interdependence, multilateralism, closeness, interconnectedness and everything other describing globalization is going to be against conservative culture and religion of the Muslim's world. The Western aspiration for financial interests and benefits are becoming bigger and bigger leading Western policy to suffer disasters or encountered problems in the Muslims world.

The literature overview is showing that Globalization in a many ways helps people in the Third World countries. If Globalization is taken as phenomena of inter-dependents and interaction in the world it helps not only individuals or benevolent organizations but fundamentalist and Islamic groups too. Griffel argued that 'Islamic fundamentalism has been, in fact, strengthened by globalization. In the Middle East, it is one of its driving forces' (Griffel, 2003). The Middle Eastern fundamental groups are benefiting from flow of information and spread of communication. It is clear that Globalization has made a 'global village' of the world; however it is making Islamic global village too. Modern technology and interconnectedness make it easy to spread the message among fundamentalist and Islamic groups. So, it is unproblematic to present the humiliation and killing Muslim's youth in Palestine, western drones of death bombing Syria's and Iraqi's towns, Islamic fundamentalist executing westerners. There is no need for fundamentalist from all over the world, either Islamic or Christian, to come to the Middle East to see it and start revenge in their neighbourhood in France, US, Belgium or elsewhere in the world. However, western support for Middle East governments in the process of Globalization fuelled conflicts between those pro-western governments and Fundamentalist movement. Anti-westernization idea is not tied only to the national state level or to the particular territory, that idea is in '*Ummah*' (the unity of the Muslims) and it is spread all over the world. So it wouldn't be the mistake to name this conflict a 'global jihad' caused by Globalization according to Griffel. Although Globalization helps fundamentalist and other radical groups to spread its ideology, it encroaches into Islamic culture, religion and other values too.

Even if economical rapid growth, easy integration into the global market using modern informational technologies helps Muslim's countries, there is still the strong impact of Globalization on Muslim culture. Globalization as a phenomenon is going beyond informational technologies and liberal market as it involves culture, moral and religion too. Many Arab thinkers share an opinion that globalisation is directed by the West, e.g. there is 'a general fear that globalization has brought an 'invasion' of American culture to Muslim societies that will 'hollow us out from the inside and domesticate our [...] identity' (LeVine, 2002). Globalization is understood as development of forced difference which guides societies to deepen poverty and inequality inside as well as between countries. The result is the same, continuation of Western domination and its hegemony as it was a hundred years ago. Only differences are that Western countries are using the new tool to overthrow present Islamic cultural norms and establishing its cultural values. Globalization is the new Western approach to realize imperialist aims in the Muslim world. Fighting against capitalism and materialism over two centuries Muslim worlds is again at the edge of the ending of its realm of quietude and immaterialism. Global 'War on terror' after 9/11 attack on the US made it even worse, killing innocent civilians increases terrorism. Radical Islamic movement uses it to mobilize young and unemployed Muslims population against western globalization promoters and negative effects of globalization.

Taking in a consideration Islam and its '*Ummah*' in entire Islamic civilization, it is obvious that many of countries and population are unable to accept global transformation, especially those negative effects of globalization which confronts tradition and religion. Rubin argues that globalization in the Muslim's world is 'seen as a major threat to tradition. Where religion is far more traditional in its practice, the defence of religion also conflicts with the acceptance of modernization' (Rubin 2003). The Islamic religion is based on holy Qur'an and the *Hadith*¹⁴. If modernisation means replacing seven centuries old tradition by a new Western tradition it will not be possible because the Quran is not subject to be changed. In the same article, Rubin

¹⁴ **Hadith, Arabic** Ḥadīth ("News" or "Story"), **also spelled** Hadīt , **record of the traditions or sayings of the Prophet Muhammad, revered and received as a major source of religious law and moral guidance, second only to the authority of the Qur'ān, the holy book of Islam.** (<http://www.britannica.com/topic/Hadith>)

is convinced that 'the very size and cohesion of an Islamic community builds a religious, and hence cultural, wall against many aspects of globalization' (Rubin, 2003). Islam is the religion with its own *Sharia*¹⁵ law based on the Qur'an and *Hadith* and ensures the proper orders to its society, so elements of globalization will be in conflict with Islamic belief. However, as a result, western product, globalization is seen as a devil's work in the many Islamic countries and as such in the future will be seen as hostile.

It is obvious that Globalization is leading the world to chaos. Lynch argued that 'the Arab Middle East stands at the centre of the conflicts and the fear associated with the backlash against the globalisation and Americanisation of the culture' (Lynch, 2006, p. 172). Globalization process is unifying radical Islamic movement in the Muslim's world. Easy and fast spreading anti-globalization Islamists messages letting it be clearly understood and hugely supported among fundamentalist creating anti-western vision justifying a reason for jihad. Muslims anti-globalization movements should not be underestimated. Learning about Islamic culture and its religion, understanding and respecting its 'right to be different' could be the way to mitigate effects made by a ruthless process. -Otherwise, the world is going to face brutal violence between civilisations, manifested through the only possible way, asymmetric warfare well-known as terrorism.

Globalization and terrorism

Terrorism existed even before globalisation process has started. It has been seen as the weapon of the weak in the conflict between states or parties within one state. The phenomenon as an old terrorism form appears in the first century in Palestine, up to new one, global, modern or jihadist terrorism seen today. It is hard to draw the line between those two eras of terrorism, but it is sure that attacks on US embassies and military installations followed by the attack on Twin Towers and Pentagon on September 11, 2001, have changed the world. Well-known terroristic organisation Al Qaeda made the deadly plan somewhere in Tora Bora mountains and exploited it few thousand miles away, in the heart of superpower. It could be evidence that

¹⁵ Sharia, also spelled **Shari'ah** the fundamental religious concept of Islam, namely its Islamic law. (<http://www.britannica.com/topic/Hadith>)

'Islamic terrorism, for example, is not only based on support for the Palestinian struggle and opposition to an invasive American presence. It is also fuelled by a resistance to "unjust" economic globalization and to a Western culture deemed threatening to local religions and cultures' (Hoffman, 2002). Other thinkers are sharing the same claim, for example, Lafraie argues that 'formation of Al Qaeda itself can be seen as a manifestation of globalization. It advocates causes directly or indirectly linked to the globalization process, and its establishment was facilitated by globalisation' (Lafraie, 2014, p.115). The main players in September 11 attack; members of 'the Hamburg Cell' were the product of globalisation process in their countries Egypt, Yemen, Saudi Arabia, Morocco, United Arab Emirates and Lebanon. As a group of young, unemployed people with different education level and religious, disappointed by the West role in their countries were the easy target of terrorist recruiters. Group indoctrinated by anti-globalist, used all benefits of globalisation to travel around and conducted training, easily received money from their founders, were covered by millions of migrants in the USA caused by globalisation and at the end, they used globalisation means, passenger planes, to attack the heart of globalisation.

Terrorism is growing up in both domestic and international arena, especially after the end of Cold War. Modern terrorism is acting violently trying to influence international system. According to Coker, 'the information technologies of the 1980s facilitate international crime and assist terrorism' (Coker, 2002). Tools of globalization to develop societies as 'the engines of globalization – the information revolution, cheap and open intercontinental transportation, global 24-hour media, electronic finance infrastructure, increasing participation in international organizations, and liberalized trade and investment' (Pollard, 2002), now being used by terrorist to weaken or even to destroy those societies. Globalisation provides power and any other means to those non-states actors or terrorist needed to project its power and methods of violence from one to another part of the world. It was not the case of the old or ordinary terrorism seen at local level sponsored by the state. Modern terrorist groups are acting out of national borders, they are acting at international stages using globalization's tools simultaneously attacking the most valuable means of globalisation and power canters of globalisation holders. That is exactly what Al-Qaida is doing at international level. Those terrorist organisations are disrupting

integration of the political, economic and cultural activities and with its violent acts nationally separate peoples. Al Qaida identified globalization as the process of Americanization, that explains why they have chosen globalization holders, World Trade Centre towers, and US military power centre, Pentagon, as their targets and changed the security future of the world. It showed that terrorists do not distinguish civil from military targets in the way of achieving their objectives.

Globalization has changed the nature of terrorism especially after the end of Cold War. Many of civilians were killed in last two decades by terrorists because 'the main reason people are targeted is that terrorists no longer distinguish between limited and restricted uses of violence' (Coker, 2002). According to Coker terrorism is 'the dark side of the global village – the ability of that village's alienated minorities to hit out at their perceived oppressors over huge distances' (Coker, 2004, p. 40). Coker argued that how radical terrorist do not reject the means of globalization but they fight against its message only. They use the common language of globalization, internet, cell phone network what is an authentic product of globalized world even if they are fundamentally against it or in conflict with. They have one in common with forces of globalization and both sides use it to control other or to influence each other. However, the influence of global terrorism as a tool of asymmetric anti-globalization war will increase with the development of modern technology. Modern technology will be equally helpful and in the same time dangerous for modern societies. There will always be some groups or societies not able to become a part of the global world and they will always be anti-global. These societies or anti-global groups have been the dark and dangerous side of globalization process. Globalization through information infrastructure will be giving them more ability to wage anti-globalization war in the future.

Cyber warfare presents an imminent threat to highly globalized countries. Considering cyber threat in the context of globalization, there is no state which can claim that a good capability of understanding of its vulnerability within its information infrastructure and its networks. Moreover,

'national borders are becoming irrelevant in the global and information environment and globalization and ICT remove the differentiation between international and domestic threats. The rapidly changing nature of the threats

enabled by globalized ICT infrastructure makes vulnerabilities difficult to understand and to identify' (Phahlamohlaka, 2008, p. 104).

Terrorists, spies, hackers and other non-state actors can, relatively easy, access and offensively use Internet Communicational Technology to support their causes and acts and on that way easily pose as threats to national security of any state. Internet networks and the computers democratize access to information and knowledge. 'Malicious hackers, virus and worm writers, identity thieves, terrorists, and transnational criminal organizations reach easily across state borders to threaten individual citizens, economic infrastructure, firms, and government operations themselves' (Herrera, 2006, p. 78) has become tools of asymmetric war. Contemporary terrorists are not depending on their headquarters. It is not important of how far away is the terrorist head; it is easy to act if they know their final goals, their common enemy. Tactics, training and procedures are available with one click on Internet. In the globalized world, even big and powerful states do not guaranty invulnerability because becoming a part of global network states become more vulnerable than before.

The population of the big cities, strategically important energy resources, informational systems that support the life of a modern state, the transportation means, tourist and banking infrastructures of the worldwide countries are only a part of the target list of attacks that have already happened and may happen in the future again. Al Qaeda and organisations, which shares the same ideology, are conducting attacks on the global level by unprofessional combatants led by an ideological and religious view, acting as individuals or groups, attacking civilians and businesses. 'War on terror', in Afghanistan and Iraq did not stop the terrorists, instead, it helped them. It inflamed 'Third world' society's passion and increased terrorist moral, recruiting power, support and ability to act within the international arena.

Conclusion

Globalization as one of the most important processes of the world development is seen as integration of the world's economies. It tends to promote western common values, economy, democracy, culture and better way of life. Nevertheless, this paper shows its dark side as a conflict generator in the world. This process strives to

change lives, culture, and tradition by shaping the world toward 'the global village'. Even though, this process is not welcomed by others, by the rest of the world by those who see globalization as Americanisation or Westernisation. As the destabilizing factor of global security, globalization encroaches into very sensitive cultural and religious domain, awakening Islamic neo-fundamentalism and terrorism. An ideological tool of world's industrialized power centres; globalization is imposing global hegemony over non globalized world. Instead to be welcomed it is rather seen as a return of western neocolonialism and hegemony in the Middle East and North African countries.

Crossing the lines which divide the civilisations and different cultures were always challenging, causing failure to respect the right to be different. Globalization is provoking more and more conflicts among global actors. Especially represents impact on the culture and religion among civilisations arousing conflicts and decreasing international security. It is clear that the bleary process gives the large share in the global insecurity and causes asymmetric conflicts. Globalization became the large part of the problem for global security. This unstoppable process leads the world to new merciless conflicts. In countering global conflicts in the future the biggest challenge will be to provide that ordinary lives continue and after all, protection of ordinary people lives in this ruthless process.

Bibliography

Amin, S., 1997, *The future of global polarization*, In: J.D. Schmidt, J. Hersh, 2003, *Globalization and Social Change*, New York: Taylor and Francis e-Library.

Coker, C., 2002, *Globalization and Terrorism* [online] Available at: <http://www.g8.utoronto.ca/conferences/2002/tokyo/cocker.pdf>

(Accessed 10 December 2015)

Coker, C., 2004, *Globalization and Insecurity in the Twenty-First Century: NATO and the Management of Risk*, Oxford: University Press.

Giddens, A., 1990. *The Consequences of Modernity*, Cambridge: Polity Press

Griffel, F., 2003, *Globalization and the Middle East: Part Two*, [online] Available at:

<http://yaleglobal.yale.edu/content/globalization-and-middle-east-part-two>

(Accessed 10 December 2015)

Herrera, G., 2006, *New Media for New World? Informational Technology and Threats for National Security*, In: J. Kirshner, 2006, *Globalisation and National Security*, Florence: Routledge.

Hoffman, S., 2002, *Clash of Globalizations*, [online] Available at: http://www.cfr.org/history-and-theory-of-international-relations/clash-globalizations/p4763__ (Accessed 20 February 2016)

Huntington, S., 1993, *The Clash of Civilizations?* [online] Available at:

<https://www.foreignaffairs.com/articles/united-states/1993-06-01/clash-civilizations> (Accessed 25 February 2016)

Jones, A., 2006, *Dictionary of Globalization*, Cambridge: Polity Press.

Lafraie, N., *Afghanistan, the 'War on Terror' and the Continuing Quest for Security* In: R. Patman, 2006, *Globalisation and Conflicts, National security in a New Strategic Era*, London and New York: Routledge.

Lerche III C.O., 1998, *The Conflicts of Globalization*, [online] Available at:

http://www.gmu.edu/programs/icar/ijps/vol3_1/learch.htm (Accessed 23 February 2016)

Kirshner, J., 2006, *Globalization and National Security*, Florence: Routledge.

LeVine, M., 2002, *Muslim Responses to Globalization*, [online] Available at: https://openaccess.leidenuniv.nl/bitstream/handle/1887/16788/ISIM_10_Muslim_Responses_to_Globalization.pdf?sequence=1

(Accessed 05 January 2016)

Lynch, M., 2006, *Globalization and Arab Security* In: J. Kirshner, 2006, *Globalisation and National Security*, Florence: Routledge.

Phahlamohlak, J., 2008, *Globalisation and National Security Issues for the State: Implications for National ICT Policies* In: Avgerou C. and others; *IFIP International Federation for Information Processing, Volume 282; Social Dimensions of Information and Communication Technology Policy*, Boston: Springer.

Poku, N., Therkelsen, J., 2013, *Globalization, Development, and Security* In: A. Collins, 2013, *Contemporary Security Studies*, 3rd ed. Oxford: University Press.

Pollard, N., 2002, *Globalization's Bastards: Illegitimate Non-State Actors in International Law*, [online] Available at:
<http://www.tandfonline.com/doi/abs/10.1080/0966284042000279009>
(Accessed 10 November 2015)

Rubin, B., 2003, *Globalization and the Middle East: Part One*, [online] Available at:
<http://yaleglobal.yale.edu/content/globalization-and-middle-east-part-one>

(Accessed 05 January 2016)

Stepanova, E., 2008, *Terrorism in Asymmetrical Conflict (SIPRI Research Report No. 23)*, Oxford: University Press [online] Available at:
<http://books.sipri.org/files/RR/SIPRIIR23.pdf> (Accessed 13 December 2015)

Write, R., 2002, *A Real War on Terrorism*, [online] Available at:
http://www.slate.com/articles/news_and_politics/the_earthling/features/2002/a_real_war_onterrorism/does_globalization_cause_terrorism_or_cure_it.html
(Accessed 07 February 2016)

Is network theory the most suitable for understanding terrorist radicalisation?

MAJ Mari Cecilie Tolfen Reinskou

Introduction

Is network theory the most suitable for understanding terrorist radicalisation? Terrorist radicalisation has been broadly discussed in different research environments, and there are many different opinions about reasons why some people resort to such extreme acts of terrorism. In January 2015 the Kouachi brothers went into the satire company of Charlie Hebdo in France and killed 12 people, and in November the same year a group of terrorists killed 139 people in different attacks in Paris. There have been many terrorist attacks not only in European countries, but also around the world in general. It is not something new, but the globalisation and closeness to the media makes us more aware of the terror than earlier. Video transmission of terror attacks, photos of victims and terrorists are being showed almost daily in the media. A question to ask is why or how did these perpetrators turn into violent terrorists? It is not an easy answer or a clear understanding of why some people become terrorists, and some of them do not.

The purpose of this essay is to argue, by using different theories within the terrorism studies, that network theory is not the most suitable way to understand terrorist radicalisation, but that different theories in general supplement each. The way they supplement each other is because the researchers explore different aspects of radicalisation, use different methods, and the objects they study are also different. Some researchers focus more or less on different levels, such as individual level, group or state level. In the beginning I will clarify some terminology, introduce network theory, compare theories on the basis of different factors like understanding terrorist's background, and look at both internal and external factors that influence individuals. Further on I will compare the different theories on how well they explain the root causes for violent actions, and finally make a conclusion in order to answer the main question; Is network theory the most suitable for understanding terrorist radicalisation?

Terminology and structure

The word *terrorism* is not clarified properly within the area of research, and there does not exist a universally acceptable definition of the term. Because of that it is also challenging to agree on a unified *terrorist profile*, what kind of traits or characteristics are special for terrorists. One scholar, Walter Laqueur expresses in Kleinmann's book his understanding of the term terrorism as follows: 'many terrorisms exist, and their character changes over time and from country to country. The endeavour to find a *generic theory* of terrorism, one overall explanation of its roots, is a futile and misguided enterprise'(Kleinmann, 2012, p. 280). As Laqueur explains, there is not only one clear definition of the term terrorism. In one way we can look at terrorism as *activities*, asymmetric attacks from violent radical groups or individuals in order to accomplish a goal. In some discussions one can say that it is a poor man's weapon. One person alone, or together with others can cause huge disasters without a lot of resources. Terrorism is inexpensive and considered to be a simple method. One goal of terrorism is to change the environment, and terrorism uses means like deterrence and destruction in order to accomplish that. The sadness is that in many ways deterrence is working. An example is the polarisation and protectionism happening in Europe and other countries.

In this essay I will use sources and theories based on studies of global Salafi Jihad, other social movements and use findings that focus more into the psychological aspects. Salafi Jihad is considered to be Islamic extremism associated with Wahhabism and Salafism, but the latter two directions do not support terrorism (McCauley and Moskalenko, 2011, p.5). The Jihadists use violent actions in order to spread and turn the environment back to what the persons think is *true* Islam. The consequence of their beliefs is that everyone else, having another opinion or belief is regarded as enemies. The challenge is that the movement is global, and as mentioned earlier violent attacks can happen all around the world. The essence in the social movement is that some people sacrifice themselves for a greater good, in a belief that is more important than the person him/herself.

In order to study terrorism one need to look at the process of becoming a terrorist. Radicalisation can be seen as a process, where a person or a group is becoming convinced that their belief and values are the superior one, and that they have to

change the status quo in order to achieve this new status or environment. It is useful to make some distinctions between radicals; those people holding radical ideas, and violent radicals, those holding radical ideas and turn their beliefs into violent actions. Some even have the opinion to see radicalisation as the *pathway* to terror. In this essay radicalisation will be understood as violent activities, such as terrorism. In Scott Kleinmann's book, terrorism expert Peter Neumann expresses violent radicalisation as; 'changes in attitude that lead towards sanctioning and, ultimately, the involvement in use of violence for a political aim' (Kleinmann, 2012, p. 282).

Network theory

The network theory approach is mainly a study of social networks, which provides a distinctive focus on social relations such as patterns of relationships. It can be studied how these patterns of network ties can be linked to other patterns of network, and can be analysed to find patterns of how decision-making is happening within a group or network (Kilduff and Tsai, 2003, p.19). The approach includes studies of the connections and influences within different structures like terrorist networks, such as researcher Marc Sageman's studies. Some researchers criticise network theory for being a collection of methods and that it contains or borrows other theories such as statistical comparison theories and psychological theories (Kilduff and Tsai, 2003, p.37). Network theory has been shifting the level of analysis from the established hierarchical group to *horizontal networks*. The study concentrates more on horizontal rather than hierarchical ties (Pedahzur and Perlinger, 2006, p.1989). Traditional hierarchies are based on a top-down management, while networks are decentralized with decision-making and action dispersed among multiple actors. These actors may hold a high degree of local autonomy. Although hierarchy in a traditional sense is absent from the network, the boundaries between networks and hierarchies are not always clear-cut. 'Networks are never managed by a single central authority' (Eilstrup-Sangiovanni and Calvert, 2008, p.12). Another criticism is from Anja Dalgaard-Nielsen. She states that the scholars of network theory or social networks lack real explanations, because they do not gain access to individuals personally involved in radical groups. Her opinion is that the network researchers rely on interview objects like community leaders and outcome from other person's interviews, like social workers in the field (Dalgaard-Nielsen, 2010).

Terrorist's background

Looking into the substance and explanations of understanding violence, it is true that the explanations concerning why some people use violence has become a controversial topic, particularly among researchers in the area. Many researchers have various theories as to why some people resort to violent activity, such as terrorism. The root causes to become violent have been discussed for years, from earlier to include explanations like poverty, trauma, ignorance and madness, the understanding that only *mad* people are capable of taking another person's life (Sageman, 2004, p. 80). Network theory and the study of social networks offer an important insight into understanding the radicalisation and recruitment process in general, and especially how young Muslims around the world join these networks. The theory has a focus on *who you know*, and underline the importance of group processes and socialisation. Sageman and another scholar Wiktorowicz advocate that the social networks are the ones that transmit radical ideas, and that violent radicalisation takes place within smaller groups, where bonding, peer pressure, and indoctrination gradually change the individual's view of the world (Dalgaard-Nielsen, 2010, p. 801). Marc Sageman provides a good overview of the different terrorist networks around the world, and explains the power and compulsion that exist within a group. On the other hand the theory is limited in explaining why they use violence in order to accomplish their goal.

Looking especially at the work of Sageman, we discover that among a study of 132 terrorists, over 60% had some kind of college education and the leadership which is represented by 80%, 20% of the leaders have doctorate degrees (Sageman, 2004, p. 75). It actually shows that these terrorists are more educated than average people worldwide, and that they often come from completely average family relationships, standards and economic security. Sageman also concludes that terrorists are surprisingly normal in terms of mental health (Sageman, 2004, p. 83). This research by Sageman surpasses the former explanations that some people become terrorists because of poverty and madness. Another researcher, Jitka Malečková also give the same explanation as Sageman when it comes to the statement that terrorists do not necessary come from a poor background. Malečková states that; 'One of the major criticisms of the inference that poverty is not a root cause of terrorism because

terrorists are less likely to come from impoverished background than their non-terrorist countrymen is that terrorists may act out of concern for their poor countrymen or other disadvantaged groups of population, not out of their own personal desperation' (Bjørge, 2005, p. 36). This statement can be understood that there is not anything wrong with their mental health, but can immediate show that they can have the ability to care for their own countrymen, those who believe in the same understanding of how the world should be like.

Even though here are still some scholars who explain that lack of opportunities and poverty still has a place among the potential causes of terrorist activities. In Malečková's conclusions she says that; 'research suggest that neither the participants nor the adherents of militant activities in the Middle East are recruited predominantly from the poor' (Bjørge, 2005, p. 41). Further on she also states that there is no evidence from her group's research on both individual and national level that there is any direct linkage between poverty and terrorism (Bjørge, 2005, p. 41). Her statements also add up and support Sageman's findings. A distinction between Malečková and Sageman is that Sageman lack the explanations in regards to different levels, while Malečková express the levels better in her studies.

The results from these arguments give us a picture that there has been a change of understanding when it comes to discussing the background of terrorists, their level of education, also mental health, that they do not act only because of poverty or madness. They can also act violently because they care for others who have the same belief and common understanding of what is important. On one hand the study of terrorist networks give us an understanding of the terrorist's background, that they come from educated societies, and that poverty in itself does not represent a main reason. Marc Sageman also explains how the group members share common social background, common psychological make-up, and a particular situation at the time of recruitment (Sageman, 2004, p. 69). The network theory is providing a good overview of statistical information, but on the other hand it is limited in seeing how some of the statistical information can give answers and it is useful to understand the radicalisation process.

Internal and external aspects

There are different ways to understand how individuals and groups become radicalised. Within the area of research there can be both internal psychological aspects within a person, but there can also be external factors like compulsion from outside, the society, other individuals or groups. Both scholars Sageman and Wiktorowicz focus on the power of small communicative communities to create shared worlds of meaning that shape identity, perceptions, and preferences. Wiktorowicz also explains the framing theory, which forms the individuals into collectivity. Network theory is more of a sociological theory and explains that radicalisation is a group process where extremist individuals radicalise other people within their social networks (Kleinmann, 2012, p. 280). According to the researcher Scott Kleinmann the network theory is only a part of understanding radicalisation process, and that there are other theories that can complement the overall understanding. Kleinmann refers to other theories like national cultural theory, which make a distinction between the individualists, who are more likely to attack their own people, and the collectivists who are more likely to attack *outsiders* to defend the in-group. Another direction, which he mentions, is; 'that people who live in violent regions and who witness terrorism regularly may seek to imitate terrorists or learn from a culture that glorifies terrorists' (Kleinmann, 2012, p. 280). One of the main arguments within network theory is the compulsion and power that happens within the terrorist network groups, the social bonding and the influence between the group members are external factors that influence each member over time. Network theory explains that the decisions to act violently lie within the group, as group decisions, not as single member's decisions. Another theory, the I3M by Kirkpatrick and Schneider provides a more generic theory, which can be used on all different actors. It makes a framework, which contains both external and internal factors. The I3M model's main factor is *mobilisation*, which means how a person or a group act and support the social movement. For a person to be become mobilized there are three main facilitators; (1) *Identification* with the group, (2) *indoctrination*, how individuals get influenced to join the group and the last one is (3) *interest*, which is the curiosity for the movement. Underneath there are three incentives that trigger the person on physical, emotional and ideological ways through the facilitators (Kirkpatrick and Schneider, 2013, p. 24). This model provides a good overview and includes several

factors, both internal and external factors that provide a more complete picture when analysing. Network theory has a lot of its focus on external factors, especially group compulsion in order to explain the radicalisation and decision-making process, but it immediately seems to lack the individual internal aspects, like motivation and incentives.

Scott Kleinmann determines the understanding of radicalisation into three levels. The first one is the; (1) *individual-level*, those that address internal forces which only directly affect the person who is radicalising; (2) *group-level*, which include top-down social movement and horizontal social-network recruitment; and (3) *mass-level*, which argue that societal forces or strains that affect large populations are radicalising mechanisms. Kleinmann's understanding is that by; 'categorising radicalisation theories in this manner allows for comparison within and across disciplines' (Kleinmann, 2012, p. 280). Other theorists that search for answers about the radicalisation process are McCauley and Moskaleiko. They explain different root causes to violence, both at individual, group and mass level. In their studies one of their findings is that sometimes the decision to act violently appears to be a personal one, often triggered by an individual crisis in that person's life. It can be based on personal psychological aspects, such as grievances, insults, being an *out-sider* in the society, not being understood, or not being loved (McCauley and Moskaleiko, 2011). This theory goes more into explaining the depth of what happens on the individual level, and it shows that it can come from inside of a person, not necessarily from outside compulsion. To sum up the last examples from other theorists the network theory focuses more on external factors rather than inherent psychological characteristics or socioeconomic deprivation to understand violent radicalisation. The empirical background conclusions on network studies can be understood as limited, since they do not contain comparisons between different motivations and incentives at the individual level, nor make a distinction between radicalisation processes happening on different levels. In order to get a better understanding of terrorist radicalisation it is important to see the process that happens on different levels of the society. Individual aspects to act violently are something McCauley and Moskaleiko have a better overview of in their studies, especially talking about the example concerning individual crisis as a trigger. Kleinmann's understanding of three levels of

radicalisation, I3M model with its different factors, hereby both external and internal factors can complement network theory.

Root causes and identity

Among scholars there seems to be a common opinion that there is no single root cause of terrorism. Even though there can be many different causes, it is not a reason for stop searching for different explanations. As mentioned, McCauley and Moskalenko's research provides good explanations about individual, group and mass radicalisation. One of their main factors is grievance, which you can find on all three levels. Another researcher and film producer, Deeyah Khan has studied Brits who become religious fighters, but later on were rebuilt; they left the status of being jihadists and later started to prevent others from joining the terrorist networks. One female tells her story about when she was raped in Britain. She went to the police, but the case lacked evidences and was closed down. She was not supported, the perpetrator was not prosecuted and she did not get any form of reconciliation. The woman became angry, especially towards the government. She searched for support and solutions, and wanted the perpetrator to be punished. As a part of that rejection she was not heard, neither understood and became radicalised. She said that in that *new* society perpetrators were punished within the system (Khan, 2015). Another example of grievance is also underpinned by the actions taken by the Black widows of Chechnya. Their way of sealing revenge for their own experience of rape, but also deaths of husbands, brothers, sons at Russians hands (McCauley and Moskalenko, 2011, p.16). The reaction for revenge or justice can be against an individual or against a whole group. From these examples one of the triggers to become violent can be the anger that appears of not being heard or understood, when a terrible crisis appears. McCauley and Moskalenko explain it as follows; 'harm to self or loved ones can move individuals to hostility and violence towards perpetrators' (McCauley and Moskalenko, 2011, p. 13). Another scholar who studied Islamic radicalisation in Western Europe, Syed Mansoob Murshed identifies that also group grievance can be turned into individual grievance. He argues that; 'low social standing may encourage individuals to abandon their primary identity in favour of other, less frowned upon, identities (Murshed, 2011, p. 265). Murshed in his conclusions explains that; 'political

and economic inequalities suffered by Muslims, both worldwide and within Europe, are central to the formation of their collective grievances. Evidence from the country-based profiles further shows that discrimination against Muslims is rife, leading to conditions that are ripe for political mobilisation' (Mansoob Murshed, 2011, p. 275). The same aspects here mentioned is also represented in Khans documentary where young Muslims in Britain get angry at the government and the society because they feel constantly watched, accused, suspected, feel as outsiders, and are not able to find their identity. In Scott Kleinmann's work you find the same arguments; 'joining a terrorist movement offers an *identity stabilizer* for people with low self-esteem or for those who, as excluded minorities, are searching for belonging as a way to consolidate and defend their identity' (Kleinmann, 2008, p. 280).

Not all persons who become terrorists are connected to a network; an example is the white male Anders Behring Breivik who killed 69 persons in Norway because he had a different view on how the environment should look like. It is though stated that he is not mentally ill, and therefor he got convicted. He might share same opinions as others, or other groups, but there were not any clear linking that he was integrated in a network. Another discussions in this case is how you categorize and see his actions, are they an act of terrorism or as a mass murderer? Since there is no clear common definition of terrorism it can be difficult to distinguish and categorize the activity.

Looking at the root causes and to understand violent radicalisation there are theories that revolve around case-study approaches that a more nuanced view of the different motivations and trigger factors that can lie within different individuals. In these studies there are researchers who look at cases across Europe, like Petter Nesser. He explains and shows that the socioeconomic profiles of individual members vary widely. Besides this he also discovers and identifies a limited number of personality types or roles within terrorist groups. These personalities have different roles and play different parts also in the recruitment process and decision-making process (Dalgaard-Nielsen, 2010). On the one hand network theory provide many factors to how people join the terrorist networks, but somehow lack further explanations as root causes to violent actions. On the other hand theories presented give more knowledge about root causes such as grievances on individual, group and mass level, individual crisis as a trigger, feeling as an out-sider of the society and not able

to find an identity. As already mentioned, not all terrorists are necessarily connected to a network either, and these individual terrorists also need to be studied.

Conclusion

Is network theory the most suitable for understanding terrorist radicalisation? In general the answer is no. The network theory itself does not give a clear answer to why some people turn into violent actions, especially on the individual level. Though the theory is providing a good overview of statistical information, such as the network itself, the connections between different individuals, terrorist's background such as their level of education. It gives a good overview of the relations between the individuals and explains the group compulsion and the recruitment process. On the other hand it is limited in how to identify the root causes in order to understand the radicalisation process.

Also the empiric background conclusions on network studies can be understood as limited, since they do not contain comparisons between different motivations and incentives at the individual level, nor does the theory distinguish the different levels within the radicalisation process. As mentioned network theory does not explore the root causes or triggers of violent actions thoroughly, or make a clear distinction between into internal and external aspects that influence a person. Elements about individual aspects to act violently are something McCauley and Moskalenko have a better overview of in their studies, especially the example about how an individual crisis can be a trigger for violence, and also their explanations of grievances on different levels. Kleinmann's three levels of radicalisation and the I3M model's can complement the network theory in offering a more structured analysis. The I3M model gives a good overview, because it provides different facilitators and incentives, which can be used on both individuals and groups. The model also includes triggers that can develop from both internal and external factors. The physiological incentives can be related to individuals, and manipulation as facilitator can be related to group.

As final comments, all the different theories available use different sources, studies different levels and areas of why some people become violent terrorists. It is rather

difficult to provide only one theory that provides all the correct answers. Looking at all these different theories it seems like they need to be studied individually, but also be compared to each other. The final argument is that the theories need to be looked upon as complementary to each other, as they concentrate on different levels of analysis. Even though network theory does not fulfil the main explanation of terrorist radicalisation, it is useful in a broad context, especially to drive mapping of terrorist networks in general. The analysis can locate both informal and formal leaders, who are essential for the networks survival and decision-making process. The information drawn from the network analysis can provide results, which are essential for counter terrorism. Further research and theories on terrorism might give or draw better links between the already mentioned theories. The findings from research will change, because the environment change, terrorism change and so do the terrorists.

Bibliography

Bjørge, T. 2005. *Root Causes of Terrorism*. Routledge, Taylor and Francis Group. London and New York.

Coolsaet, R. 2011. *Jihadi terrorism and the radicalizations challenge. European and American Experiences*. Farnham: Ashgate.

Dalgaard-Nielsen, A. 2010. *Violent Radicalization in Europe: What We Know and What We Do Not Know*. *Studies in Conflict and Terrorism*, Vol.33, pp. 797-814.

Della Porta, H. 2012. *Patterns of radicalization in political activism*. *Social Science History*, 36:3, pp. 311-320.

Eilstrup-Sangiovanni, M. and Calvert, J. 2008. *Assessing the Dangers of Illicit Networks: Why al-Qaida May Be Less Threatening Than Many Think*. MIT Press.

Karagiannis, E. 2012. *European converts to Islam: Mechanisms of Radicalization*. *Politics, Religion and Ideology*, Vol.13, No.1, pp. 99-113.

Kirkpatrick, J. and Schneider, M. 2013. *I3M Interest. Identification. Indoctrination. Mobilization.*

Kilduff, M. and Tsai, W. 2003. *Social Networks and Organizations: Is There Social Network Theory? A Critical Examination of Theoretical Foundations.* London: Sage Publications Ltd.

Kilduff, M. and Tsai, W. 2003. *Social Networks and Organizations: Understanding Social Network Research.* London: Sage Publications Ltd.

Kleinmann, S. 2012. *Radicalization of homegrown Sunni militants in the United States: comparing converts and non-converts' in Studies. Conflict and Terrorism.* Vol. 35, pp. 278-297. Routledge.

McCauley, C. and Moskalenko, S. 2013. *Friction. How radicalization happens to them and us.* Oxford: Oxford University Press.

Murshed, S. M. and Pavan, S. 2011. *Identity and Islamic Radicalization in Western Europe. Civil Wars,* Vol.13, No.3, pp. 259-279.

Pedahzur, A. and Perlinger, A. 2006. *The Changing Nature of Suicide Attacks – A Social Network Perspective.* Oxford University Press.

Sageman, M. 2004. *Understanding Terror Networks.* Philadelphia: University of Pennsylvania Press.

Documentary movie

Khan, D. 2015. *Jihad: A Story Of the Others.* Norwegian-English Documentary. Fuuse Films.

The Russian A2/AD capabilities in Baltic Sea region: are they existential threat to the defence of Baltic countries, or another buzzword?

MAJ Klaus-Jürgen Kaivo

'The success of any major operation or campaign depends on the free movement of one's forces in the theatre. Without the ability to conduct large-scale movements on land, at sea, and in the air, operational warfare is essentially an empty concept.'

-Dr. Milan Vego

Introduction

Recent statements in media and also in official meetings from NATO top generals and politicians concerning Russia's emerging Anti Access and Area Denial (A2/AD) capabilities in Baltic Sea, Black sea and Syria have highlighted the importance of the issue to NATO and especially to three Baltic States. In interview to Defence News NATO Deputy Secretary General Alexander "Sandy" Vershbow stated

The things that worry us the most are their anti-access/area-denial [A2/AD] capacity — the Bastion defence system capability that they are building up in the high north in Murmansk, the Kola Peninsula, in Kaliningrad and in the Black Sea, and potentially now in the eastern Mediterranean — as potentially impeding and complicating NATO reinforcements and other NATO operations.

Same message was reinforced by US Air Force (USAF) General Frank Gorenc, the commander of US Air Forces in Europe and Africa, who stated in Air Force Association's annual symposium last year that he is particularly concerned about two A2/AD zones - Crimea on the Black Sea and Kaliningrad on the Baltic Sea

This essay will argue that Russia has strong A2/AD capabilities around Estonia, Latvia and Lithuania and these capabilities can strongly hinder NATO operations in Baltic Sea area. In other hand, NATO has robust counter- A2/AD capabilities and can

probably mitigate and overcome A2/AD threat from Russia. In the end the essay will answer to the main question- Are the Russian A2/AD capabilities existential threat to the defence of three Baltic countries.

The main body of essay consist of 3 parts. The 1st paragraph describes theoretical and historical background of the Anti-Access and Area Denial concept. The 2nd part deals with Russian armed forces A2/AD capabilities. Third part focuses on NATO counter-A2/AD capabilities. In the last part the essay will argue whether NATO is able to defend Baltic countries in Russian robust Anti-Access/Area Denial environment or no.

Theoretical and historical background of the Anti-Access and Area Denial concept.

Throughout the history of warfare, enemies have regularly attempted to deny one another freedom of movement on the battlefield. Past forms of anti-access served to both protect friendly forces and prevent enemies from gaining positions of advantage.. Well known historical examples of systems built to deny adversaries freedom of movement on the battlefield are the Great Wall of China and the Maginot Line in France. As technologies emerged, the domains to deny opponent also increased, to include combination of information, space, sea, and air denial.

When the German navy attempted to use U-boat attacks to interdict American ships in the North Atlantic during World War II, they were executing an anti-access strategy. During the Vietnam War, U.S. attempts to interdict the Ho Chi Minh trail, although equally unsuccessful, were an effort to deny the North Vietnamese access to the battlefields of South Vietnam. During the Cold War Soviet Union developed navy and capabilities to stand against US supremacy in aircraft carriers and force-projection capabilities they provided. Soviet navy was sea-denial organization, meant to destroy US carrier groups, but not for control of sea regions beyond immediate areas close to land (the Barents sea, the White Sea, the Black sea and the Sea of Othotsk).

After the 1991 Gulf War and US superiority in every aspect of battle space, big countries, like China and Russia started to think how to counter the technological superiority of US. China developed a counter-intervention strategy and associated

reconnaissance-strike complexes aimed not at controlling the airspace, waters and electromagnetic spectrum in areas surrounding China but, rather, at denying the use of those domains to opposing forces. Most known capacities from this strategy are anti-satellite warfare and development and deployment of hypersonic long range DF-21 anti-ship ballistic missile. Due the economic reasons Russia was unable to significantly research and field new A2/AD equipment until Mr Putin's coming to power and deep funding increase to armed forces budget.

To counter China's new and powerful A2/AD capabilities, USA military developed the concept of Air-Sea Battle, designed to assure access to parts of the 'global commons' – those areas of the air, sea, cyberspace and space that no one 'owns,' but which we all depend on – such as the sea lines of communication in contested situation where adversary has military capabilities include new generations of cruise, ballistic, air-to-air, and surface-to-air missiles with improved range, accuracy, and lethality, quiet modern submarines and stealthy fighter aircraft complement new naval mines equipped with mobility, discrimination and autonomy. Both space and cyberspace are becoming increasingly important and contested. In year 2015 the framework of Air-Sea Battle was re-conceptualized as Joint Operational Access Concept, to emphasis need for joint approach versus only air and sea.

During research the author was unable to find meaningful information about Russia's overall Anti-Access/Area Denial doctrine or concept. This does not mean that such a concept does not exist, as Russia is employing or exporting Anti-Access/Area Denial capabilities all around the world, Crimea and Syria the latest example. According to Alcazar It is not known if Russia's doctrine is explicitly built on A2/AD, but indications in recent years suggest it has a good grasp of A2/AD (Alcazar, 2012) According to Moscow's new Maritime Doctrine to 2020, published year 2015, Russian Navy will adopt of "asymmetric means of warfighting" and the "art of sea denial", what translates into the build-up of an "arc of steel" between the Arctic and the Mediterranean, via the Baltic and Black Seas, resembling China's Anti-Access/Area Denial (A2/AD) approach to the South China Sea .

Research and discussion from Europe is limited and mostly focuses on reiterating the thinking and concepts from USA armed forces, stipulating the importance of power projection and expeditionary operations to NATO as a whole .

Anti-Access (A2) is defined by Centre for Strategic and Budgetary Assessment as adversary capabilities, actions which impede (preclude, prevent, mitigate) the movement of US forces to their desired locations (war-fighting positions, staging locations, etc.) Area Denial (AD) is adversary capabilities which impeded the free movement of US forces within the employment envelopes of maximum effectiveness, efficiency, or advantage to US forces . This definition is of course USA centric, but can be modified to .meet NATO needs. Simply put anti-access (A2) strategies aim to prevent NATO and its allies forces entry into a theatre of operations, area-denial (AD) operations aim to prevent their freedom of action in the narrow confines of the area under an enemy's direct control. Another definition is provided by former US Navy officer and author Sam J Tangredi

the objective of an anti-access or area denial strategy is to prevent the attacker from bringing its operationally superior forces into the contested region or to prevent the attacker from freely operating within the region and maximizing its combat power .

If one considers Estonia, then Anti-Access activity from Russian Federation side is to deny through Integrated Air Defence Systems the deployment of airborne troops from Very High Readiness Joint Task Force to Ämari or Tallinn airport. Area Denial activities would be actions like cyber-attacks against command and control system and cruise missile attack against in staging areas inside Estonia. The line between Anti-Access and Area Denial is not set into stone, and usually the weapon systems and platforms are same. Usually two terms are mixed together in one term, written as follows: Anti-Access/Area Denial (A2/AD). Some authors argue, that Anti-Access/Area Denial is nothing new, it's been around hundreds of years and is not worth separate term and A2/AD warfare is simply warfare . Modern A2/AD differs from historical iterations of anti-access due to the combination of increased range, accuracy and lethality of adversaries advanced, networked weapons systems.

Russian armed forces A2/AD capabilities in Baltic Sea region.

During the last ten years Russia military-industrial complex has heavily invested money and time to develop and field long-range Anti-Access/Area Denial capabilities. Nowadays, according to majority of experts, Russia is no longer a weak power in

terms of deployment of advanced long range Anti-Access/Area Denial capabilities in Kaliningrad or near Baltic states eastern borders, having the potential to neutralize NATO's defence in-depth posture by keeping at bay its reinforcements or cutting the access to the Baltic Sea, thus generating a huge deterrence and freedom of movement problem for NATO .

In this paragraph I cover the main long-range Anti-Access/Area Denial capabilities owned by Russian Federation armed forces. Some of the capabilities are dual use, some like modern air defence systems Redut and Vitjaz are still in development. In other hand, in short to medium timeframe these systems will be fielded and deployed to ships in Baltic Fleet and air defence units in western military district.

Firstly, the main threat to NATO air forces are Integrated Air Defence Systems in Kaliningrad region, Baltic Fleet and units belonging to Russian-Belarusian joint regional air defence system near Estonian, Latvian and Lithuanian eastern border. With range up to 400 kilometres, S-400 SA-21 "Growler" air defence system can close the whole airspace Estonia, with the batteries physically locating still in Russian side of river Narva. From western side of operations area batteries in Kaliningrad can kinetically influence airplanes as far as Poznan. Complimented by older and lesser range S-300 SA-10 Grumble and newest Pantsyr-S1 (SA-22 Greyhound) the Integrated Air Defence Systems could close Baltic Sea until Bornholm and Gulf of Finland fully, pending the Baltic Fleet modernization effort. Supported by modern *Krashuka*-class jammers used against NATO Intelligence, Surveillance, Target Acquisition and Reconnaissance assets and Airborne Warning and Control System aircrafts and, simply speaking, leaving NATO combat airpower into informational darkness. If needed, anti- satellite capabilities are available to neutralize NATO surveillance, detection and reconnaissance capabilities, in the same time utilising own space assets together with robust and effective cyber warfare capabilities Supporting all these capabilities are land forces short and medium range mobile organic air defence assets, to engage all threats that penetrated higher level air defence systems.

Secondly, the capabilities threatening the NATO fleet operating in Baltic Sea. Newest anti-ship missile K-300P Bastion-P, with range up to 300 km, is the most formidable asset in Russian coastal defence forces inventory. If Russia is to occupy islands of

Bornholm and Gotland, the K-300P could close the Danish Straits to NATO or US Navy ships, denying access and reinforcement to Baltic States . Baltic Fleet with its modern *Steregushchy*-class corvettes and diesel submarines is not as formidable as Northern or Pacific fleets, but still foe to acknowledge. Supported by Kaliningrad based fighters, bombers and rotary wing assets the fleet's main mission is coastal defence and has capabilities to deny smaller nations shipping and naval activities. Due to the shallow depth of the Baltic Sea naval operations by large vessels groupings, particularly a U.S. navy carrier task force, are also limited.

Thirdly, the capabilities threatening NATO reinforcements to Baltic States through Suwalki Gap, the only land link between Estonia, Latvia, Lithuania, and the other NATO countries. This 60 miles long small piece of land between Kaliningrad and Belorussia can be denied by 3 brigades (some sources state that there is only two brigades) plus supporting arms units from Kaliningrad side and supporting attack from Belorussian side, factually stopping all land traffic and cutting Baltic states off from access to Europe . This force can be reinforced by Air Bridge from the mainland Russia in 24 to 48 hours, delivering approximately 10000 lightly armed troops with supporting light artillery to Kaliningrad airfields. Supported by heavy artillery and air strikes, and if needed, by precision strikes by Tochka-U tactical ballistic missile against high value targets. Together with naval and air defence activities Russia has capability to deny reinforcements, air support and heavy forces deployment from Germany or Poland to help Baltic States delay and stop Russian Federation attack from east, so fulfilling the Anti-Access/Area Denial operation.

Fourthly, the ballistic missile and cruise missiles strike capability against medium and long range targets. Iskander-M has a range of 400 kilometres and is nuclear-capable. Used to strike high value targets with conventional or special warhead, the platform serves also as deterrence and anti-escalatory capability. If armed with nuclear warhead, it should prevent NATO to overrun units engaged in Suwalki Gap, as there is no political will from NATO political side to escalate conflict to nuclear exchange between adversaries. Some analysts argue, that A2/AD is only applicable to a limited conflict, because the risk of escalation (particularly nuclear) would make any cost-benefit analysis useless . Complementing this capability is Iskander-K cruise missile with range about 1000 kilometres and Kalibr multipurpose cruise missile with range up to 2500km. Naval version of Kalibr to Baltic fleet is planned in medium term .

Together with air launched cruise missiles from Russian Aerospace Forces Long Range Aviation aircraft , namely Tu-160, Tu-95 and Tu-22M3, this capability gives Russia armed forces possibility to strike targets deep inside Western-Europe and Scandinavia from different directions and different altitudes, making defence against attacks complicated.

NATO Counter-A2/AD capabilities in Baltic Sea region.

The analysis of the threat from Russia's Anti-Access/Area Denial capabilities and NATO possible response can be put into several perspectives, like strategic perspective, operational perspective, military and industrial perspective, bureaucratic perspective and political perspective . Due the limited amount of space, the author will cover operational perspective, and only from Baltic Sea region standpoint.

One of the main concerns for NATO in Baltic States is hybrid warfare type of scenario, where the actions of Russian forces are below Article 5 activation threshold. If Russia can enter to one or multiple Baltic States without provoking alliances prompt response and the same time activating all Anti-Access/Area Denial capabilities in region, NATO is unable to react fast enough, and faces a fait accompli as the territorial integrity of member or members of alliance is violated and territory occupied. To prevent this to happen, different measures must implemented by SACEUR. First, better intelligence sharing between nations, NATO structures and other partners, including internal, is a must. To have correct indicators and warnings for detecting and assessing possible hostilities from east more comprehensive approach into intelligence data, sensor images and also to products is needed. Without correct intelligence sharing is almost impossible to figure out reasons and intentions behind another 100 000 plus "snap exercise" near Baltic States borders.

Since the NATO Summit in Wales some NATO members have sent their troops to Baltic States bolstering NATO forward presence to ensure that any Russian attack will be met with resistance by troops of all 28 NATO nations, so increasing the political cost of any such attack to an unaffordable political level. NATO troops would be a "tripwire", ensuring adequate response from all alliance members. So far this plan has not been fully implemented, as some nations are hesitant to anger Russia more than absolutely needed.

Plans to deploy US armour and heavy equipment back to Central and Eastern Europe is also a strong signal to Mr. Putin. According to Military Times, the European Reassurance Initiative budget for year 2017 is \$3.4 billion, or \$ 2.6 billion more than this year, and will incorporate brigade size unit with pre-positioned war stocks and modern, well-maintained combat vehicles and other gear prepared for full-scale operations . This is start, but only for a year, and pending the political situation in US could easily be reversed. Together with Baltic national and other deployed NATO forces this initiative is probably minimal to deal with hybrid, or “little green man” type of scenario. On the other hand, one of the biggest mistakes from military history is to prepare for old type of conflict and not look into possible new scenarios, so for example saturation attacks by cruise missiles or defence from Chemical, Biological, Radiological or Nuclear agents should be considered,

To counter Russia’s hybrid and conventional Anti-Access/Area Denial capabilities in short, medium and long term perspective, NATO has to focus on taking all the necessary measures to promote, develop, deliver and implement interoperable military capabilities and in the same time NATO nations to acknowledge that the Alliance’s superiority in a number of domains could be challenged. Air superiority is one key example. Also are mobility and rapid deployment of troops and equipment across the Alliance . Operation Unified Protector showed clearly that NATO as alliance relies too heavily onto US to provide critical counter-Anti-Access/Area Denial mission capabilities, like Suppression of Enemy Air Defence, Electronic Attack and Air-to Air Refueling . There is a inherent risk that if US is involved in conflict with some other global power, like China , other NATO members are unable or unwilling to destroy the Russian advanced Anti-Access/Area Denial capabilities in Baltic Sea region. Even when US is fully involved and will bring to the table stealth planes F-22 and B-2 with precision or standoff munitions, it takes time to clear the way for airborne reinforcements needed to stop possible attack from the east. Other capability lost to NATO in case of Anti-Access/Area Denial operation with Russia is the use of non-stealthy cruise missiles like US Navy’s Tomahawk, widely used in conflicts before, because S-400 SA-21 is believed to have credible capability against them. In this contest is really worrisome that to deploy VJTF alone and by air to one of the Baltic Countries airbase would require 450 flights by C-17 heavy strategic transport aircraft .

One of the least talked topics in Anti-Access/Area Denial situation in Baltic Sea region is nuclear issue. Russian Nuclear Deterrence Policy states concept of nuclear de-escalation. According to research made by University of Copenhagen 'nuclear de-escalation means the use of tactical (sub-strategic) nuclear weapons should a local war escalate into a regional war' . What is the NATO nuclear-capable nations position on use of the nuclear weapons, are they willing to deploy the tactical nuclear weapons closer to the Baltic states as deterrent against the Russia and are we, Baltic states, willing to take responsibility for nuclear exchange in our countries, even if this gives us back our freedom. This question has to be debated in highest levels of NATO, and if consensus is reached, communicated to all parties. It's all about NATO's credibility- are we willing to make tough decisions to deter Russia, and do we have capabilities to fulfil the decision made.

Last part of this paragraph is going to shortly investigate the usefulness of Baltic States national regular and National Guard /Home Guard units as counter- Anti-Access/Area Denial capability. Firstly we can perceive them as deterrent force, and with sufficient training, communications and weaponry they are able to fulfil this task. Of course, if we take to account budgets of our countries and size of population, they can be deterrent only together with NATO deployed forces and other enablers. Second and maybe more easily reached capability is to use them as counter-Special Forces (*SPETSNAZ*) units. As natives, who have good understanding of local geography and also can freely communicate with local population, they are able quickly and efficiently deny Russian Special Forces deep access to our respectful countries . Third area of interest should be defensive and offensive cyber warfare capabilities to counter Russian possible cyber-attacks and also target and inflict most damage to his capabilities. NATO is officially defensive organization, so the offensive capabilities development is great way to try Baltic cooperation in bi- or trilateral configuration.

Conclusion

The aim of this paper was to analyse Russian Armed Forces Anti-Access/Area Denial capabilities in Baltic Sea Region and compare them with NATO counter- Anti-Access/Area Denial capabilities, in order to determine impact to the defence of Baltic nations against possible Russian attack.

Russia has developed robust and comprehensive Anti-Access/Area Denial capabilities package inside Russian mainland and also in Kaliningrad area. Encompassing all domains (air, sea land, space and cyber) the threat from Anti-Access/Area Denial capabilities to NATO operations are big. Especially when NATO has to deploy forces to Baltic states after the first hostilities are commenced and all Access/Area Denial capabilities are fully deployed, activated and in full battle mode. From technological and sophisticated weaponry standpoint the most difficult capabilities to overcome are Integrated Air Defence Systems, anti-ship supersonic missiles and tactical ballistic missiles. Complementing these capabilities are powerful Electronic Warfare assets to blind and neutralize ISTAR and C2 aircraft, denying NATO the situational understanding in area of operations. The threat of nuclear escalation is also a big issue here, possibly making nations less decisive for directly countering Russia and its military forces.

From NATO side the counter- Anti-Access/Area Denial capabilities are available to nations, but the technological edge is lessening fast. This means that the effort and capabilities to overcome operational level problem will take more time, assets, troops, training, money and political will than before. For example, stealth-technology is available for only some of nations, in the same time Russia top end air defence systems are effective against non-stealth aircraft, making the Suppression of Enemy Air Defence campaign really complicated. Same can be said to naval deployment of NATO task groups into Baltic Sea. Due the relative shallowness of Baltic Sea and the chokepoint of the Danish Straits big naval movements are restricted or even prohibitively risky.

The only way to overcome these problems is to demonstrate to Russia the credibility of NATO to stand united and in accordance with spirit of the Treaty. Sizable rotational or standing forces together with all enablers give NATO this credibility. Rigorous planning and training effort from NATO command structure to prepare for all known and yet unknown scenarios is important too. If the deterrence fails and Russia attacks, the national forces together with NATO forces must be able to stand against first wave of attack and give NATO forces in Europe time to crack the Kaliningrad fortress, so that reinforcements can be deployed. These counter-Russian A2/AD capabilities are existential to the defence of three Baltic countries and alone or with only token force from NATO, Baltic States are unable to defend against conventional

attack from Russia, making the Russian A2/AD capabilities existential threat to survival of Baltic States.

Bibliography

- Alcazar, V., 2012. Crisis Management and the Anti-Access/Area Denial Problem. *Strategic Studies Quarterly*, Volume 8, p. 42.
- Bender, J., 2015. *A new Chinese anti-ship ballistic missile is bad news for US aircraft carriers*. [Online]
Available at: <http://www.businessinsider.com/chinas-growing-military-power-may-make-us-aircraft-carriers-obsolete-2015-10>
[Accessed 1 April 2016].
- Bodner, M., 2016. *NATO Deputy SecGen: Russia's Anti-Access/Area-Denial Build-Up Is Biggest Worry*. [Online]
Available at: <http://www.defensenews.com/story/defense/policy-budget/leaders/interviews/2016/02/13/nato-deputy-secgen-russias-anti-accessarea-denial-build-up-biggest-worry/80343130/>
[Accessed 3 April 2016].
- Brustlein, C., 2011. "Toward the End of Force Projection? I. The Anti-Access Threat. *Focus stratégique n° 20 bis*, Volume 20.
- Davin, M. E., 2013. *Anti-Access/Area Denial: Time To Ditch the Bumper Sticker?*, Newport: US Navy Naval War College.
- Gaub, F., 2013. *The North Atlantic Treaty Organization and Lybia..* [Online]
Available at: <http://www.strategicstudiesinstitute.army.mil/pdffiles/pub1161.pdf>
[Accessed 2 April 2016].
- Glatz, R. L. & Zapfe, M., 2016. *German Institute for International and Security Affairs*. [Online]
Available at: https://www.swp-berlin.org/fileadmin/contents/products/comments/2016C05_glt_Zapfe.pdf
[Accessed 26 02 2016].
- Hawk, J., 2016. *Russia Defense Report – Jan. 30, 2016: Fortress Kaliningrad*. [Online]
Available at: <https://southfront.org/russia-defense-report-fortress-kaliningrad/>
[Accessed 1 April 2016].
- Kazianis, H., 2013. *Air-Sea Battle 2.0: A Global A2/AD Response*. [Online]
Available at: <http://thediplomat.com/2013/11/air-sea-battle-2-0-a-global-a2ad-response/>
[Accessed April 2016].
- Krepinevich, A., Watts, B. & Work, R., 2003. *Meeting the Anti-Access and Area-Denial Challenge*, Washington, DC: Center for Strategic and Budgetary Assessments.
- Lasconjarias, G. & Marrone, A., 2016. *How to Respond to Anti-Access/Area Denial (A2/AD)? Towards a NATO Counter-A2/AD Strategy",.* [Online]
Available at: <http://www.ndc.nato.int/news/news.php?icode=906>
[Accessed April 2016].
- Maceda, J., 2015. *Why the Suwalki Gap Keeps Top U.S. General in Europe Up at Night*. [Online]

Available at: <http://www.nbcnews.com/news/world/why-suwalki-gap-keeps-top-u-s-general-europe-night-n469471>
[Accessed April 2016].

Malenic, M., 2015. *AFA 2015: Russia has closed air power gap with NATO, US warns*. [Online]
Available at: <http://www.janes.com/article/54311/afa-2015-russia-has-closed-air-power-gap-with-nato-us-warns>
[Accessed 3 March 2016].

Manea, O., Visan, G. & Gosu, A., 2015. *Black Sea in area denial age*, s.l.: Romania Energy Center.

McCarthy, C. J., 2010. *Anti-Access/Area Denial: The Evolution of Modern Warfare*, Newport: US Navy Naval War College.

Morris, T. S., 2015. *Securing Operational Access: Evolving the Air-Sea Battle Concept*. [Online]
Available at: <http://nationalinterest.org/feature/securing-operational-access-evolving-the-air-sea-battle-12219>
[Accessed April 2016].

RAND Corporation, 2015. *The U.S.-China Military Scorecard Forces, Geography, and the Evolving Balance of Power, 1996–2017*, Washington: RAND Corporation.

Sutjagin, I., 2016. *Panel 4: 'From #Collective Defence to #Deterrence Plus?'*. Tartu, Baltic Defence College.

Tangredi, S. J., 2013. *Anti-Access Warfare-Contering A2/AD Strategies*. 1st ed. Annapolis: Naval Institute Press.

Theiner, T., 2015. *Gotland – the Danzig of our time*. [Online]
Available at: <http://euromaidanpress.com/2015/03/22/gotland-the-danzig-of-our-time/#arvlbdata>
[Accessed March 2016].

Tilghman, A., 2016. *More U.S. troops deploying to Europe in 2017*. [Online]
Available at: <http://www.militarytimes.com/story/military/2016/02/02/more-troops-deploying-europe-2017/79693680/>
[Accessed 2 April 2016].

University of Copenhagen Centre for Military Studies, 2015. *Baltic Sea security conference proceedings*. Copenhagen, University of Copenhagen.

van Tol, J., 2014. *Center for European Policy Analysis*. [Online]
Available at:
[http://www.cepa.org/sites/default/files/documents/Deterrence%20Paper%20A2A D-.pdf](http://www.cepa.org/sites/default/files/documents/Deterrence%20Paper%20A2A%20D-.pdf).
[Accessed 29 March 2016].

Was Stuxnet an Act of War?

MAJ Janis Jansons

Introduction

Modern society is living in complex and fragile information environment in which data processing and exchange are growing exponentially. Already, different digital computerized systems are supporting most of key infrastructures like financial systems, power and water supplies, air traffic management, public and military communications. To increase accessibility to those systems in the information domain requires interoperability and interconnectivity which makes them complex to maintain and vulnerable to cyber-attacks/intrusions. Furthermore, this new reality of information exchange shows that the societies are deeply dependent on information and communication technologies which are interconnected in one global network named Internet. This addiction to the Internet is a major source of vulnerability and full control over the information domain in these conditions is next to impossible. So, somebody could use those vulnerabilities to breach national security from afar and influence economic, political and social situation in other countries.

The Internet is an ownerless, ubiquitous and open for all information exchange domain which can shape the international relations through the cyber field. The Internet is a computer network that uses standardized protocols to interconnect states, organizations and individuals worldwide. Neither states nor organizations, nor single persons are the owners of the Internet. While there is one non-profit organization which simply manages Internet protocol numbers and Domain Name System root, the others are providing a piece of infrastructure just to be part of the Internet. There is no one international entity that can control and affect the data flow. Each country has its own legislation to react and influence local users throughout Internet service providers. Only close cooperation among the states can help to identify and prevent illegal activities against other states as well as support foreign countries during investigations. So, the states' political willingness to cooperate in the cyberspace shapes dialogues internationally. However, there are vague circumstances where some cyber activities original from one state against another state critical infrastructure could be interpreted as an act of war or a covert action.

This essay will uncover how cyber weapon was used to influence state struggling becoming a nuclear power. Was the use of cyber weapon an act of war? This essay will claim that Stuxnet was not an act of war, but rather a covert action with possible future consequences. To argue this statement, this essay is divided into two parts where the first will explain the essence of two terms - act of war and cyberspace to understand the environment where Stuxnet was applied. The second part will focus more on impact and reaction to Stuxnet.

Act of war and cyberspace

The phrase 'Act of war' is characterised as a political term than a military or legal one (Nakashima, 2012). This term is used in an international environment by politicians in situations where it was a violent and non-violent act. The terrorist attacks (Cella, 2015), key leader killings (Strange, 2013), shooting down airplane during peace time (Vinogradov, 2015), blockade of sea lines of communication (Global Research, 2015.), imposing economic sanctions (Saundersaug, 2014), cyber-attack (Gorman and Barnes, 2011) etc., have motivated politicians to use the phrase 'act of war'. This term does not have a united definition worldwide and its application for cyber incidence seems to be questionable. However, there is a country which defines 'act of war'. The United States (U.S.) to prevent possible cyber '*Pearl Harbor*' (Stiennon, 2015) has come to the conclusion that cyber-attacks originating from another country can be interpreted as an 'act of war' to counter using all kinds of military force (Gorman and Barnes, 2011). While the international law avoids the term 'act of war' in favour of other phrases like 'illegal intervention', 'use of force', 'armed attack', or 'act of aggression'. For example, the act of aggression includes more serious uses of force and armed attack, whereas all uses of force are not only armed attacks, but could also be illegal interventions (Fidler, 2011). Despite those definitions, legal experts Charles Dunlap, a retired Air Force Major General and professor at Duke University law school, or retired Gen. James Cartwright, former vice chairman of the Joint Chiefs of Staff have said that only the president and Congress in the U.S. could decide that the social or financial impairment is sufficient to consider a cyber-attack as an act of war (Nakashima, 2011). So, the use of this term is depending on the targeting country's leadership who would decide whether to respond with military force to cyber-attacks. As a result the phrase 'act of war' becomes more political. If it

is so, then what could be the trigger for politicians in cyberspace to respond militarily? For this reason, it is important to understand the cyberspace as such.

The cyberspace like the term 'act of war' has no a single internationally recognised definition. The cyberspace is a revolutionary human-made ubiquitous, networked, and virtual environment which seems to be driven by swift electronic communication and information technologies progress. This is a possible way how to explain cyberspace in own words. In spite of this innovative sketch, the overall definitions of cyberspace are disputable (Ottis and Lorents, 2010). Therefore, trying to find the exact perfectly expressed definition of cyberspace seems to be a wicked problem. It is therefore more prudent to stick to one definition and to analyse step-by-step what these separate components are.

Firstly, it is important to examine some historical background of wording, which could be the main milestone of further definitions. The term cyber appears to stem from the Greek word *kybernetes* which means steersman or the governor. So, in 1948, to appreciate Maxwell control loop feedback mechanism, the famous mathematician and philosopher N. Wiener (1985) introduces the first application of cyber as 'cybernetic... the entire field of control and communication theory, whether in the machine or in the animal'. In the initial stages of a technology's development the term cyber relates originally to data processing and intercommunication activities or name it 'Wiener component' of cyberspace definition. However, in later years, the word cyber has been used so to emphasize another environment in networks and computers rather than physical appearance.

Secondly, the prefix cyber is basically exploited as the part of a composite word, then it is used as a single term. The compound word, for instance, cyberspace could be considered in order to obtain a metaphysical or certain meaningful definition. Without knowing about computers and the Internet, speculative fiction novelist and essayist W.Gibson (1984) in his novel 'Neuromancer' introduced first time the word cyberspace as 'a consensual hallucination' on the computerized network. That means its appearance provides any kind of physical medium. This could lead to the feeling of outside of physical reality, which is more related to 'Gibson's component' of cyberspace definition. Seamlessly using advantage of new technologies, human beings tend to believe in the existence of such an environment. This stimulates the

search for comprehensive and coherent definition, where actors are the key element to interact in this environment.

The lack of security in cyberspace offers an opportunity for a wide range of actors like in social -physical space, where persons have various reasons and capabilities to challenge law enforcement. The unauthorized actors originally in cyberspace were cyber criminals, whose strong intent was to gain financial benefits, blackmailers, who used evidence to intimate key leaders, or simply hackers, who wanted to prove their brain potential. Moreover, the national government and non-government actors like private institutions, crime and extremist groups, subsidised agents are capable of demonstrating cyber-attacks in more sophisticated way. In the targeted states those groups of attackers might undermine the finance system, and disrupt the critical infrastructures (Omand, 2013). The actors are divided into two main groups as insiders and outsiders.

The insiders are the most harmful to an organization, which they work for. Insiders are trusted parties such as current and former employees, service providers, and business partners, who have the knowledge about the insides and security measures of organization and access to organization network or even sensitive information. Two examples of insiders who caused serious damage to government organization are former soldier of the U.S. B.E. Manning and former Central Intelligence Agency employee E.J. Snowden. B.E. Manning was convicted after disclosing to WikiLeaks sensitive military and diplomatic documents, which he as an intelligence analyst elicited from classified databases. The second famous insider, E.J. Snowden, was able to copy information from the U.S. National Security Agency (NSA) and after then publicly released the sensitive information about numerous global surveillance programs. Both cases carried out by insiders have weakened the national security of the country and relations with various international partners (Sovereign Intelligence, 2014).

The outsiders are a defined group of attackers, who are possible to split into three main groups such as individuals, non-government organizations and government organizations (Geest, 2015).

Individuals as potential cyber attackers could be divided into three main subgroups: amateurs, hackers and hacktivists. The amateurs or beginners can easily learn the

first steps for hacking on the internet by doing a certain category of attacks. However, hackers are more capable to threaten any computerized system. This preconception is not always truthful characterization of hackers due to their different attitudes. Hackers are noticeably divided like white (blue), grey and black hat (Kovacs, N., 2015). White and grey hat hackers break the security for testing vulnerabilities to improve computerized systems. The only difference is that grey hat hacker's experiment the targeted system without the owner's authorization or awareness. They inform the system administrator about the discoveries and sometimes ask for a fee to correct the security problems. Although, this attitude of hacker appears to be ethical, the unauthorised access is illegal. The black hat hacker is cybercriminal, who use its abilities only for malicious or unlawful purposes to gain financial profit (Graves, 2010).

Non-government cyber organizations are mostly cybercriminal and ideological groups like anonymous cyber protesters. Hacktivist or anonymous cyber protester is predominantly driven by a political reason rather than financial benefits. They are able to build the virtual groups, which conduct an amount of cyberattacks to fight the state's powers and large industries when they step over the "red" line. In 2014 before the release the comedy *The Interview* on the fictional assassination of North Korea's leader an allegedly hacktivist group attacked Sony Pictures Entertainment leaking company's classified information. The U.S. government, however suspects that North Korea government sponsored hacker group is behind these attacks and as a consequence, this issue escalated into a diplomatic crisis between two countries (Grisham, L., 2015). So, those cyber incidences possible being maintained by hacktivists were able to raise a public attention and diplomatic consequence without gaining any financial benefit. While organized criminal groups make profits and disappear before law enforcement identifies them (Broadhurst, et al., 2014). The global cybercriminal organizations exist and have structures similar to the Mafia (Peachey, 2014), some of them are protected by weak and corrupted governments (Rifkind, 2011). The criminal organizations are mostly profiting by buying and selling stolen individual's bank credit cards information and company's intellectual properties. Conversely, the ideological groups have more extensive goals, which occasionally are politically motivated and supported by government organizations to keep within an international law (Garcia, 2010).

Government organizations or nation-states have the largest capabilities and they can target a wide-array of institutions and individuals from private and government research and development institutions to defence, finance and public sector organizations. Government-organized attacks could range from dissemination of propaganda to intelligence gathering to multiform operations on critical infrastructures for example Russian online “troll” (Iasiello, 2015), operation ‘Titan Rain’, and Operation ‘Olympic Games’ (Stiennon, 2015. p.125).

The main effort of cyber-attacks is to gain economic benefits rather political or military dominance. Organized cyber-attacks disrupt actively the information and communication systems of the financial institutions, cause serious reputation and economic damage. Reputation damage is more related to the company, trust and ability to safeguard costumers’ and own money. In order to reduce probable direct financial loss and to recover expenditures from cyber-attacks, companies and governmental institutions need to provide the additional cost of securing networks. Global cyber activities profit yearly up to US\$1 trillion, which are comparatively more than global drug trafficking and piracy together (McAfee, 2013). That means overall cyber activities are more oriented to finance sector rather to overcome the security systems of well protected governmental information and communication system. Moreover, compare these numbers what should be official salary to attract well skilled hackers who will be ready to serve in a country reaching political aims by targeting key infrastructure of opponent site. This request respective resources and organize structure which is capable to produce sophisticated cyber tools to penetrate in the well protected system or even standalone systems.

Cyber-attacks are a major influence tool during or before major political and military conflicts. The traditional dominant cyber actors in the international arena are the U.S., Russia and China, all of which have huge capabilities and resources to support cyber offensive operations (Lewis, 2013). For example, Russia is dominating over the neighbouring countries in the cyber space. In 2007 the Estonia government had decided to relocate the Soviet time memorial from centre of capital city to a military cemetery. Putin’s supported regime shamed Estonians and reacted to the relocation with the cyber power. Estonia suffered widespread politically motivated cyber-attacks that have been first brute-force denial of service attacks from Russia site. This cyber incident lasted several days by paralysing information domain of Estonia, electronic

banking system and affecting the daily life of Estonian citizens (Traynor, 2007). However, this cyber-attack was not declared as an act of war. So, in 2007 Estonia did not use NATO Article 5. However, during Georgia War in 2008 and Ukraine crises in 2013 was disclosed real Russian tactics using cyber tools in tandem with a conventional military campaign. In Georgian War Russian state operated companies like Rostelecom and Comstar and volunteer cyber warriors were blocking the internet traffic in Georgia. Moreover, in 2014 attackers from Russia targeted computerized election system in Ukraine to disrupt president election's results from around the country. Before this cyber-attack the government officials and security units of Ukrainian battling pro-Russian rebels were targeted to cripple intelligence-gathering and decision-making (Coker and Sonne, 2015). In those cases there was not proved evidence that Russia as a state was certainly behind the attacks (Kirchner, 2009). These facts indicate that government sponsored and covert cyber-attack tend to be more sophisticate and capable of obtaining political and military goals.

Stuxnet worm

The Operation 'Olympic Games' was a secret campaign under which Stuxnet worm seems to be formed (Stiennon, 2015). Some provided thoughts that Stuxnet could be starting point in a new era of cyber war. Some higher education institutions define that the cyber war is the highest level of cyber conflict between or among states in which actors who is acting on behalf of a governmental body carry out cyber-attacks as part of military operations (Godwin, et al., 2014.). Based on the empirical definition war is possible between states if the conflict involves at least 1,000 battle-related deaths per year (Harrison, et al., 2015). Rid convincingly argued that Stuxnet was not connected to a conventional military operation and did not kill any military person (Rid, 2013). Some argued that the Stuxnet was a first demonstration of cyber offensive capability which is able to carry out physical destruction of strategic targets in military style (Broad, et al., 2011). Fidler was also not sure to define the Stuxnet's release as an act of war (Fidler, 2011). Former head of the NSA and CIA director retired general Hayden fully rejected that Stuxnet was an act of war (CBSNews, 2012). However, it is clear that the Operation Olympic Game is still officially not acknowledged military campaign. For that reason, there are so many denials, many rumours and uncertainty around the Stuxnet. To prove Hayden and reject Fidler

argument there is need to understand what the Stuxnet were and what was its impact on target, and what were reactions to this cyber incident.

The goal of Stuxnet was to destroy or significantly delay Iran's potential nuclear weapon production capability. The main focus was Natanz uranium enrichment plant where was thousands centrifuges used to enrich the uranium gas. The worm was able to shut down and caused damage to 984 centrifuges that spin uranium gas material (Albright, et al., 2010). After this attack Iran has interrupted work at its nuclear facilities without explanation to international community (Katz, 2010). It is unclear that the worm was the reason to do so.

Stuxnet has more technical sophistication and precisely targeted malware than a normal computer worm. Worm is a code which is capable to run without host program, self-reproduce and propagate to other computer systems through downloaded files or network. The worm can spread using one or more methods like email, instant messaging and file-sharing programs, social networking sites, network shares, removable drives with Autorun enabled, and software vulnerabilities (Microsoft, 2015). In 2010 Stuxnet was discovered in the databanks of critical infrastructures like power plants, traffic control systems, and different factories around the world (Keizer, 2010), but Iran was the most targeted country about 60% of all infection (Halliday, 2010). Stuxnet was able to manipulate the speed of centrifuges and damage the uranium enrichment process. At the same time this worm was changing Siemens SCADA control software parameters in such way that system's indicators show normal working condition (Langner, 2013). Unlike most worms Stuxnet does not exploit the usual forged digital certificates that help to intrude into computer systems. It actually used real stolen Realtek Semiconductor and JMicron Technology Corporations, global microchip producers in Taiwan, digital certificates which allow intruders signing fake software drivers for Windows operating systems (Zetter, 2011). Stuxnet exploited security holes in the systems. Those gaps that system's creators are unaware of are known as zero-day vulnerabilities. The details of zero-day vulnerabilities are extremely valuable and can be sold on the black market for five to several hundred thousand dollars U.S. dollars each (Zetter, 2014). The most successful malwares are exploiting them and Stuxnet was not exceptional. Actually Stuxnet used 20 zero-day vulnerabilities (Rapoza, 2012) to penetrate in a computer system. When it accesses the system, this worm does not always activate.

In Stuxnet codes was defined specific Siemens settings of programmable logic controllers (PLC) that control and monitor the speed of the centrifuges (McMillan, 2010). It was searching for this specific target without that target worm remains hidden (McMillan, 2010).

It is unclear if Stuxnet was effective to reach political goals, but it was the motivation for Iran to develop cyber capabilities. Iran increased its cyberwarfare capabilities with different organizations like High Council of Cyberspace, Cyber Defence Command, loyal, high skilled hacker group named Iranian Cyber Army, which has links with the Revolutionary Guard and the Asiana hacker forum (Wheeler, 2013). The Iranian Cyber Army was behind a wave of cyberattacks on the U.S. banking systems, and they hacked into Israeli computers to steal information from government officials in 2011 (Baker, 2015). So, it looks like that Iranians seem to have or try to find evidence which countries were involved to build and release of Stuxnet.

Only a state or group of states seems to be willing and capable to build and use such cyber weapon like Stuxnet. The major issue for the United Nations (UN) was to prevent Iran getting the nuclear bomb. In 2006 the UN Security Council's (UNSC) five permanent members; namely China, France, Russia, the United Kingdom (UK), and the U.S.; plus Germany were struggling with diplomatic efforts to stop the Iranian nuclear program without success (Küntzel, 2015). Moreover, in 2008 UNSC adopted new Resolution 1803 to enforce all steps from the previous resolution. In 2009 the U.S. started shaping world community attention against Iran, and Israel threatened with possible nuclear action (Lyons, 2015). There was also questioned, if the U.S. decided to launch conventional attack would it set the Iranian nuclear program back. Beside that it could induce Middle East in another war and the Americans would not be ready for uninterrupted military actions and possible growing oil price (Blas, 2012). It looks like that the U.S. and Israel were searching for desired outcome with minimal effort and maximum gains. There are no sufficient and conclusive evidences beyond rumours, which country could have the potential to develop such cyber weapon and willing in 2010 to attack Iran. However, only an economically developed country can afford at least 400\$ million to develop a Stuxnet worm (Langner, 2010), because according previous argument the individuals or organized criminals are more interested to gain money than to spend it. Due to this fact, some have it that the U.S. was involved in the testing and development of expensive cyber weapons. Others

believe that Israel is responsible for the attack, because the worm code has the biblical reference (Timmerman, 2010). Iran's officials have accused Siemens Mobile Company, which software was used to prepare the ground for the Stuxnet worm (The Telegraph, 2011). There is some evidence, but not a real investigation and lack of state cooperation to find out who was behind Stuxnet could raise the questions. If there is no clear proof about state and conventional military troop's involvement, there is no reason to define Stuxnet as an act of war.

Stuxnet does not have a warlike nature to influence political and military condition of another state. According Clausewitzian concept of war as a continuation of politics by other means Rid argued that any act of war related to cyber incidents has to be lethal, has to have clear means and ends, and has to be politically motivated or the state should be behind them (Rid, 2013.). Stuxnet worm had clear means and ends to significant impact Iranian nuclear program, as well as multiple anonymous sources have indicated that at least two states were involved to launch the operation. Despite of those facts Stuxnet did not result any battle deaths of military personnel. Although, it seems to be a new form of war, which skips the battlefield, by definition any war should be violent. That means this cyberattack has not warlike nature, but it could be a kind of hidden action performed by state to influence opponent state.

Stuxnet worm is most likely a covert action supported by the U.S. Government. After release of Mr. Sanger's book in 2012 brought a fast request from an American Republican party to investigate by the FBI the leaks of information about a U.S. covert cyber operation to shut down Iran's nuclear enrichment facilities with a computer worm named Stuxnet (Scarborough, 2013). According to Mr. Sanger information "“Should we shut this thing down?” Mr. Obama asked, according to members of the president's national security team who were in the room” it seems to be secretly ordered by the U.S. president to use Stuxnet in order to delay the Iranian nuclear program. The president based on the domestic legal framework has two possibilities to authorize a cyber-attack against another state. So, the Olympic Game operation should rely on military or intelligence legal authority. Under military domain, it could be difficult to carry out cyber-attacks without triggering solid diplomatic and security troubles for the U.S., but the intelligence domain has more flexibility to maintain hidden cyberattacks (Brecher, 2012). According to National Security Act Sec. 503 (e) the U.S. Intelligence community has the possibility to clandestinely

prepare personnel, who is not uniformed military personnel to attack an enemy. The U.S. policymaker defined this activity as a covert action “to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly” (Peritz and Rosenbach, 2009). Moreover, during interview about the Stuxnet former head of the National Security and CIA director Michael Hayden formulated that this cyber-attack was not a warlike activity because the opposite site did not respond as if it was an act of war. He is sure that this cyber incident was a thing between peace and war so called covert action (CBSNews, 2012). So, it could be the reason why there are only rumours and no investigation to find out which country is behind Stuxnet worm.

Conclusion

To conclude the findings of this essay, the phrase ‘act of war’ has more political term than a legal one because the international law use different term and country which defined it need to have its political leadership decision to respond with military force to the attacks in cyberspace. The cyberspace is complex and dynamic environment which is characterised by two components - physical (Wiener) and non-physical (Gibson), where actors are the part of physical element. The lack of security in cyberspace offers an opportunity for a wide range of actors who have a various reasons and capabilities to challenge law enforcement. The predominance of cyber-attacks effort seeks to gain economic benefits. To penetrate into the well protected system or even standalone systems cyber attackers exploit vulnerabilities of the information systems and personal information. Therefore, social media is one of the sources where cyber actor like governmental organizations can use to collate information, and use it in future to break security walls of the system targeting opponent and, for example, its critical infrastructure. For example, the cyber-attacks possibly maintained by the Russian regime against opponent's critical infrastructure are a major influence tool during or before major diplomatic and political trouble or even military conflicts. Russia as a state did not disclose their involvement in those attacks. Due to complexity of cyberspace and lack of willingness and cooperation to investigate the cyber incident, it is not easy to prove that state actor was behind cyber-attack.

The Operation Olympic Games under which Stuxnet worm was possibly formed seems to be another good example of state sponsored secret campaign in the cyberspace. Stuxnet opened a new era of cyber reality by showing more technically sophisticated and precise approach to destroy or significantly delay Iran's potential nuclear weapon production capability. Since 2006 only some UNSC permanent members like China, France, the United Kingdom (UK), and the U.S. had been struggling with diplomatic efforts to stop the Iranian nuclear program without success. Therefore, there are many rumours that the U.S. was involved in the testing and development of expensive first cyber weapon like Stuxnet. Due to lack of clear evidence about state and conventional military troop's involvement, there is no reason to define Stuxnet as an act of war. Beside that Stuxnet does not have a warlike nature because of no battle deaths of military personnel and targeting state no willingness to respond. To summarise, Stuxnet worm is most likely a covert action supported by the state which has offensive cyber capabilities to maintain so expensive campaign to prevent possible conventional military attack. Nevertheless, Iranians seem to try to find evidence which countries were behind Stuxnet and they seek to retaliate.

Cyber environment is a unique opportunity for the cyber powers to shape international relations. Stuxnet has shown a new cyber reality which warned of an impending cyber 'Pearl Harbor'. Therefore, based on those findings in this essay, the future political leaders should be aware the potential of cyber powers, but military leaders should be ready to operate in complex and fragile information environment in the similar way as it requires in other domains.

Bibliography

- Albright, D. Brannan, P. and Walrond, C., 2010. *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant? Preliminary Assessment*. [online] Available at <http://isis-online.org/isis-reports/detail/did-stuxnet-take-out-1000-centrifuges-at-the-natanz-enrichment-plant/> [Accessed 07.02.2016]
- Baker, J.W., 2015. *Iran: The Cyber Nation – Timeline of Every Hack*. [online] Available at <http://xpatnation.com/iran-the-cyber-nation-timeline-of-every-hack/#.y77h98T7y> [Accessed 10.02.2016]

Blas, J., 2012. *The oil price reaction to an Iranian strike*. [online] Available at <http://www.ft.com/intl/cms/s/0/e977f55c-f780-11e1-ba54-00144feabdc0.html#axzz41DLBucjD> [Accessed 12.02.2016]

BNN, 2014. *SP: Kremlin-financed internet trolls operate in Latvia* [online] Available at <http://bnn-news.com/sp-kremlin-financed-internet-trolls-operate-latvia-122404> [Accessed 25.11.2015]

Brecher, A.P., 2012. *Cyberattacks and the Covert Action Statute: Toward a Domestic Legal Framework for Offensive Cyberoperations*. [online] Available at <http://repository.law.umich.edu/cgi/viewcontent.cgi?article=1081&context=mlr> [Accessed 01.03.2016]

Broad, W.J. Markoff, J. and Sanger, D.E., 2011. *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*. [online] Available at http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0 [Accessed 10.03.2016]

Broadhurst, R., etc. 2014. *Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime*. [online] Available at <http://www.cybercrimejournal.com/broadhurstetalijcc2014vol8issue1.pdf> [Accessed 08.11.2015]

CBSNews, 2012. *Gen. Hayden: Stuxnet virus "Not an act of war"*. [online] Available at <http://www.cbsnews.com/news/gen-hayden-stuxnet-virus-not-an-act-of-war/> [Accessed 04.02.2016]

Cella, M., 2015. *Paris Attacks Called 'Act of War'*. [online] Available at <http://www.usnews.com/news/articles/2015/11/14/paris-terror-attacks-by-isis-called-act-of-war> [Accessed 11.01.2016]

Coker, M. and Sonne, P., 2015. *Ukraine: Cyberwar's Hottest Front*. [online] Available at <http://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671> [Accessed 25.11.2015]

Fidler, D.P., 2011. *Was Stuxnet an Act of War? Decoding a Cyberattack* [online] Available at http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5968088&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D5968088 [Accessed 02.02.2016]

FromDev, 2014. *100+ Free Hacking Tools To Become Powerful Hacker*. [online] Available <http://www.fromdev.com/2014/09/free-hacking-tools-hacker.html> [Accessed 06.11.2015]

Garcia, E.C., 2010. *Regulating Nation-State Cyber Attacks in Counterterrorism Operations*. [online] Available at <https://www.hsd1.org/?view&did=10513> [Accessed 08.11.2015]

Geest, D.S., 2015. *Cybersecurity and the dividing nature of global competing ideologies*. [online] Available at <http://www.hscentre.org/global-governance/cybersecurity-dividing-nature-global-competing-ideologies/> [Accessed 06.11.2015]

Gibson, W., 1984. *Neuromancer*. New York: Berkley Publishing Group

Global Research, 2015. *Turkey's Blockade of Russian Naval Vessels' Access to the Mediterranean, Russia's Black Sea Fleet Completely Cut Off*. [online] Available at <http://www.globalresearch.ca/turkeys-blockade-of-russian-naval-vessels-access-to-the-mediterranean-russias-black-sea-fleet-completely-cut-off/5492688> [Accessed 13.02.2016]

Godwin, J.B. Kulpin, A. Rauscher, K.F. and Yaschenko, V., 2014. *The Russia-U.S. Bilateral on Cybersecurity – Critical Terminology Foundations, Issue 2*. EastWest Institute and the Information Security Institute of Moscow State University

Gorman, S. and Barnes, E.J., 2011. *Cyber Combat: Act of War*. [online] Available at <http://www.wsj.com/articles/SB10001424052702304563104576355623135782718> [Accessed 13.02.2016]

Graves, K., 2010. *Certified Ethical Hacker study guide*. [online] Available at <http://ir.nmu.org.ua/bitstream/handle/123456789/133057/768e0fbfd4fe2971f189aecf8c038201.pdf?sequence=1> [Accessed 07.11.2015]

Grisham, L., 2015. *Timeline: North Korea and the Sony Pictures hack*. [online] Available at <http://www.usatoday.com/story/news/nation-now/2014/12/18/sony-hack-timeline-interview-north-korea/20601645/> [Accessed 07.11.2015]

Halliday, J., 2010. *Stuxnet worm is the 'work of a national government agency'* [online] Available at <http://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency> [Accessed 05.02.2016]

Harrison, L. Little, A. and Lock, E., 2015. *Politics: The Key Concepts*. London: Routledge

Iasiello, E., 2015. *Russia's Propaganda Trolls Make an Impact in Cyberspace*. [online] Available at <http://darkmatters.norsecorp.com/2015/08/27/russias-propaganda-trolls-make-an-impact-in-cyberspace/> [Accessed 09.11.2015]

Katz, Y., 2010. *Stuxnet may have destroyed 1,000 centrifuges at Natanz*. [online] Available at <http://www.jpost.com/Defense/Stuxnet-may-have-destroyed-1000-centrifuges-at-Natanz> [Accessed 07.02.2016]

Keizer, G., 2010. *Why did Stuxnet worm spread?* [online] Available at <http://www.computerworld.com/article/2516109/security0/why-did-stuxnet-worm-spread-.html> [Accessed 05.02.2016]

Kirchner, S., 2009. *Distributed Denial-of-Service Attacks under Public International Law: State Responsibility in Cyberwar.* [online] Available at https://www.researchgate.net/publication/251287009_Distributed_Denial-of-Service_Attacks_under_Public_International_Law_State_Responsibility_in_Cyberwar [Accessed 15.12.2015]

Kovacs, N., 2015. *What is the Difference Between Black, White and Grey Hat Hackers?* [online] Available at <http://community.norton.com/en/blogs/norton-protection-blog/what-difference-between-black-white-and-grey-hat-hackers> [Accessed 07.11.2015]

Küntzel, M., 2015. *Germany and a Nuclear Iran.* [online] Available at <http://jcpa.org/article/germany-and-a-nuclear-iran/> [Accessed 12.02.2016]

Langner, R., 2010. *The short path from cyber missiles to dirty digital bombs.* [online] Available at <http://www.langner.com/en/2010/12/26/the-short-path-from-cyber-missiles-to-dirty-digital-bombs/> [Accessed 14.02.2016]

Langner, R., 2013. *To Kill a Centrifuge.* [online] Available at <http://www.langner.com/en/wp-content/uploads/2013/11/To-kill-a-centrifuge.pdf> [Accessed 05.02.2016]

Lewis, J., 2013. *Hidden Arena: Cyber Competition and Conflict in Indo-Pacific Asia.* [online] Available at http://csis.org/files/publication/130307_cyber_Lowy.pdf [Accessed 14.12.2015]

Lyons, K., 2015. *Iran nuclear talks: timeline.* [online] Available at <http://www.theguardian.com/world/2015/apr/02/iran-nuclear-talks-timeline> [Accessed 12.02.2016]

McAfee, 2013. *The Economic Impact of Cybercrime and Cyber Espionage.* [online] Available at <http://www.mcafee.com/mx/resources/reports/rp-economic-impact-cybercrime.pdf> [Accessed 09.11.2015]

McMillan, R., 2010. *Was Stuxnet Built to Attack Iran's Nuclear Program?* [online] Available at http://www.pcworld.com/article/205827/was_stuxnet_built_to_attack_irans_nuclear_program.html [Accessed 06.02.2016]

Microsoft, 2015. *Malware Protection Center.* [online] Available at <https://www.microsoft.com/security/portal/mmpc/shared/glossary.aspx> [Accessed 15.03.2016]

Nakashima, E., 2011. *U.S. cyber approach 'too predictable' for one top general.* [online] Available at https://www.washingtonpost.com/national/national-security/us-cyber-approach-too-predictable-for-one-top-general/2011/07/14/gIQAYJC6EI_story.html?tid=a_inl [Accessed 13.02.2016]

Nakashima, E., 2012. *When is a cyberattack an act of war?* [online] Available at https://www.washingtonpost.com/opinions/when-is-a-cyberattack-an-act-of-war/2012/10/26/02226232-1eb8-11e2-9746-908f727990d8_story.html [Accessed 10.01.2016]

Omand, D., 2013. *Security Europe: The steps needed to protect the EU's critical infrastructure against cyber-attack.* [online] Available at <http://europesworld.org/2013/10/01/the-steps-needed-to-protect-the-eus-critical-infrastructure-against-cyber-attack/#.VjzxylLotjo> [Accessed 06.11.2015]

Ottis, R. and Lorents, P., 2010. *Cyberspace: Definition and Implications.* [online] Available at <https://dumitrudumbrava.files.wordpress.com/2012/01/cyberspace-definition-and-implications.pdf> [Accessed 02.11.2015]

Peachey, P., 2014. *Mafia Cybercrime Booming and With It a Whole Service Industry, Says Study.* [online] Available at <http://www.independent.co.uk/news/uk/crime/mafia-cybercrime-booming-and-with-it-a-whole-service-industry-says-study-9763447.html> [Accessed 08.11.2015]

Peritz, A.J. and Rosenbach, E., 2009. *Covert Action.* [online] Available at http://belfercenter.ksg.harvard.edu/publication/19149/covert_action.html [Accessed 01.03.2016]

Rapoza, K., 2012. *Is It Time For Another Stuxnet Attack On Iran?* [online] Available at <http://www.forbes.com/sites/kenrapoza/2012/05/28/is-it-time-for-another-stuxnet-attack-on-iran/#1879269474fb> [Accessed 06.02.2016]

Rid, T., 2013. *Cyber War Will Not Take Place.* London: Hurst

Rifkind, J., 2011. *Cybercrime in Russia.* [online] Available at <http://csis.org/blog/cybercrime-russia> [Accessed 08.11.2015]

Rutledge, P., 2013., *How Obama Won the Social Media Battle in the 2012 Presidential Campaign* [online] Available at <http://mprcenter.org/blog/2013/01/how-obama-won-the-social-media-battle-in-the-2012-presidential-campaign/> [Accessed 25.11.2015]

Sanger, D.E., 2012. *Obama Order Sped Up Wave of Cyberattacks Against Iran.* [online] Available at <http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> [Accessed 04.03.2016]

Saundersaug, P.J., 2014. *When Sanctions Lead to War*. [online] Available at http://www.nytimes.com/2014/08/22/opinion/when-sanctions-lead-to-war.html?_r=0 [Accessed 13.02.2016]

Scarborough, R., 2013. *In classified cyberwar against Iran, trail of Stuxnet leak leads to White House*. [online] Available at <http://www.washingtontimes.com/news/2013/aug/18/trail-of-stuxnet-cyberwar-leak-to-author-leads-to-/?page=all> [Accessed 04.03.2016]

Sovereign Intelligence, 2014. *THE INSIDER THREAT: Implications for Corporate Security* [online] Available at <http://www.sovereign-llc.com/wp-content/uploads/2014/09/SI-Insider-Threat-WP.pdf> [Accessed 23.11.2015]

Stiennon, R., 2015. *There Will be Cyber War: How the Move to Network-Centric War Fighting has set the Stage for Cyberwar*. IT-Harvest Press, 2015

Strange, H., 2013. *US raid that killed bin Laden was 'an act of war', says Pakistani report*. [online] Available at <http://www.telegraph.co.uk/news/worldnews/asia/pakistan/10169655/US-raid-that-killed-bin-Laden-was-an-act-of-war-says-Pakistani-report.html> [Accessed 11.01.2016]

The Telegraph, 2011. *Iran accuses Siemens over Stuxnet cyber-attack*. [online] Available at <http://www.telegraph.co.uk/technology/news/8457658/Iran-accuses-Siemens-over-Stuxnet-cyber-attack.html> [Accessed 13.02.2016]

Timmerman, K., 2010. *Computer Worm Shuts Down Iranian Centrifuge Plant*. [online] Available at <http://www.newsmax.com/KenTimmerman/iaea-stuxnet-computer-worm/2010/11/29/id/378288/> [Accessed 10.02.2016]

Traynor, I., 2007. *Russia accused of unleashing cyberwar to disable Estonia*. [online] Available at <http://www.theguardian.com/world/2007/may/17/topstories3.russia> [Accessed 25.11.2015]

Vinogradov, D., 2015. *Turkey Committed Act of War By Shooting Russian Plane in Syria*. [online] Available at <http://sputniknews.com/middleeast/20151124/1030684495/russian-plane-turkey-shot-syria.html> [Accessed 13.02.2016]

Wheeler, A., 2013. *The Iranian Cyber Threat*. [online] Available at <http://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/> [Accessed 10.02.2016]

Wiener, N., 1985. *Cybernetics: Or Control and Communication in the Animal and the Machine*. 2nd ed. Cambridge: The M.I.T. Press

Zetter, K., 2011. *How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History*. [online] Available at <http://www.wired.com/2011/07/how-digital-detectives-deciphered-stuxnet/2/> [Accessed 05.02.2016]

Zetter, K., 2013. *Stuxnet Attack on Iran Was Illegal 'Act of Force'*. [online] Available at <http://www.wired.com/2013/03/stuxnet-act-of-force/> [Accessed 10.12.2015]

Zetter, K., 2014. *Hacker Lexicon: What Is a Zero Day?* [online] Available at <http://www.wired.com/2014/11/what-is-a-zero-day/> [Accessed 06.02.2016]

The Implications of Russian Federation Security Strategy for the Baltic States' military security.

MAJ Andrius Jagminas

'In the Soviet days we scared the world. (...) But ten years ago we decided for some reason that everyone heartily loves us. (...) We must get rid of imperial ambitions on the one hand, and on the other clearly understand where our national interests are, to spell them out, and fight for them'.

Vladimir Putin (as quoted in Donaldson and Noguee, 2002, p. 341)

In the light of Crimea annexation and ongoing Ukrainian crisis 'Russian Federation (RF)' president Vladimir Putin delivered a speech at Valdai International Discussion Club in 2014. He emphasized that the crisis in Ukraine is a result of U.S. and European partners hasty backstage decisions disrespecting Russian national interests (Putin, 2014). He stressed that 'since he have come to where he is today and to this office he holds, he considers it his duty to do all he can for Russia's prosperity, development and to protect its interests' (Putin, 2014). Since fundamental RF national interests are defined in 'Russian National Security Strategy to 2020 (RNSS)', it deserves closer attention as it provides insight into the RF strategic national priorities and prescribes measures to ensure RF security and development. The analysis of the RNSS could suggest on how Moscow plans to address its security concerns and what three 'Baltic States (3Bs)' could face in the future.

This essay aims to analyse what threats constitutes RNSS towards 3Bs and how respective States' defence concepts are addressing the issues in military domain? Research question is - What are the implications of RNSS for the Baltic States' military security? Thus, it can be said that in the meantime RF claims to have a peaceful agenda and is not a threat to Baltic States. Despite this widespread Kremlin's view the paper will argue that RNSS constitutes wide spectrum of internal and external threats towards 3Bs. These threats implies that national military defence concepts primarily should focus on initial independent territorial defence capability as precondition for NATO collective defence. Due to the essay constrains it is narrowed

to military domain only although it cannot ensure comprehensive state defence alone and requires employment of all national instruments of power¹⁶. For this reason firstly the paper will analyse the main threats arising from RNSS towards 3Bs. Secondly it will evaluate actual Lithuanian, Estonian and Latvian defence concepts feasibility to counter threats emerging from RNSS and implications for the Baltic States' military security.

1. Main threats emerging from RNSS towards the 3Bs

The realisation of RNSS is ensured by consolidation of all national instruments of power to defend Russia's national interests and to pre-empt internal and external threats which comprises wide range of threats towards 3Bs. Senior Military Analyst of Virginian National Institute for Public Policy Ciziunas argues that 'since 1991 Russia has been attempting to outline its identity where it has seen itself as a great power in a shifting international security environment while three Baltic countries were seen as a buffer zone against West' (Ciziunas, 2008, p. 287). This faith is reflected through Russia's attempts to influence the 3Bs policies which are considered as part of Russia's sphere of interests and influence (Ciziunas, 2008, p. 287). Additionally Ciziunas argue that to ensure its national interests Russia has tried to influence Baltic States through a number of political and economic pressure, propaganda, economic leverage and energy controls, exploiting ethnic and social discontent as well discrediting governments via political influence (Ciziunas, 2008, p. 287). Later in 2009 RNSS outlined strategic objectives, national interests and ways to achieve them which has been replaced in 2015 by adopting new 'Russia's National Security Strategy (NSS)'. According to the New York University professor Galeotti the new RF NSS's tone reflects 'Russia's new antagonism with the West', but fundamentally strategy remained unchanged (Galeotti, 2016). Further he contemplates that the Russia's drive for the success in future security is based on the protection of its own interests and territorial integrity by non-military methods and if it fails by use of military means including nuclear weapons against existential threat (Galeotti, 2016).

¹⁶ Military, Political, Economic, Civil.

Additionally BALDEFCOL faculty member Romanovs shares similar point of view that RF transformation into the of world leaders¹⁷ causes ultimate changes in Europe as illustrated in ongoing Russian aggression in Ukraine (Romanovs, 2015, p. 44). However, Galeotti suggests that NSS like RNSS is considerably dedicated to issues such as financial stability, health, economic, education and so on, because Moscow is fully aware that these concerns influence security domain (Galeotti, 2016). For example declining demographic and poor health weakens RF conscript pool and reserve of human resources, economic decline reduce defence budgets and social expenditure which produces public unrest. Indeed Galeotti claims that in several ways Moscow demonstrates its conceptual advance in realising that security and governance are basically inseparable therefore 'Russia's hybrid warfare is a rational reflection of that understanding' (Galeotti, 2016). This understanding of the contemporary full spectrum 'political-informational-economic battlespace' is still unappreciated by their Western counterparts *is 'not necessary a military threat to West'* (Galeotti, 2016).

This view is mirrored in the RF Military Doctrine para 5 which explicitly mentions that RF is committed to implement military measures to protect its national interests only after political, diplomatic, legal, economic, informational and other non-violent instruments have been exhausted (RF, 2014). This approach exemplified by aggression against Ukraine has increased concerns in Estonia, Latvia and Lithuania. The 3Bs are EU and NATO members therefore enjoy protection by NATO collective defence and the EU 'Common Foreign and Security Policy (CFSP)' and 'Common Security and Defence Policy (CSDP)'. Nevertheless, 3Bs are smallest and geographically most vulnerable their members. This fact has led to increase interests not only in Russia's traditional military threats but also in other forms of threats against the 3Bs which could be found in both security strategies as pretext for the aggression. Further analysis of RNSS and NSS revealed RF fundamental coercion areas towards Baltic States which are considered as threats to Russian national interests and consequently could be best exemplified by 2008 Georgian war, 2013 annexation of Crimea and ongoing Ukrainian crisis. They are as follow:

¹⁷ RNSS §1.

1. Expansion of NATO, its infrastructure, increasing military activities close to Russian borders are unacceptable and constitute direct military threat especially towards Kaliningrad area¹⁸.
2. Effective defence of the rights and lawful interests of Russian citizens abroad¹⁹ poses direct threat towards Latvia (24%) and Estonia (27%) because of large numbers of Russians compared to Lithuania (6%) (Central Statistical Bureau of Latvia, 2011, Statistics Estonia, 2012 and Statistics Lithuania, 2011).
3. Attempts to revise Russia's role and place in world history²⁰ including different views and interpretation of Molotov-Ribbentrop pact (1939) which enslaved Eastern Europe and led to the Second World War.
4. Finally both Russian strategies includes consolidation of political, military, diplomatic, economic, information and other means, directed towards the defence of Moscow's national interests²¹.

In fact Lithuanian foreign minister Linkevicius caught the essence of the 3Bs threats saying that 'the Ukrainian conflict is a major breach of rules by Russia not just a simple deviation of views, "but grabbing pieces of land and keeping them not to be confused with peacekeeping" (Linkevicius, 2014). According to him Russian realized its aggression by fully utilizing of political, military, economic and energy means, including ruthless info-warfare, encouraging of separatism and terrorism and supplying them with weapons (Linkevicius, 2014). It reflects new Russian nonlinear approach to conflict so called Gerasimov doctrine. RF Chief of the General Staff General Gerasimov claims that rules of war are changed and most important fact is that in many cases 'non-military means exceeds the power of military force in their effectiveness in reaching political and strategic goals' as exemplified in annexation of Crimea (Gerasimov, 2013). This appreciation that all conflicts are only means to the political ends leads to the conclusion that actual use of force is irrelevant if non-

¹⁸ RNSS §17 and NSS §16, §17, §106.

¹⁹ RNSS §38 and NSS §44.

²⁰ RNSS §81 and NSS §79.

²¹ RNSS §98 and NSS §30, §31, §36.

military means can reach the goal more effectively. Therefore Russia must increasingly 'look for non-military instruments such as the wide use of political, economic, informational, humanitarian and other non-military means in conjunction with coordinated protest potential of the population' (Gerasimov, 2013). Furthermore Gerasimov emphasises the use of concealed character of supplementing military means, including information operations and use of Special Force while open use of force is expected just under the auspice of peacekeeping in crisis regulation (Gerasimov, 2013). However peace is restored only to a particular stage to achieve ultimate goals and success in the conflict (Gerasimov, 2013). This approach is not really new as exemplified in long standing and current Russian peacekeeping operations in Transnistria (Moldova), South Ossetia and Abkhazia (Georgia) and ongoing implementation of Minsk agreement in eastern Ukraine.

Now then the concept of Russian aggression is defined it is right time to summarize the actual situation in 3Bs and highlight potential threats. First, the 3Bs are member of former Soviet Union therefore fall under the Russia's national interest which could be protected by all means necessary. Second, Latvia and Estonia have large number of Russian citizens/compatriots, while Lithuania stands in the way to Kaliningrad District, so Russia could decide to protect its citizens abroad. Third, 3Bs have small armed forces and see themselves vulnerable despite being NATO and EU members (see Annex 1). For that reason if Russian could launch an aggression against 3Bs it is likely to take non-linear form according the Gerasimov doctrine to avoid triggering NATO Article V. Fourth, Russian economic sanctions against one or all Baltic States has become rather regular especially in energy, transportation and trade fields which were used to promote Russia's agenda. Fifth, Russian companies are increasingly trying to dominate media industry in 3Bs and support Russian agenda. In that context very sensitive topic is concerning the opposing views on the Soviet Union occupation of the Baltic States in 1940 as exemplified in the dispute over the Bronze Statue in Tallinn in 2007' (Winnerstig, 2014, p. 19). And finally, what worries, is expressed by security services about Russian efforts to 'influence policymaking in Baltic States' (Winnerstig, 2014, p. 19). The whole picture indicates that Baltic States are now in the transition from the first hidden/unnoticed, emerging phase to the second sharpening phase in interstate conflict resolution where according to the Gerasimov doctrine military acts only as deterrence element (see Figure 1).

2. Lithuanian, Latvian and Estonian defence concepts.

Lithuania, Latvia and Estonia rely on both EU and NATO which provide security and defence framework in case of crisis or war. Under the 2009 Lisbon Treaty EU adopted a CFSP to generate a military and defence framework for the EU policy which is aiming to establish a common European defence capability and conflict prevention (EU, 2016). Furthermore according to the 1949 North Atlantic Treaty, NATO is aiming to defend the freedom and security of its members through political and military means (NATO, 2015). Therefore Baltic States defence should be viewed within the context of EU and NATO membership.

2.1. Lithuanian defence concept

Lithuanian deterrence strategy is rather declarative, because national means available are inconsistent with its aims in conventional terms to convince an aggressor that any military actions against Lithuania will fail resulting in unacceptable losses. According to the LTU 'Ministry of Defence (MoD)' Lithuanian defence is based on the concept of total, unconditional, individual and collective defence with EU and NATO allies as core of the deterrence strategy (LTU MoD, 2012). This concept involves three main components: deterrence, ensuring national security in peace time and finally individual and collective defence in a war time (LTU MoD, 2012). However, deterrence requires: well-trained, well-armed and capable forces to defend Lithuania against potential aggression (LTU MoD, 2012). Furthermore, as there are no permanently stationed Allied forces on the Lithuania territory it requires well developed 'Host Nation Support (HNS)' system which enables deployment of Allied forces and preparing citizens for total armed defence and unarmed civil resistance (LTU MoD, 2012). According to the official Lithuanian MoD information 'Lithuanian Armed Force (LAF)' in 2015 constituted two brigade size units and small 'Territorial Defence Units (TDF)' (LTU MoD, 2015). In contrast Russian Western Military District constitutes 36 brigade size units from Central Command, 6th and 20th Armies (Hedenskog and Pallin, 2013, p. 58). Furthermore Russian owns extensive conventional offensive and defensive capabilities in contrast with ill equipped LAF (see Annex 1). Finally Lithuanian Defence Budget for 2015 constituted '1.43% (555m €) of GDP' (LTU MoD, 2015). While Russian expenditures constituted '4.4% of GDP

(6425b €) for national defence' (Hedenskog and Pallin, 2013, p. 103-106). It seems illogical that the hundredfold smaller army could be able to deter Russia on its own.

So, according to the defence concept national defence is 'balanced between territorial and collective defence', that implies respond to aggression by conventional and non-conventional means (LTU MoD, 2012). One of the decisive factors to deter potential aggression is attributed to prepare citizens for the total armed defence and 'unarmed civil resistance (UCR)'. UCR falls under the responsibility of Lithuanian government and directly depends on population's will to resist in coordinated manner and allocated resources to fulfil it. Last time successful UCR in Lithuania was observed in 1991 when Moscow has tried to crackdown on Lithuanian's aspiration for independence (BBC, 1991). Subsequently, effective deterrence depends not on LAF capabilities alone or defence concept itself but rather on government's and population's will to resist, on EU and NATO allies' actions, and how potential aggressor perceives this deterrence. Therefore, TDF which are composed of volunteers and perceived as both military and civilians at once would form base for local military resistance which is likely to be decisive in case of crisis as exemplified in 1939 Russian winter war against Finland (Howard, 2016). In addition due to the changing character of threats LAF together with supporting institutions shall respond to non-military and military threats occurring in the peacetime and provide military assistance to civilian authority (LTU MoD, 2012). According to legislation, employment of LAF in peace time is legal only on request of civilian authority to assist and manage extraordinary situations within Lithuanian territory in supporting role²² (LTU Parliament, 2011).

However Ukrainian example revealed a need to deploy armed forces in very quick and firm manner against hybrid warfare threats in peace time. Regulations on how to deal in such situations were implemented in 2014 and exercised in 2015 during an exercise Lightning Strike 2015 (LTU JHQ, 2015). Analysis of LAF military capabilities in conjunction with working procedures, political will and readiness to employ it in response to military threats could be assessed as 'well balanced and appropriate'

²² Reinforcing Border police in protection of LTU border, reinforce police and internal security force to protect key infrastructure, search and rescue and etc.

(LTU JHQ, 2015). In spite of the fact that LAF is relative prepared to act against hybrid threats in initial stages and provide assistance to civilian authority it seems doubtful that Lithuania could seriously deter potential aggressor on its own. For this reason, the military security environment suggests that LAF will be required to take initial independent defence influenced by the geographical distinctiveness similar as Latvia and Estonia. That implies that LAF should be capable to sustain prolonged war and TDF are better suited and self-sustainable for this task as they know area and people, if they are trained and equipped to fight conventional warfare by using guerrilla warfare²³. Ukrainian crisis revealed that potential aggressor could instigate aggression as non-international and therefore short in preconditions to activate of NATO Article V. Therefore in case of aggression similar like in Ukraine LAF should defend territorial integrity individually (LTU MoD, 2012). In summary Lithuanian defence concept is relative well balanced to face peace time challenges; however recipe to deter Russia is not justified with reasonable resources. The situation implies that greater utilisation of TDF in more efficient way, especially to fight superior aggressor by using irregular warfare methods needs to be reconsidered.

2.2. Latvian defence concept

If properly developed 'Latvian National Guard (LNG)' as TDF could become credible preventive measure to deter potential threats or as self-defence capabilities reinforcing 'National Armed Forces (NAF)' with modern capabilities and effective personnel reserve. Latvian's defence concept is laid down as a comprehensive State defence based on expeditionary Armed Force and relatively large and quickly accessible mobilization of reserves (Cabinet of Ministers of the Republic of Latvia, 2012). Moreover NAF together with state institutions, local governments and society must conduct defence in support of the arrival and deployment of allied forces (Cabinet of Ministers of the Republic of Latvia, 2012). It requires NAF to guaranty early warning, military preventive measures, self-defence capabilities and HNS for deployment of Allied forces (Cabinet of Ministers of the Republic of Latvia, 2012). Consequently the ultimate strategic tenet is to 'minimise potential threats to national security by preventing, defeating and overcoming them' (Cabinet of Ministers of the

²³ Currently LTU TDF is not tasked to conduct such a task in war time.

Republic of Latvia, 2012). However, Research fellow of Latvian Institute of International Affairs Rublovskis argues that NAF current institutional structure with total force less than 5000 troops in conjunction with low GDP allocated for defence resulting in situation where NAF is not able to provide modern combat capabilities (Rublovskis, 2014).

Furthermore, Rublovskis claims that in the case of conventional or unconventional war the current form of NAF and its command and control structures would 'cease to exist' (Rublovskis, 2014). Moreover anticipated early warning system, which was aiming to allow NAF to prepare for the war, is losing its relevance as warning timings become too short to meet required preparations. For example RAND's Shlapak and Johnson's wargaming suggest that in conventional terms 'Russia could be able to reach the outskirts of Tallinn and Riga within 36-60 hours' (Shlapak and Johnson, 2016, p. 4-5). Taking into an account that Russia is periodically conducting snap exercises along borders of 3Bs as exemplified in 'Western Military District "Complex" Readiness Exercise in 2014 involving approx. 150,000 troops (Norberg, 2015, p. 75). Consequently, no early warning system will be able to warn early enough to prepare the state for war (Norberg, 2015, p. 75). This situation implies that military preventive measures should be in place or ready to be employed within very short time what are not in line with the expeditionary armed force concept. Nonetheless LNG, which is aiming to strengthen NAF military capabilities, could potentially be developed in both fields as important military preventive measure and as a self-defence capability to act in early stages based on its permanence.

In addition, Rublovskis argues that the lack of financial resources and declining demographic situation will have negative impact on NAF manning causing 'deficiency in recruiting and maintaining required number of qualified personnel and reserve' (Rublovskis, 2014). This implies that the development priorities of NAF operational capabilities should be reassessed involving further development of LNG. If developed properly LNG potentially could act as source to train and maintain adequate NAF reserve. Furthermore, LNG aspect of TDF aggregates civilian population and integrates it into the national security matters which just by active presence minimise potential military threats. Finally LNG could be employed as deterrence measure and if required as self-defence capability to act in early stages of hybrid war because of its local knowledge and permanence.

2.3. Estonian defence concept

Estonian defence concept is well managed and resourced, but requires integration of Russian minorities into defence force, otherwise they will continue to constitute ground for Russian intervention. Estonian defence concept is based on the tenet of sufficient defence capabilities to guarantee State's sovereignty which relies on both territorial and non-territorial units for initial independent defence capability and on NATO's collective defence (EST MoD, 2011, p. 10-11). It envisions principal of total defence as basis for collective defence in case of surprising attack and provision of military assistance to civilian authority in case of emergency in both peace and war times (Parliament of Estonia, 2010, p. 13). This concept basically requires to ensure control of territory, to provide early warning, HNS, efficient reserve force and mobilisation system and finally to develop mobile, modern, sustainable and rapid response units (Parliament of Estonia, 2010, p. 14). According to the Junior Fellow of the 'Centre for Eastern Studies (OSW)' Szymanski:

Estonian defence concept is backed up with wide consensus to allocate NATO's 2% of GDP for defence as a precondition to develop mobile, modern, sustainable and rapid response units. (...) Estonia's decisions to keep its conscription system and maintain the TDF (Kaitseliit) as a traditional volunteer formation proved to be correct in long term (2015).

Currently Estonian Defence Force consists of approx. 6,000 professional troops and 15,000 TDF troops (see annex 1) being a reliable force (Estonian defence force, n.d.). However there are two major issues to solve. Firstly integration of Russian minorities (same as in Latvia) with following assimilation into both country's life and armed force especially into TDF, and secondly with 16 days of training per year TDF cannot reach the same level as professional troops (Szymanski, P, 2015). This implies that TDF should prioritize their training to those vital areas for initial independent defence and try to involve Russian minorities. According to the Estonian MoD conscription will remain the main source of reserves generating efficient readiness and mobilisation system which in conjunction with early warning and command and control will allow initial independent defence capability (Estonian MoD, 2011, p. 12). The most important requirement is rapid reaction especially in case of surprising attack and TDF are well suited for this purpose as TDF members are living and working in respective areas. Ongoing crisis in Ukraine revealed necessity to

defend key infrastructure which according to the Estonian MoD are precondition for collective defence (Estonian MoD, 2011, p. 11). Therefore Szymanski argues that:

Estonia's decision to align TDF with regular force by providing TDF formations with similar equipment to the regular forces has far reaching positive consequences. In chasing for security Estonia continues to develop TDF anti-tank capabilities, by 2022 intent to increase number of TDF members to 30,000 and finally battalion size units are to be replaced by more mobile company size units which are recruited from locals. Furthermore, to increase reaction time TDF staff would like to raise authorised TDF members who allowed to keep their personal weapons and ammunition at home to 75% (2015).

To summarize Estonia's defence concept mirrors Finnish defence model by absorbing the principles of total defence, conscription with professional element and most important classic TDF which in current situation suits the best in order to counter threats posed by RNNS.

3. Conclusions

Changing security environment, unfriendly neighbour driven by their national interests, diverse view of history and minority issues will continue to dictate 3Bs defence concepts. Therefore it must be constantly adapted to adequately meet actual security challenges. The evidences suggest that in current security environment 3Bs are dependent on NATO's deterrence and collective defence in case of a crisis. However absence of permanent Allies troops in Baltics and geographical peculiarity prescribes that 3Bs must retain initial independent defence capability in case of a surprising attack as prerequisite for collective defence or as defence against non-linear war. In spite of this view Lithuania and Latvia, unlike Estonia, put expeditionary capabilities higher priority over TDF though it is obvious that importance of TDF is increasing for both 3Bs and NATO. In case of attack against 3Bs NATO should respond militarily and expel aggressor or accept Russian strategic victory leading to catastrophic consequences for alliance. Therefore it is so important to deter and if failed to expel an aggressor, however conventional approach to preposition of substantial force is rather demanding. Because it would require indefensible funding, would be pretext for escalation and vulnerable for pre-emptive strike. Otherwise deploy it immediately after the crisis breaks out due to the slow NATO decision making would give an aggressor time to achieve its objectives and becomes challenging due to the Russian's anti-access and anti-denial capabilities. Resulting in

the situation, that in all cases 3Bs will be responsible for the initial independent defence with all national means available.

Consequently, Russian superiority in case of linear warfare should be fought by exploiting its weakness and using own strengths such as sabotage and guerrilla warfare. Therefore, if properly trained and equipped TDF could operate independently or according to the national defence plan in support of professional armed force. Furthermore it could support civilian authority or operate in decentralized and aggressive civilian resistance or even organize it. If successful, such an approach disrupts aggressors land lines of communication, damage command and control infrastructure, slows down dig in and denies easy victory by buying time for Allies to fight back. Such an approach in conjunction with political will and comprehensive defence approach go over traditional TDF efforts. Therefore an integrated defence concept would serve both ways to deter and if failed to defend. In fact such a defence concept should be integrated into national security strategy to make best use of single elements by putting them together into an all-encompassing defence strategy which aims primarily to deter potential aggressor.

Bibliography

BBC, 1991. 1991: Bloodshed at Lithuanian TV station. [online] Available at: http://news.bbc.co.uk/onthisday/hi/dates/stories/january/13/newsid_4059000/4059959.stm [Accessed 2 December 2015].

Cabinet of Ministers of the Republic of Latvia, 2012. The State Defence Concept. Approved by the Saeima (Parliament) on 10 May 2012. [online] Available at: http://www.mod.gov.lv/~media/AM/Par_aizsardzibas_nozari/Plani,%20konceptijas/2012_va_EN.ashx [Accessed 24 January 2016].

Central Statistical Bureau of Latvia, 2011. Population and Housing Census 2011 [online] Available at: <http://www.csb.gov.lv/en/notikumi/key-provisional-results-population-and-housing-census-2011-33306.html> [Accessed 1 February 2016].

CIA, 2015. The World Factbook [online] Available at: <https://www.cia.gov/library/publications/the-world-factbook/> [Accessed 23 January 2016].

Ciziunas, P., 2008. Comparative Strategy. Russia and the Baltic States: Is Russian Imperialism Dead?, p. 287. [online] Available at: <http://www.tandfonline.com/loi/ucst20#.VpVZY1LUjIU> [Accessed 15 December 2015].

Connell, M.E. and Evans, R., 2015. Russia's "Ambiguous Warfare" and Implications for the U.S. Marine Corps. CNA's Occasional Paper., p. 5. [online] Available at: https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf [Accessed 15 January 2016].

David A., Shlapak, D.A. and Johnson M.W., 2016. Reinforcing Deterrence on NATO's Eastern Flank. Wargaming the Defense of the Baltics. Rand corporation. [online] Available at: http://www.rand.org/pubs/research_reports/RR1253.html [Accessed 9 February 2016].

Donaldson, R.H., and Noguee, J.L., 2002. The Foreign Policy of Russia: Changing Systems, Enduring Interests, 2nd ed. Armonk. M. E. Sharpe.

Estonian defence force, n.d. Estonian Defence Forces. [online] Available at: <http://www.mil.ee/en/defence-forces> [Accessed 9 February 2016].

Estonian MoD, 2011. National Defence Strategy of Estonia. [online] Available at: http://www.kaitseministeerium.ee/sites/default/files/elfinder/article_files/national_defence_strategy.pdf [Accessed 12 February 2016].

EU, 2016. Foreign & Security Policy. [online] Available at: http://europa.eu/pol/cfsp/index_en.htm [Accessed 12 February 2016].

Galeotti, M. 2016. Russia's New National Security Strategy: Familiar Themes, Gaudy Rhetoric. [online] Available at: <http://warontherocks.com/2016/01/russias-new->

national-security-strategy-familiar-themes-gaudy-rhetoric/ [Accessed 9 January 2016].

Gerasimov [Герасимов], V., 2013. The Value of Science in Prediction. Military-Industrial Kurier, February 27, 2013 Nr. 8 (476). [online] Available at: <http://www.vpk-news.ru/articles/14632> [Accessed 15 January 2016].

Global Firepower, 2016. Countries Ranked by Military Strength. [online] Available at: <http://www.globalfirepower.com/countries-listing.asp> [Accessed 23 January 2016].

Hedenskog, J. and Pallin, C. V., 2013. Russian Military Capability in a Ten-Year Perspective – 2013. FOI. [online] Available at: <http://www.foi.se/templates/Pages/DownloadReport.aspx?FileName=\\4afd4665-7fca-451e-bdd6-d0ce7107c38a.pdf&rNo=FOI-R--3734--SE> [Accessed 10 November 2015].

Howard, E. 2016. Lithuania's key role in countering Russian A2/AD challenge to Baltics. Delfi by The Lithuanian Tribune. [online] Available at: <http://en.delfi.lt/opinion/lithuanias-key-role-in-countering-russian-a2ad-challenge-to-baltics.d?id=70576206> [Accessed 3 March 2016].

Ioffe, J., 2015. Exclusive: The Pentagon Is Preparing New War Plans for a Baltic Battle Against Russia. Foreign Policy. [online] Available at: <http://foreignpolicy.com/2015/09/18/exclusive-the-pentagon-is-preparing-new-war-plans-for-a-baltic-battle-against-russia/> [Accessed 2 December 2015].

Linkevicius [Linkevičius], L., 2014. Putin has defended the Nazi-Soviet pact. Time for the west to wake up. The Guardian. [online] Available at: <http://www.theguardian.com/commentis-free/2014/nov/07/vladimir-putin-defended-nazi-soviet-pact-west-world-war-two> [Accessed 15 December 2015].

LTU Parliament, 2011. Law for organization of national defence system and military service [Krašto apsaugos sistemos organizavimo ir karo tarnybos įstatymas], 2011. Approved by Lithuanian Parliament No. VIII-723. [online] Available at: http://www3.lrs.lt/pls/inter3/dokpaieska.showdoc_bin?p_id=416354 [Accessed 2 December 2015].

LTU JHQ, 2015. Main Lithuanian national exercise “Lightning Strike 2015”. [online] Available at: <http://www.jungtinisstabas.lt/lt/nacionalines-pratybos/zaibo-kirtis-2015/> [Accessed 2 December 2015].

LTU MoD, 2012. The Military Strategy of the Republic of Lithuania. Approved by Order No. V-1305 of the Minister of National Defence of the Republic of Lithuania on November 22, 2012. [online] Available at: [http://www.kam.lt/download/32127/the%20military%20strategy%20\(3\).doc](http://www.kam.lt/download/32127/the%20military%20strategy%20(3).doc) [Accessed 2 December 2015].

LTU MoD, 2015. Numbers and Facts. [online] Available at: http://www.kam.lt/lt/personalo_politika_512/skaiciai_ir_faktai_537.html [Accessed 2 December 2015].

NATO, 2015. The founding treaty. [online] Available at: http://www.nato.int/cps/iw/natohq/topics_67656.htm [Accessed 2 December 2015].

Norberg, J., 2015. Training to Fight – Russia’s Major Military Exercises 2011–2014. FOI., p. 75 [online] Available at: <http://www.foi.se/sv/Sok/Sammanfattningssida/?rNo=FOI-R--4128--SE> [Accessed 9 February 2016].

Parliament of Estonia, 2010. National Security Concept of Estonia., p. 13-14 [online] Available at: http://www.vm.ee/sites/default/files/content-editors/JPA_2010_ENG.pdf [Accessed 12 February 2016].

Putin, V., 2014. Excerpts from transcript of the final plenary meeting of the Valdai International Discussion Club’s XI session. [online] Available at: <http://en.kremlin.ru/events/president/news/46860> [Accessed 2 December 2015].

Romanovs, U., 2015. The means and ends of Russia’s security strategy., p. 44. [online] Available at: <http://liia.lv/en/publications/riga-dialogue-towards-a-shared-security-environment/> [Accessed 10 January 2016].

Rublovskis, R., 2014. Current challenges for the Latvian Defence System in Light of the Ukraine Conflict. *Diplomaatia*. No. 129, May 2014. [online] Available at: <http://www.diplomaatia.ee/en/article/current-challenges-for-the-latvian-defence-system-in-light-of-the-ukraine-conflict/> [Accessed 23 January 2016].

Russian MoD website, n.a. Russia's participation in peacekeeping operations. online] Available at: http://eng.mil.ru/en/mission/peacekeeping_operations.htm [Accessed 14 January 2016].

Stockholm International Peace Research Institute, 2015. SIPRI Military Expenditure Database. [online] Available at: http://www.sipri.org/research/armaments/milex/milex_database/milex-data-1988-2014 [Accessed 23 January 2016].

Szymanski [Szymański], P., 2015. The Baltic States' Territorial Defence Forces in the face of hybrid threats. OSW Commentary. [online] Available at: <http://www.osw.waw.pl/en/publikacje/osw-commentary/2015-03-20/baltic-states-territorial-defence-forces-face-hybrid-threats> [Accessed 10 February 2016].

The Security Council of the Russian Federation, 2009. Russian National Security Strategy to 2020. [Совет Безопасности Российской Федерации, 2009. Стратегия национальной безопасности Российской Федерации до 2020 года, утверждена Указом Президента Российской Федерации от 12 мая 2009 г. № 537] [online] <http://www.scrf.gov.ru/documents/99.html> [Accessed 10 November 2015].

The Security Council of the Russian Federation, 2014. The Military Doctrine of the Russian Federation. Approved by the President of the Russian Federation on December 25, 2014 No. Pr.-2976. [online] Available at: <http://www.theatrum-belli.com/the-military-doctrine-of-the-russian-federation/> [Accessed 9 January 2016].

The Security Council of the Russian Federation, 2015. Russian Federation National Security Strategy. Moscow [Стратегия национальной безопасности Российской Федерации, утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. № 683] [online] Available at: <http://kremlin.ru/acts/news/51129> [Accessed 9 January 2016].

Statistics Estonia, 2012. Native languages spoken in Estonia [online] Available at: http://www.stat.ee/64629?parent_id=39113 [Accessed 1 February 2016].

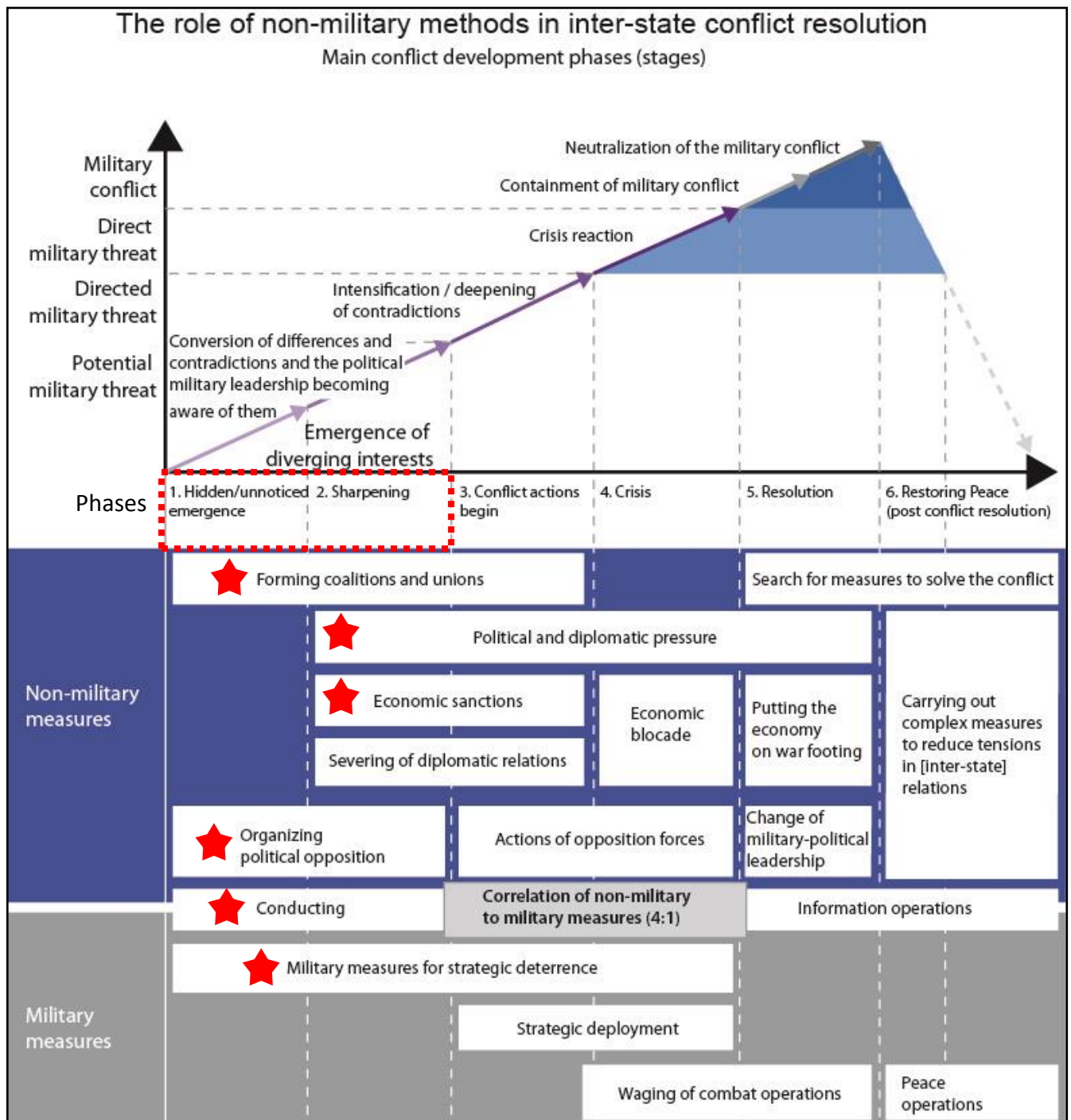
Statistics Lithuania, 2011. Ethnicity, mother tongue and religion [online] Available at: http://statistics.bookdesign.lt/dalis_04.pdf [Accessed 1 February 2016].

Winnerstig, M., 2014. Tools of Destabilization. Russian “Soft Power” and Non-military Influence in the Baltic States. FOI-R--3990—SE., p. 19. [online] Available at: http://www.google.lt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwiwy-6VtqrKAhWGfg8KHRXYC7kQFggfMAA&url=http%3A%2F%2Fwww.foi.se%2FReportFiles%2Ffoir_3990.pdf&usg=AFQjCNEgJZfsLvm1x-hiCtWJluaPTixQ8A [Accessed 15 January 2016].

Annex 1. Contextual base line of military capabilities covering time period from 2013 to 2015 expressed in absolute numbers.

	Lithuania	Latvia	Estonia	EU	NATO	Russia
Population (CIA, 2015).	2,884,433	1,986,705	1,265,420	510,540,617	906,002,051	142,423,773
GDP (US\$) (CIA, 2015).	79,93 billion	48,36 billion	36,78 billion	16,63 trillion	37,480 trillion	3,577 trillion
Military expenses in 2014 (US\$ billion) (Stockholm International Peace Research Institute, 2015).	0,377	0,299	0,509	303	919,917	84
Troops number (active) (Global Firepower, 2016).	~14,900	~6,000	~6,000	~1,691,217	~3,585,000	~771,000
Major military equipment (Global Firepower, 2016).						
Total Naval Strength	12	18	6	1,521	1,783	352
Total Aircraft	10	4	6	6,740	21,699	3,429
Tanks	0	0	0	6,691	19,124	15,398
Armoured Fighting Vehicles (AFVs)	432	250	318	48,971	97,738	31,298
Self-Propelled Guns (SPGs)	0	0	0	2,312	5,140	5,972
Towed-Artillery	54	20	66	3,492	4,928	4,625
Multiple-Launch Rocket Systems (MLRSs)	0	0	0	1,069	3,153	3,793

Figure 1. Gerasimov's concepts of hybrid warfare (Connell and Evans, 2015, p.5).



Legend:

Deployed measures indicator ★

Is Russia a strong or a weak power?

MAJ Davit Aghabekyan

Introduction

Recent Russian activity in the international arena such as the annexation of Crimea followed by indirect involvement in Ukrainian armed conflict, as well as direct intervention in the Syrian civil war by mass airstrike's provides cause for reflection. Alleged Russian military support to separatists in Ukraine increases, a new wave of contention between the West and Russia. This raises the question, whether Russia is strong or weak? The answer is sophisticated due to there not being an exact definition of a weak or a strong country. Dr. Querine Hanlon claims: 'Strong, weak, failing, or failed states are defined (1) by their ability to control their own territory, (2) by their capacity to perform core functions, and (3) by their vulnerability to challenges to their legitimacy' (Hanlon, 2011). One may disagree with this statement, however history of some strong but fallen states can justify that claim. This essay will find some concurrences of the political system of the former Union of Soviet Socialist Republics (USSR) and the contemporary Russian Federation (RF) which led USSR to fail.

The USSR had ability to control its own territory due to strength of armed forces backed by a huge arsenal of weapons of mass destruction (WMD). Furthermore, Moscow was able to influence on international geopolitics and threatening the sovereignty on formally independent countries. However, at the same time population of the USSR had been suffering because of economic deficit and high level of corruption, which was a common aspect of the life. On this stage Moscow was not able or was not willing to perform its core functions by providing economic stability and appropriate productive struggle against corruption. One may argue that military power was enough to consider the USSR as a strong country. Probably it was, but only for the short term. Leon Aron quotes the last leader of USSR Gorbachev's interview:

The Soviet model was defeated not only on the economic and social levels; it was defeated on a cultural level. Our society ... rejected that model on the cultural level because it does not respect the man, oppresses him spiritually and politically (Aron, 2011).

The collapse of the USSR is a clear example of the fact that a strong state should not only enhance military power, but should also consider the economic development of the state and respect its citizens as well. Nevertheless, after the collapse of the USSR population of fifteen independent countries looked on to a life from the different angle with Russia among those states. On December 12, 1993 in nationwide referendum Russia adopted its constitution. According to that constitution a man, his rights and freedoms are the supreme values; the recognition, observance and protection of the rights and freedoms of man and citizen shall be the obligation of the State (The Constitution of the Russian Federation, 1993). The Russian Constitution based upon democratic values such as liberty, equality and justice. However, the government of Russia instead of obtaining all benefits of free market to improve the economic situation and build democratic institutions in the state began to raise military expenditure and violate human rights, thus repeating USSR history.

The desire of an average citizen of any country in the world might be security, economic prosperity, justice, freedom of expression and speech, protection of human rights. In his speech in Cairo, President Obama argues that:

... all people yearn for certain things: the ability to speak your mind and have a say in how you are governed; confidence in the rule of law and the equal administration of justice; government that is transparent and doesn't steal from the people; the freedom to live as you choose (Obama, 2009).

One might argue that among above mentioned factors Russia succeeds in security in terms of technologically advanced armed forces and that is enough to be defined as a strong state. However, this essay will argue that despite of modernized and combat-ready military Russia is a weak power because of a fragile economy, questionable democratic values and demographic problems.

Modernized and combat-ready military

Putin with his actions in an international environment impressed officials who thought that greater military capabilities of Russia left far behind in the past and contemporary armed forces of Russia something other than the remnants of the former power. Current air strikes and launched surface to surface missiles in Syria verified Moscow's determinations to reveal the present capability of Russian armed forces to

the international society. This is how Lt. Gen. Ben Hodges, the commander of United States Army forces in Europe responds to Russia's modern military capabilities: 'What continues to impress me is their ability to move a lot of stuff real far, real fast' (Lee Mayers, et al., 2015).

Regardless of CNN media reports claiming about the vast amount of casualties among civilian population in western Syria caused by Russian airstrike's (Mullen, 2015), military forces loyal to Syrian President Bashar al-Assad took great advantage of it and seized several strategic villages and towns south of Aleppo in northern Syria (ARA news, 2015). Andrew Bowen writes: 'To Putin, an important state will not only have a modern military, but be able to display it through exercises and demonstrations' (Bowen, 2013).

After dissolution of USSR, Russia became legatee of it with all obligations and huge military resources including biggest arsenal of WMD (Federation of American Scientists, n.d.). However, due to political and economic instability in the country at the end of the twenty century Russia was not able to develop armed forces and they remained at the lowest level of combat readiness. Military operations in Chechnya certainly demonstrated above mentioned conditions of Russian armed forces. Generals were not able to analyse the situation properly and adapt armed forces to the demands of guerrilla warfare, but they just relied on a huge military power stayed after the collapse of the USSR and wished to complete campaign in short duration. At the same time, Chechen insurgents were able to fight successfully against state's conventional forces despite of lack of armament and manpower. Furthermore, the high level of corruption played a significant role in that campaign, especially in the first Chechen war. Mansur Mirovalev claims that: 'The fighters, in turn, blackmail corrupt officials who embezzle lavish funds from Moscow' (Mirovalev, 2014). Eventually the Russia's armed forces were able to overcome the insurgents and stabilise the North Caucasus by employing all tough military power.

Moscow's great power ambition remained as a core challenge for foreign policy. In spite of the country being in a weak, declining economic condition, Russian foreign minister Primakov in January 1996 declared: 'Russia has been and remains a great power, and its policy toward the outside world should correspond to that status' (Donaldson, 2000). The statement became more realistic after election of new

President Vladimir Putin in 2000. As Andrew Bowen writes: ‘..., Putin has launched an ambitious military *modernizatsii* [modernization] program and seeks to create a modern force that is not only professional, but is able to project Russia’s ambitions and interests’ (Bowen, 2013). Richard A. Bitzinger argues: ‘The arms industry suffered considerably after the collapse of the Soviet Union in the early 1990s and subsequent years of neglect due to a precipitous drop in military spending’(Bitzinger, 2015). Nevertheless, during the time armed forces had been able to slowly recover some of its former authority, capability, and operational efficiency. Despite of progress, the war with Georgia in 2008 exposed numerous obvious insufficiencies, particularly in command and control structure, thus justified the requirements of innovation. During that conflict Russian armed forces were still organised within the large divisions which were designed to conduct conventional battles against opposing NATO armed forces. In spite of its mighty size, army was not able to react to a rising armed conflict with significant demands of well synchronized operations, but to fight large tank battles. Moscow applied lessons learned after the war and large bulky divisions were changed to brigade size units. The reforms continued and six military districts were converted to four operational strategic commands. According to Andrew Bowen the military modernization State Armament Program (SAP-2020) initiated by Putin had pursued to finance \$773 billion by 2020 and overall goal is to arm 70% of the Russian military with modern weaponry such as 350 new fighter jets, including the new fifth generation T-50 fighter, some 1000 helicopters, 54 surface ships and 24 new submarines, including “Borei” class ballistic missile submarine and additional nuclear strike capabilities which includes designing a new Inter Continental Ballistic Missiles, the RS-26 (Bowen, 2013).

In accordance with the Global Fire Power, military expenses of Russia in 2015 were about \$47 billion, which is roughly three times less than the military budget of China and about twelve times less than the military budget of the US (Global Fire Power, 2015). Therefore, fragile economy of Russia has direct impact on the plans of Moscow to modernize 70% of weaponry in army by 2020. Nevertheless, despite of a declining economy in Russia, Putin is not only keeping the development of armed force capability, but he continues to increase military expenditures to his enormous military project. According to Admiral Vladimir Komoyedov, the Duma plans to spend 3.1 trillion roubles (\$76 billion), or 3.7 percent of gross domestic products (GDP), on

defense in 2016 and 3.23 trillion (\$79 billion), or 3.6 percent of GDP, in 2017' (The Moscow Times, 2014a). Justification of Russian improvement in military industry might be the argument that RF is a second exporter of the weaponry in the world. Moreover, according to BBC's released information Russia sells 27% of all armaments in the globe (BBC, 2015a).

The last but not least important stage of improvement is the transition of the conscript consisting army to contract professional soldiers army. According to Andrew Bowen by 2017 number of professionals in the army should reach up to 425,000 soldiers, however the amounts of so called *kontraktniki* [contractors] in military by 2013 was about 200,000 and a consequential goal of 425,000 professionals by 2017 remains under question due to demographic problems which is facing Russia and lack of volunteers to sign contract and become professional soldier (Bowen, 2013).

Although effective improvements of Russian armed forces, Moscow's plan to accomplish the SAP by 2020 is under a big question due to fragile economy and demographic problems.

Fragile economy

RF is the biggest country in the world. As Glenn E. Curtis claims: 'Russia accounts for around 20 percent of the world's production of oil and natural gas and possesses large reserves of both fuels' (Curtis, 1996). In 1991, Russia emerged from the Soviet Union and with big potential of fossil resources began to develop its economy based on global integration and free market with decentralized planning mainly relying on the private sector. In the beginning of 1990s, first president of Russia Boris Yeltsin initiated privatization program in the country and because of it, no less than 70 percent of GDP pertain to the private sector by 1997 (Aslund, 2008). It was a time when Russia's first official billionaire-oligarchs appeared. Nevertheless, at this stage of the reforms Russia has not moved to a new level of economic prosperity. As a senior fellow at the Peterson Institute Anders Aslund argues: 'Because of extraordinary political resistance by rent seekers, ranging from old state enterprise managers to novel oligarchs, Russia had an average budget deficit of 9 percent of GDP from 1993 until 1998' (Aslund, 2008).

After the presidential election in 2000, Putin has stood up at the power of the Russia and with new ideas prolonged economic reorganizations originated by his predecessor. Putin in his annual address to the Federal Assembly in 2002 declared: 'The norm of the international community and the modern world is tough competition—for markets, investments, political, and economic influence... nobody is eager to help us. We have to fight for our place under the economic sun' (Putin, 2002).

Nevertheless, reforms are not significant and as it was in Soviet era main profit to Russian GDP still based on income from the export of gas and oil, therefore it has a direct dependency on world market prices. Walter Laqueur writes:

...the country's economic and municipal infrastructure is very poor, and its dependence on the export of oil... is undesirable and in the long run, dangerous. A lack of economic diversification will make it increasingly difficult for Russia to compete in global markets and maintain its status as a great power (Laqueur, 2010, p. 156).

Attempts initiated by the leaders of Russia to diversify economical dependency from oil and gas were not successful so far. The Wall Street Journal published an article by Greg IP on September 2, 2015 arguing that: '... Prime Minister Dmitry Medvedev had sought to spur innovation to diversify away from oil and gas. But ..., even those diversification efforts depend on subsidies generated by oil and gas' (IP, 2015).

Although economic conditions in the country are far from stable, Putin's reputation in Russia has grown up since its involvement in Syria's military campaign. The propaganda launched by contemporary Russian government reminds hard legacy left by soviet thinking mentality. Bridget Kendall claims: '...the message being pumped out by nationalist Russian media is reminiscent of the propaganda produced in the Soviet Union' (Kendall, 2014). According to a CNN report Putin's popularity reached to a historic maximum 89 percent in June 2015 (Cullinane, 2015).

The sanctions launched by West against Russia deteriorate the economic situation in the country. Mark Agerton argues that: 'As a consequence of the sanctions, the value of the Russian Rouble fell precipitously as nervous investors removed their capital from the country' (Agerton, 2015). However, Moscow applied soft power to divert attention of own population from economic instability in the country. CNN reporter

Susannah Cullinane quotes daughter of assassinated opposition leader Boris Nemtsov, Zhanna Nemtsova: 'Putin has two truths: He has oil price and propaganda. Now oil prices fell down. They lost half of its value. Now he has only one tool left, and that is propaganda. And that is why he is so popular in Russia' (Cullinane, 2015). The Business Insider in a 2014 published article regarding Russian economic dependency on gas and oil. According to that source roughly 68 percent of all Russian exports in 2013 composed of gas and oil materials to compare with US export revenue where about 60 percent comprised of 122 different items while fuel or heating oil and petroleum products make up just 8 percent (Wile, 2014). Accordingly, the Russia's GDP per capita in 2014 was about 12,735 US dollars, which is more than two times less than Spain (World Bank, n.d.). Nevertheless, Spain's economy is not counted as a strongest among EU partners. The digits become even worse if you would compare with globe leading countries such as the US which GDP per capita in 2014 according to same source was \$54,629. Moreover, according to the Moscow Times average monthly salary across the Russia drop down to 31,200 roubles (\$500) in January 2015 which is 8 percent less than the same month in 2014 and about 50 percent fall in dollar terms due to rapid inflation of Russian national currency (Spinella, 2015). One may argue that size of population of Spain and Russia is not the same; therefore Spain's GDP per capita is more than in Russia. However, this number represents the people, which should be foundation of the country and as it was mentioned in Dr. Hanlon's argument, strong country differs by its ability to perform core function, in this case by facilitating economic prosperity of the own population, which has not been achieved so far.

Questionable democratic values

Although the democratic values are quite broad topic to discuss, this essay will slightly touch some of them such as human rights and freedom of speech. Article 19 of Chapter 2 of the Russian constitution states that:

The State shall guarantee the equality of rights and freedoms of man and citizen, regardless of sex, race, nationality, language, origin, property and official status, place of residence, religion, convictions, membership of public associations, and also of other circumstances (The Constitution of the Russian Federation, 1993).

In addition, according to the RF constitution article 80 President of the RF shall be guarantor of the Constitution, the rights and freedoms of man and citizen (The Constitution of the Russian Federation, 1993). However, behaviour of leader of southern province Chechnya, Ramzan Kadyrov is not equitable with that statement. Amanda Taube quoted chilling directive of Kadyrov to his security officers in April 23, 2015 who said: 'I would like to officially state: Open fire if someone from Moscow or Stavropol — it doesn't matter where from — appears on your turf without your knowledge' (Taube, 2015). The above mentioned statement can explain that even though Chechnya is the part of the RF, Kadyrov is not eager to accept control from Moscow. It is difficult to imagine that kind of performance in other democratic countries. As Amanda Taube writes: 'It is common if unofficial knowledge that Putin and Kadyrov have a deal: Putin installed Kadyrov in power, granting him near-complete autonomy in Chechnya and generous federal subsidies. In return, Kadyrov has ensured that Chechnya does not return to separatist conflict' (Taube, 2015). In other words Chechnya is a country within the country and the claim depicted in article 4 of Constitution that: 'The Constitution of the RF and federal laws shall have supremacy in the whole territory of the RF' (The Constitution of the Russian Federation, 1993) is not applicable in this circumstance and what is written in the constitution is not working in reality.

Another value of democracy which is undermined in Russia is freedom of expression. The article 29 of RF Constitution states that: 'Everyone shall be guaranteed the freedom of ideas and speech' (The Constitution of the Russian Federation, 1993). Nevertheless, according to the BBC, Russian TV is dominated by channels that are either run directly by the state or owned by companies with close links to the Kremlin (BBC, 2015b). In addition, journalists are taking a big risk of physical violence or even be killed if they explore too deeply into delicate issues like corruption. Until recent times the internet was one of the Islands of free expression drifting in media domain. Yet, as Tanya Lokshina claims: 'In December 2013, President Putin signed a law criminalizing public calls to separatism' (Lokshina, 2015). As a result of this law one can face up to five years in the jail if the government decides that one's comments in internet including social network may challenge countries territorial integrity. According to Remi Piet, Federal Service for Supervision in the Sphere of Telecom, Information Technologies and Mass Communications (ROSKOMNADZOR) has

authority to shut down any website labelled as "extremist" - a loosely defined term which could include anything from terrorism to merely disagree with the current regime - as well as imprison people who post alleged calls to extremism (Piet, 2014).

The inherent attributes of a democratic system is the institution of opposition. However, Moscow is not accepting other views rather than one, accepted by the government. The Moscow Times quotes deputy chief of staff Vyacheslav Volodin who said; 'There is no Russia today if there is no Putin' (The Moscow Times, 2014b). According to the Guardian the daughter of the murdered Russian opposition leader, Boris Nemtsov, has accused Vladimir Putin of being "politically responsible" for her father's death; moreover, she said that after his death the opposition is beheaded and everybody is frightened (Quinn, 2015). Yet, the spokesman of Putin declared that the murder of Nemtsov had been 100% provocation intended to make Russia look bad and the president has taken personal control of the investigation (Walker, 2015). As a cause for reflection, leader of Chechnya Kadyrov described the man who pulled the trigger as "a hero of Russia" (Walker, 2015).

Analysis of aforementioned arguments drives to conclusions that even if Russia declares to be a democratic state with appropriate constitution, the government in behalf of presidents is not keen to perform its core function, such as constitutional execution guarantees. Therefore, in a country where the law is subservient to the elite and acts selectively eradicated and freedom of speech under various pretexts sooner or later will lead to a political vacuum and cannot be considered as strong state.

Demographic problems

Last but not least important problem to discuss is a demographic challenges faced by post-Soviet Russia. The demographic crises supposed to be related to overall crises after collapse of SU, therefore it is logical to expect demographic equilibrium when the situation is stabilized. However, economy of present Russia since it had emerged from SU is not stable. Moreover, depopulation of Russia especially sparsely populated Siberia has reached enormous dimensions and became one of the priorities of the country. Putin on his annual address to the Federal Assembly in 2006 declared: 'I want to talk about the family, about the most acute problem facing our

country today – the demographic problem.... You know that our country's population is declining by an average of almost 700,000 people a year' (Putin, 2006). The government applies the concept of demographic policy to increase population. As Anatoly Vishnevsky writes: 'It assumes a growth in life expectancy to 75 years by 2025 and in a total fertility rate of up to 1.9-2 children per woman...' (Vishnevsky, 2009). In order to overcome shrinking population, Moscow should solve following challenges; increase fertility, decrease mortality, minimizes emigration and maximise immigration. According to Joseph Chamie and Barry Mirkin, although the number of births in Russia in 2014 was about 1.7 births per woman, which is higher than in 1990s, yet is still about 20 percent less to ensure population replacement. (Chamie, et al., 2014). Moreover, the abortion rate in Russia is the highest in the world and estimated at two abortions for every birth (Chamie, et al., 2014). Accordingly, high mortality is due to high rates of smoking, alcohol consumption, drug use, HIV/AIDS, tuberculosis, obesity, heart disease, violence, suicide and environmental pollution. (Chamie, et al., 2014). The policies to decrease the health disaster are not effective. The Moscow Times published an article regarding health care condition in Russia, according to the State Statistics Service; from 2005 to 2013 the number of health facilities in rural areas fell by 75 percent, from 8,249 to 2,085. (Epple, et al., 2015). Anatoly Vishnevsky claims that: '... the economic and political situation in Russia does not allow us to expect such a revolutionary change in the health care system in the near future' (Vishnevsky, 2009). The life expectancy for males is about 64 years, which is 15 years less than in Germany, Italy or Sweden. Mark Adomanis backed by Rosstat released information regarding preliminary demographic data for January 2015 argued that: 'Compared to the previous year, deaths were up and births were down by 2 and 4% respectively' (Adomanis, 2015).

After the collapse of SU, Russia has become home for many immigrants, mainly from former Soviet republics. However, the flow of new settlers did not compensate shrinking population of Russia. In addition, anti-immigrants sentiments among Russians are certainly growing, which has a direct impact on migration rate and create additional challenges for officials. Russia is suffering by high tempo of emigration as well. According to the Russian State Statistics Service, Russians who left the country in 2012 was 122,751 people which is nearly four times more than those who left in 2011 (36,774) (Sinelschikova, 2015). Ankit Panda writes that: '...five

times as many Russians are emigrating now, during Vladimir Putin's third term, than in the early 2000s' (Panda, 2014). And as the President Obama states: 'Immigrants aren't rushing to Moscow in search of opportunity' (The Economist, 2014).

The demographers Joseph Chamie and Barry Mirkin argue that: 'Russia's population will most likely decline in the coming decades, perhaps reaching an eventual size in 2100 that's similar to its 1950 level of around 100 million' (Chamie, et al., 2014). Consequently, the country where government is unable to carry out adequate reforms in the health care system and migration policy should not be regarded as a strong country.

Conclusion

There is a well-known quotation by Winston Churchill: 'Russia is never as strong as she looks; Russia is never as weak as she looks'. However, in 2002 Putin declare his version of Churchill's quotation: 'Russia was never so strong as it wants to be and never so weak as it is thought to be' (Katz, 2006). What is interesting here that these quotations were declared in different period of time and the question if Russia is strong or weak relevant today as well.

The possession of massive storage of WMD and current Russian military doctrine, which allows massive use of weapons based on new physical principles, comparable in efficiency with nuclear weapons (Military Doctrine of the RF, n.d.) sets preconditions in geopolitics to take to consideration Russia's position. Moreover Russian permanent membership in the UN Security Council contributes to a decision making process in geopolitical domain. An example might be current debates between the Russia and the West related to military conflicts in Syria and Ukraine. Similar to USSR, Russia has its unique place among international partners due to strong military. However, adequate lessons learned from the history were neglected by Moscow and imperial ambitions of USSR emerged in modern Russia, which is later became the cause of the deterioration in the country. Current leaders of Russia are unable to diversify the economy and like their predecessors mainly rely on gas and oil market. As a result, national currency dramatically fell down due to decreased oil prices. Yet, at the same time expenses on military sector were increased irrespective of worsening economic situation. Country cannot be considered as a

strong state where the health care system is in low level, demography is downgrading and life expectancy for males is about 64. Country cannot be considered as a strong state, which has high level of emigration, where people leave their motherland for better and worthy life and become citizens of new state, where rights of a man is of priority for government and the rule of law applies to everyone regardless of his/her position and wealth.

Bibliography

Adomanis, M., 2015. Russia's demography just took a significant turn for the worse. *Forbes*. [online] Available at: <http://www.forbes.com/sites/markadomanis/2015/03/12/russias-demography-just-took-a-significant-turn-for-the-worse/#6c977bca672f> [Accessed 14 February 2016].

Agerton, M., 2015. Oil price, exchange rates, and the convoluted impact of sanctions on Russia. *Forbes*. [online] Available at: <http://www.forbes.com/sites/thebakersinstitute/2015/04/27/oil-price-exchange-rates-and-the-convoluted-impact-of-sanctions-on-russia/#64732c12d2d9> [Accessed 14 February 2016].

Ankit, P., 2014. Russian emigration spikes in 2013-2014. *The Diplomat*. [online] Available at: <http://thediplomat.com/2014/07/russian-emigration-spikes-in-2013-2014/> [Accessed 14 February 2016].

ARA news, 2015. *Backed by Russian airstrikes, Syrian army regains key areas south Aleppo*. [online] Available at: <http://aranews.net/2015/11/backed-by-russian-airstrikes-syrian-army-regains-key-areas-south-aleppo/> [Accessed 14 February 2016].

Aron, L., 2011. Everything you think you know about the collapse of the soviet union is wrong. *Foreign Policy*. [online] Available at: <http://foreignpolicy.com/2011/06/20/everything-you-think-you-know-about-the-collapse-of-the-soviet-union-is-wrong/> [Accessed 14 February 2016].

Aslund, A., 2008. Peterson Institute for International Economics. *An assessment of Putin's economic policy*. [online] Available at:

<http://www.piie.com/publications/papers/paper.cfm?ResearchID=974> [Accessed 14 February 2016].

BBC, 2015a. *China becomes the world's third largest arms exporter*. [online] Available at: <http://www.bbc.com/news/technology-31901493> [Accessed 14 February 2016].

BBC, 2015b. *Russia profile - Media*. [online] Available at: <http://www.bbc.com/news/world-europe-17840134> [Accessed 14 February 2016].

Bitzinger, R., A., 2015. Russian Arms Transfers and Asian Military Modernization. [online] Available at: <http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=195382> [Accessed 14 February 2016].

Bowen, A., 2013. Military Modernizatsiia and Power Projection. *The interpreter*. [online] Available at: <http://www.interpretermag.com/military-modernizatsiia-and-power-projection/> [Accessed 14 February 2016].

Chamie, J. and Mirkin, B., 2014. Russian demographics: The perfect storm. *YaleGlobal*. [online] Available at: <http://yaleglobal.yale.edu/content/russian-demographics-perfect-storm> [Accessed 14 February 2016].

The Constitution of the Russian Federation, 1993. [online] Available at: <http://www.constitution.ru/en/10003000-01.htm> [Accessed 14 February 2016].

Cullinane, S., 2015. Putin's popularity at record high, government-funded poll says. *CNN*. [online] Available at: <http://edition.cnn.com/2015/10/22/europe/russia-putin-poll/> [Accessed 14 February 2016].

Curtis, G.E., 1996. U.S. Library of Congress. *Russia: A Country Study*. [online] Available at: <http://countrystudies.us/russia/59.htm> [Accessed 14 February 2016].

Donaldson, R., 2000. Boris Yeltsin's foreign policy legacy. [online] Available at: <http://www.personal.utulsa.edu/~robert-donaldson/yeltsin.htm> [Accessed 14 February 2016].

The Economist, 2014. *An interview with the president*. [online] Available at: <http://www.economist.com/blogs/democracyinamerica/2014/08/barack-obama-talks-economist> [Accessed 14 February 2016].

Epple, N., Grozovsky, B. and Aptekar, B., 2015. Russian health care is dying a slow death. *The Moscow Times*. [online] Available at: <http://www.themoscowtimes.com/opinion/article/russian-health-care-is-dying-a-slow-death/519253.html> [Accessed 14 February 2016].

Federation of American Scientists, n.d. *Status of World Nuclear Forces*. [online] Available at: <http://fas.org/issues/nuclear-weapons/status-world-nuclear-forces/> [Accessed 14 February 2016].

Global Fire Power, 2015. *Defence budget by country*. [online] Available at: <http://www.globalfirepower.com/defense-spending-budget.asp> [Accessed 14 February 2016].

Hanlon, Q., 2011. *Adapting America's Security Paradigm and Security Agenda*. [online] Available at: <http://www.strategycenter.org/wp-content/uploads/2011/07/State-Actors-21st-Century.pdf> [Accessed 14 February 2016].

IP, G., 2015. For Russia, Oil Collapse Has Soviet Echoes. *The Wall Street Journal*. [online] Available at: <http://www.wsj.com/articles/for-russia-oil-collapse-has-soviet-echoes-1441215966> [Accessed 14 February 2016].

Katz, M.N., 2006. Policy watch: Is Russia strong or weak? *UPI*. [online] Available at: http://www.upi.com/Business_News/Security-Industry/2006/07/10/Policy-Watch-Is-Russia-strong-or-weak/39541152565695/ [Accessed 14 February 2016].

Kendall, B., 2014. Russian propaganda machine 'worse than Soviet Union'. *BBC*. [online] Available at: <http://www.bbc.com/news/magazine-27713847> [Accessed 14 February 2016].

Laqueur, W., 2010. Moscow's Modernization Dilemma: Is Russia Charting a New Foreign Policy? *Foreign Affairs*, Vol. 89 (6), November/December, p.153-160.

Lee Myers, S. and Schmitt, E., 2015. Russian military uses Syria as proving ground, and West takes notice. *The New York Times*. [online] Available at: http://www.nytimes.com/2015/10/15/world/middleeast/russian-military-uses-syria-as-proving-ground-and-west-takes-notice.html?_r=1 [Accessed 14 February 2016].

Lokshina, T., 2015. Dispatches: Russia, Crimea, and the Shrinking Space for Free Speech. *Human Rights Watch*. [online] Available at: <https://www.hrw.org/news/2015/09/18/dispatches-russia-crimea-and-shrinking-space-free-speech> [Accessed 14 February 2016].

Military doctrine of the RF, n.d. [online] Available at: <https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf> [Accessed 14 February 2016].

Mirovalev, M., 2014. Chechnya, Russia and 20 years of conflict. *ALJAZZERA*. [online] Available at: <http://www.aljazeera.com/indepth/features/2014/12/chechnya-russia-20-years-conflict-2014121161310580523.html> [Accessed 14 February 2016].

The Moscow Times, 2014a. *Russian Defense Budget to Hit Record \$81 Billion in 2015*. [online] Available at: <http://www.themoscowtimes.com/business/article/russian-defense-budget-to-hit-record-81bln-in-2015/509536.html> [Accessed 14 February 2016].

The Moscow Times, 2014b. *'No Putin, No Russia,' Says Kremlin Deputy Chief of Staff*. [online] Available at: <http://www.themoscowtimes.com/news/article/no-putin-no-russia-says-kremlin-deputy-chief-of-staff/509981.html> [Accessed 14 February 2016].

Mullen, J., 2015. Rights group: Russian airstrikes in Syria may have killed dozens of civilians. *CNN*. [online] Available at: <http://edition.cnn.com/2015/10/25/middleeast/syria-russia-airstrikes-hrw/> [Accessed 14 February 2016].

Obama, B., 2009. Remarks by the President at Cairo University. *The White House*. [online] Available at: <https://www.whitehouse.gov/the-press-office/remarks-president-cairo-university-6-04-09> [Accessed 14 February 2016].

Piet, R., 2014. Russia: RIP freedom of speech? *ALJAZZERA*. [online] Available at: <http://www.aljazeera.com/indepth/opinion/2014/07/russia-rip-freedom-speech-2014731823530549.html> [Accessed 14 February 2016].

Putin, V.V., 2002. Послание Федеральному Собранию Российской Федерации в 2002 году [Annual address to the Federal Assembly of the Russian Federation in 2002]. [online] Available at: <http://www.archipelag.ru/agenda/povestka/message/message-2002/> [Accessed 14 February 2016].

Putin, V.V., 2006. Annual address to the Federal Assembly. [online] Available at: http://archive.kremlin.ru/eng/speeches/2006/05/10/1823_type70029type82912_105566.shtml [Accessed 14 February 2016].

Quinn, B., 2015. Boris Nemtsov murder: Putin 'politically responsible' – daughter. *The Guardian*. [online] Available at: <http://www.theguardian.com/world/2015/mar/12/putin-politically-responsible-for-boris-nemtsov-daughter> [Accessed 14 February 2016].

Sinelschikova, Y., 2015. The politics of emigration: Why are Russians packing their bags again? *Russia beyond the headlines*. [online] Available at: http://rbth.com/politics/2015/06/24/the_politics_of_emigration_why_are_russians_packing_their_bags_again_47215.html [Accessed 14 February 2016].

Spinella, P., 2015. Russians' average monthly salary falls to \$500 as food prices skyrocket. *The Moscow Times*. [online] Available at: <http://www.themoscowtimes.com/news/article/russians-average-monthly-salary-falls-to-500-as-food-prices-skyrocket/516947.html> [Accessed 14 February 2016].

Taube, A., 2015. Putin is weak. VOX. [online] Available at: <http://www.vox.com/2015/7/8/8845635/putin-is-weak#crisis> [Accessed 14 February 2016].

Vishnevsky, A., 2009. The challenges of Russia's demographic crisis. [online] Available at: <https://www.ifri.org/sites/default/files/atoms/files/ifridemographyvishnevskiengjune2009.pdf> [Accessed 14 February 2016].

Walker, S., 2015. Boris Nemtsov murder: Chechen chief Kadyrov confirms link to prime suspect. *The Guardian*. [online] Available at: <http://www.theguardian.com/world/2015/mar/08/boris-nemtsov-five-suspects-appear-in-court-over-opposition-leaders-killing> [Accessed 14 February 2016].

Wile, R., 2014. Here's how dependent Russia's economy is on oil and gas. *Business Insider*. [online] Available at: <http://www.businessinsider.com/russia-oil-and-gas-dependence-chart-2014-7> [Accessed 14 February 2016].

World Bank, n.d. *World Development Indicators*. [online] Available at: http://databank.worldbank.org/data/reports.aspx?Code=NY.GDP.PCAP.CD&id=af3ce82b&report_name=Popular_indicators&populartype=series&ispopular=y [Accessed 14 February 2016].

Given the nature and understanding of what is being called Hybrid Warfare today, how can NATO, as a collective alliance, effectively counter hybrid threats? What would an Alliance Counter-Hybrid Warfare Operating Concept look like? What would be some of the challenges associated with such a concept?

MAJ Darius Meilunas

Alliance Counter-Hybrid Warfare Operating Concept should be based on the Comprehensive Approach. All-dimensional educational aspect has to be central to that concept.

Introduction

Since the end of the Cold War, a significant effort has been invested in understanding irregular warfare (Perry, 2015). For the last few decades the phenomenon of western military activity and thinking was counter-insurgency operations (COIN). Following Russo-Georgian war (2008) and especially Russia's occupation of Crimea (2014) and the ongoing contemporary war in eastern Ukraine, the focus apparently was shifted to the concept of hybrid warfare. The term 'hybrid war' seems to be on the lips of the world media to describe the new Russian threat to western, specifically European, security (Charap, 2015). Due to the close proximity of the recent 'battlefield' to borders of European Union and NATO countries, discussions on how to prevent, or counter, Russian backed hybrid threats are on the top of the political and military agendas. *This essay argues that an Alliance Counter-Hybrid Warfare Operating Concept should be based on the principles of the Comprehensive Approach Concepts used by NATO and Coalition COIN operations in Afghanistan and Iraq.* As ongoing discussions in public and among the politicians and the militaries show the misunderstanding of the nature (causes-usage-consequences) of 'hybrid war', an educational aspect of NATO member states' societies is crucial to reinforce recognition of the hybrid threats' variety and ability to resist on all levels. *First*, this essay will provide a brief overview of hybrid warfare theory to demonstrate the complexity and dynamic nature of hybrid threats. *Next*, three case studies of hybrid warfare will be examined to visualize how the hybrid warfare concept is exercised in practice by state-centric actors. *Lastly*, this essay will

conclude with a recommended Alliance (NATO) Counter-Hybrid Warfare Operating Concept.

Hybrid Threats / Hybrid Warfare overview

Before developing a Counter-Hybrid Warfare Operating Concept (C-HW concept) it is necessary to understand the nature of Hybrid Threats and the character and main principles of Hybrid Warfare. The Hybrid Threat is not a new phenomenon in warfare. The grouping of threats into conventional and unconventional has been predominant for a very long time. The Vietnam and Soviet-Afghan wars contain examples of clashes between irregular forces and regular military forces by using conventional tactics and weapons supplemented with terrorism and guerrilla tactics. Analysis of the conflicts which have erupted during the last few decades shows that Hybrid Threats do not fit into this traditional understanding. Hybrid Threats in current conflicts represent simultaneous combination of various enemies and adversaries and their activities that are flexible to change and adapt over time and across various domains (Department of the US Army (DA), 2010). Those threats are designed to target specific state's vulnerabilities, and are therefore varied in different operational environments (Hoffman, 2007). As a definition within the western military community a Hybrid Threat can be described as '...the diverse and dynamic combination of regular forces, irregular forces, and/or criminal elements all unified to achieve mutually benefitting effects.' (DA, 2010). Moreover, not only purely military or kinetic activities fall under modern Hybrid Threat understanding. Non-military entities can be involved and non-kinetic actions can take place in the information, social, political, infrastructure, economic, legal and military (PMESII-L) domains. It makes Hybrid Threats unique, usually unpredictable and a complex challenge to western military communities and societies, and creates multiple dilemmas that require adaptive reactions along multiple lines of effort.

Hybrid warfare concept, which includes creative, synchronized and synergetic employment of Hybrid Threats, was for a long time mainly applied to developing states and stateless groups (Neneth, 2015). Recently, additional forms of Hybrid Warfare have been identified: state-centric and quasi-state hybrid warfare, as the Islamic State, representing the later (Neneth, 2015). Some nation-states, which identify themselves as regional powers, aspire to dominate over their neighbouring

countries. Usually they have conventional force capabilities to do so, however, due to geopolitical trends, international legal obligations, conflict escalation likelihood and international community's influence they are not willing to use those capabilities openly (DA, 2010). Those states prefer to operate in the so called 'Gray Zone' (space between peace and war, where small-footprint, low-visibility, covert and clandestine in nature operations are practiced, (Votel, 2016)) and to use other than conventional military means to destabilize regional security and consolidate their influence. Here the term 'state-centric hybrid warfare' is applied to well-developed states, such as Russia, China or any other modern core state, which use Hybrid Warfare concepts as a Modus Operandi to achieve their politico-military goals. I will put the main focus of this paper on the analysis and development of a C-HW Concept against State-centric Hybrid Warfare due to a matter of great urgency to the Baltic States.

State-centric hybrid warfare can be defined as 'a flexible military strategy that simultaneously uses varied tactics including, but not limited to, conventional tactics employing modern weapons, irregular tactics, covert operations, subterfuge and deception.' (Neneth, 2015). Under this concept states combine conventional military forces which possess sophisticated weapon systems, high-tech based command and control (C2) tools and use combined arms tactics with attributes usually associated with insurgent and criminal organizations. Any variety of non-state actors can be used as well by a state to conduct a range of activities that threaten the target state's government, its citizens and interests. Those activities include terrorism, illegal drug trading, illicit arms and strategic material trafficking, international organized crime, piracy, deliberate environmental damage, extremism, ethnic disputes and religious rivalries (DA, 2010). The combination of the state-based tools and resources with the potency of supporting and enabling non-state actors makes state-centric hybrid warfare extremely effective to present enough complexity to stretch the target nations resources, degrade intellectual capacity and restrict freedom of action of the target state directly and indirectly (DA, 2010). The states exercising hybrid warfare use technologies, media and global networks to conduct sophisticated information campaigns and to broadcast their influence over different audiences including the populations of own and target states as well as the international community. Massive disinformation campaigns designed to control the narratives are widely used in a

hybrid warfare concept (EEAS, 2015). The ability to bring influence on populations and keep it passive, unconcerned or even supportive creates positive preconditions to achieve goals of the aggressor states with limited opposition. It leads us to the necessity to educate at-risk populations to identify hybrid threats and their associated narratives in order to prepare for individual and collective societal resistance. The aggressor states take every opportunity to obtain a position within a target state's political, military, economic and social infrastructures well in advance and use it to their advantage as opportunities present themselves. Insurgency, in concert with criminal activities, is used to create instability and to alienate legitimate security forces from the population. By successfully implementing all of the above-mentioned non-military and non-kinetic activities, an adversary state may prevent the timely and adequate response of the target state's government. Physical attacks on the target state by using conventional military forces, including the use of or threat to use Weapons of Mass Destruction, in combination with unconventional and non-military activities usually is the last option in a state-centric hybrid warfare campaign. In summary, Hybrid Threats within state-centric hybrid warfare concepts '...simultaneously create economic instability, foster lack of trust in existing governance, attack information networks,..., cause man-made humanitarian crises, and physically endanger opponents' (DA, 2010). The containment of complex Hybrid Threats requires a comprehensive effort of the target state's actors along all PMESII-L domains. Further analysis of current Russian activities in the former Soviet Union area will highlight region and actor specific aspects of the state-centric hybrid warfare.

Under the presidency of Vladimir Putin, Russia invested a huge effort to resume the status of a regional power (or even claims to a global power) which was lost with the breakdown of the Soviet Union in the early 1990s. The Kremlin is making a geopolitical comeback in the former Soviet space to achieve this goal by rebuilding conventional military capabilities and projecting power in the near abroad, regaining geopolitical influence regionally, achieving economic, cultural and informational dominance, and preventing enlargement of NATO and the EU toward Russian borders (Karagiannis, 2014). It sees those organizations with US on the spearhead as a threat not only to Russia's regional or global dominance, but also as a real threat to its internal order and ruling regime through imported 'colour revolutions' (Bartles,

2016). Russia blames NATO and EU for attracting the former members of the Soviet Union from Russia's sphere of influence, thereby ignoring its natural right to regional influence. Since the fall of the Soviet Union, Russia's goal was to make the former Soviet Republics friendly and subordinate partners (Berzins, 2014). Many of those countries are already under the Kremlin's sway with significant Russian military presence and political, economic, information influence, while others are targeted for future exploitation and development (including Baltic States). A variety of tools, which fall under western descriptions of Hybrid warfare, are used to keep the former Soviet Republics under Russia's influence. The term 'Hybrid Warfare' is not used in Russian military literature. Instead of 'Hybrid Warfare', the term 'Non-Linear War' is used among the militaries and military academics. However, the meaning of those terms is the same – '... intentionally blurring the line between war and peace and creating a permanent fog of war.' (Sikory, 2015). The analysis of the latest 'colour revolutions' made a significant influence on the Russian view of the '...warfare in the twenty-first century.' (Gerasimov, 2016). A thought of the Chief of the Russian General Staff Gen. V. Gerasimov – 'The role of non-military means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness.' (Gerasimov, 2016) – became the backbone of the recent non-linear war or state-centric hybrid warfare concept.

Generally, the concept of Russian Hybrid Warfare is based on the use of political, economic, informational, humanitarian and other non-military measures supplemented by military means of a concealed character in coordination with the protest potential of the population (Gerasimov, 2016). There are plenty of tools within the 'toolbox' of this generalized concept, however, the success of the Russian Hybrid Warfare / Non-linear War concept hinges on an effectiveness of information operations to influence friendly, adversary and neutral audiences, with its subsequent exploitation by special operations forces (Perry, 2015). With the ingenious and coordinated Information Warfare campaign Russia can establish its online worldwide presence to spread its messages and misinformation through 'Russia Today' and by using internet trolls to infiltrate social media, launch cyber-attacks against government websites and disable communications systems of the target country (Siroky, 2015). As an economic influence tool, Russia uses energy dependency of many countries to achieve its political goals. The penetration of Russian energy

companies into the economy of the target state and the acquirement of its strategic assets (Karagiannis, 2014) supplemented by the destruction of critically important facilities of civilian infrastructure, if and when necessary, represents the key approach to reduce the economic potential of the opponent (Gerasimov, 2016). In the political domain, Russia uses the sponsorship of the left and right wing political parties and organisations to deepen political cleavages inside the target state (Siroky, 2015) and create an impression of the internal political clashes in the eyes of the international community. Within the framework of the Non-linear war Russia seeks to exploit the Fifth Column (representatives of any ethnical, religious or political entity who are discontent with the local government and sympathizer of Russia) to simulate a humanitarian crisis, violations of human rights, request to protect and provoke violent local government response thus justifying Russian response to bring 'stability and security'.

All above-mentioned Russian Non-linear war tools and activities could be used simultaneously through all PMESII-L domains in different combination and scope. However, Janis Berzins, a Latvian military scholar and scientist, has suggested phasing of the use of the hybrid tools and activities based on the analyses of the ongoing conflict in Ukraine. Recommended phases range from the use of non-military asymmetric instruments to the use of conventional kinetic tools and activities (Berzins, 2014).

Case study (Georgia): passportization as a tool of political warfare within a Hybrid warfare concept

Due to its strategically important position in the South Caucasus as a land bridge and a chokepoint for gas and oil flow between Russia and the Middle East, Georgia became highly important to Russian foreign policy (Karagiannis, 2014). Since the collapse of the Soviet Union, Russia took advantage of political instability in Georgia and started support to separatist movements in Abkhazia and South Ossetia by political, economic and military means (supply of light and heavy armaments) (Artman, 2011). However, on the eve of the 'Rose Revolution' (2003) and after the Adjara crisis (2004) Russia recognized a threat to lose its influence in the breakaway regions of Georgia. It forced the Kremlin to innovate and find new ways of preserving its influence in Georgia. The passportization programme was accelerated to increase

control over South Ossetia and Abkhazia by extending Russian citizenship to the local population (Dunlop, 2010).

The distribution of passports to Abkhazians, South Ossetians and Armenians allows Russia to naturalize the majority of the citizens of two secessionist regions and to transform the separatist territories into "Russian spaces" within the internationally recognized borders of the Republic of Georgia (Artman, 2011, Salhani, 2014). By passportization the Russian government '..."captured" a sizeable portion of the population and territory ... and laid the discursive foundations for war.' (Artman, 2011). In 2006 almost 90 per cents of the citizens of South Ossetia possessed citizenship of the Russian Federation (Dunlop, 2010). When the Georgian government attempted to reintegrate South Ossetia back to 'Georgian space', Russia was able to invoke the right to protect its citizens abroad as a justification for intervention. Russian intervention into Georgia in August of 2008 was justified by the inherent right to self-defence under Article 51 of the Charter of the United Nations and the clause in the Russian constitution guaranteeing defence and patronage to compatriots abroad.

As this Georgian case proves, passportization politics is one of Russian soft power tools that helps to create pressure on its opponents and maintain certain level of hegemony in the near abroad (Artman, 2011, Salhani, 2014).

Case study (Ukraine): use of military forces within Hybrid warfare concept

Within a framework of non-linear war along diplomatic, economic, political, social, information, legal means Russian also employed in Ukraine (both in Crimea and Eastern Ukraine) military means in terms of regular forces and Special Operations Forces (SOF). Due to a concealed character, clandestine nature, small footprint, great operating flexibility, ability to outmanoeuvre the adversary and operate in politically sensitive conditions SOF operations are the most effective and critical in the Russian non-linear warfare concept employed in Ukraine (Perry, 2015). Even though the Russian regular forces are based mainly on the weaponry of Soviet-era design and production, are not so well-trained and equipped (De Larrinaga, 2016) as SOF units and have to operate under strict political constraints, however, they also have played the important role during the conflict in Ukraine.

On the eve of the operation to seize Crimea, Russian military forces have been used in a show of force role when the large scale military exercise was launched including areas along the land border with Ukraine. In combination with the discussions on the use of nuclear forces and strategic bomber flights close to NATO airspace (McDermott, 2015), the exercise aimed to flex Russian muscles, distract attention from Crimea and prevent West community from intervening in Ukraine (Norberg, 2014). Early penetration of the Ukrainian state intelligence service by Russian intelligence services provided clear insight into Ukrainian response options and ability to prepare the battlefield by organizing local protests, conducting reconnaissance and subversions (McDermott, 2015).

The seizure of Crimea started by deployment of SOF units mainly through the Russian Black Sea Fleet base in the peninsula (McDermott, 2015). SOF operators took key military and civil infrastructure (governmental buildings, airports, surface-to-air missile batteries, military bases, C2 / communications nodes and fuel depots) and were able to dominate over the lines of communications (Norberg, 2014, Perry, 2015). Since they appeared as masked gunmen who wore no unit or national insignia it provided Kremlin 'plausible deniability' and delayed the rapid and consistent response from Ukrainian government and military as well as International community (Perry, 2015). Once initial SOF success was achieved, the regular forces (airborne and marine infantry) were employed to increase the military presence and free SOF units for other tasks such as an organization of pro-Russian separatists. Russian Navy was used to block exit to Black Sea (McDermott, 2015).

In the Eastern Ukraine Russian SOF has focused on training and aiding pro-Russian separatist forces, filling out their ranks with advisers, fighters and leadership (Perry, 2015, US Army SOC, 2015). SOF squad-platoon size elements have conducted independent special operations as well as provided security for arms supplies and Russian trainers educating separatists on technical weapon systems (Galeotti, 2014). The Regular forces have been involved on a larger scale comparing to Crimea campaign. The Company or Battalion Tactical Groups were at the vanguard of every battle that was occurring between separatist and Ukrainian forces (Wiser, 2015). Russian regular forces were building forward operating bases in proximity to Ukrainian border thus threatening the government of Ukraine by possible large scale intervention at any time (McDermott, 2015).

Case study (Lithuania): use of soft power within Hybrid warfare concept

The President of Lithuania, Dalia Grybauskaitė, has stated that Lithuania is already under Russian attack (Sikory, 2015). A significant effort is made by Russia along information domain lines of effort to influence national political, social and economic processes and challenge Lithuanian security. Russian foreign policy aggressively uses propaganda and strategic communications to undermine Lithuania's government and its relations with NATO and EU partners (Coffey, Kochis, 2015). Russia uses television, the internet and newspapers intensely to wage war in the cognitive domain for the minds and hearts of the citizens of Lithuania without the need for a physical military presence (Ljungman, 2014). Those activities are mainly coordinated by the Russian embassy in Vilnius using official Russian media entities and exploiting the full range of Russian sponsored nongovernmental organizations, academic-, cultural-, historic-, analytical agencies, discussion clubs, internet trollies and single public activists (State Security Service, 2016). To create a sense of distrust among Lithuanian citizens and its allies, and increase the number of Russia's sympathizers, the primary focus is made along several target lines: Lithuanian history, NATO and EU solidarity, Ethnic minorities, Lithuanian governance, and the cultural environment (Pancerovas, 2015). By muddying the Lithuanian fight for the independence story line and promoting 'the greatness' of the common fight against fascism, aggressively thrusting Russian cultural events at the nationally significant dates in Lithuania, involving Russian speaking youths in Russian educational system and events (sponsored studies, ideology-driven youths' camps and airsoft (paramilitary) clubs in Russia and Lithuania), Russia seeks to restore the feeling of soviet nostalgia and promote the narrative that Lithuania still belongs to Russia's traditional sphere of influence and the future of Lithuania is in the East, and not in the West. The narratives of Russia's propaganda on Lithuania's aggressiveness against Russia in terms of support to Ukraine, increased military spending, resumption of the conscription, and the suppression of Russian compatriots and other ethnic minorities, could be exploited to justify possible intervention by force under the guise of 'protecting Russian citizens' or 'pacifying Lithuania' when it will be reasonable.

Recommended Alliance Counter-Hybrid Warfare Operating Concept

The above-mentioned overview of hybrid threats and case studies indicates the complex and unpredictable nature of a potential hybrid conflict between state actors. NATO as an alliance and its single member states have difficulty in reacting to hybrid warfare with traditional military instruments of collective defence alone and new concept have to be developed and implemented to react flexibly to the challenges of hybrid warfare approaches (Jacobs, Lasconjarias, 2015).

My recommended concept is based on the comprehensive approach between military and civilian parties, NATO and other international organizations (such as EU, OSCE, UN specialized agencies, etc.) as well as local nationals to respond adequately to the changes in the security environment which are not necessarily of a military nature (Drent, 2011, Reisinger, Golts, 2014). The set of the necessary measures and organizational introductions are presented in annexes to this paper (see annexes 1 and 2), however, some aspects should be highlighted broadly.

NATO's decision-making requires the consensus among all members. This takes time, especially in an environment where Russia can put pressure on the single member state based on bilateral political or economic agreements. Considering this, a significant effort of preparation and execution to respond against hybrid attack has to be taken at the national level until the decision for a NATO military response will be made. All activities at the national and alliance levels should be organized along three phases: preparation, deterrence and defence as it is presented in annex 1 (Godwin, 2016). Co-ordination, consultation and intelligence sharing vertically (nation-to-NATO, NATO-to-nation) and horizontally (nation-to-nation) is crucial to establish coherent situational awareness and support the analysis of the established indicators and warnings.

Generally, NATO is the most effective military alliance, however, its military forces and capabilities mainly are owned by nations, they are widely dispersed and have different readiness statuses. In case of a Russian hybrid attack against the Baltics, Russia has some military advantages against NATO: initiative of time, specific location and scope of aggression, speed of decision-making, information dominance in the region, rapid force build-up and deployment across the borders (US Army War College, n.d.). It leads to the necessity to review the force structures, units' readiness

and deployment, and training requirements. The ability of the national and alliance military units to fight against conventional and unconventional adversaries simultaneously within the highly contested information and cyber environment should be paramount within the C-HW concept (McCuen, 2008).

Last, but not least, an important aspect inside of any C-HW concept that must be highlighted is education. The success of Hybrid warfare is granted also by the incapacity of the victim state to understand the nature of the hybrid approach to warfare. The understanding that the responsibility to defend against a hybrid adversary is no longer usurped by the militaries alone and has to be indoctrinated into the society. The Hybrid Warfare theme should be integrated into the national civil education institutions to share the common understanding among the representatives of PMESII-L domains. The rest of the society should be educated through the civil-military cooperation when the members of the national armed forces and paramilitary organizations during the regular meetings or social events train and educate the population on how to act in extreme situations, identify and avoid threats. Knowledge how Russia (or any other actor) uses non-military and military instruments within its Hybrid Warfare concept would help the citizens of the target state to avoid being manipulated in favour of the aggressor. Finally, the NATO Counter Hybrid Warfare Centre of Excellence (CoE) should be established to educate and train military and civil leaders, decision makers from NATO member and partner countries (Morris, 2015). This CoE could develop expertise, recommendations, methodology and integrate the deliverables of other NATO's CoEs such as Strategic Communications, Cyber Defence, Energy Security, Counter Improvised Explosive Devices, etc.

Even if Hybrid Warfare seeks to exploit primarily non-military instruments of the national power, militaries should take a lead to coordinate the effort to counter hybrid threats due to better understanding of the nature of hybrid threats, planning skills and both abilities and capabilities to monitor the situation and establish situational awareness.

Conclusions

Russia, for quite a while, has been keen on the establishment of its regional hegemony by expanding its dominance in the near abroad, including the Baltic States, the members of NATO and EU (Voyger, 2016) thus undermining the

credibility of those countries and organizations. Despite the significant modernization effort, the Russian Armed Forces still ‘...are quantitatively and qualitatively inferior in conventional capability...’ (Russell, 2015) to NATO, therefore major conventional clashes with NATO are not likely. However, limited in space and scope strikes against separate NATO member states (such as three Baltic States) cannot be ruled out. Apart from the military, Russia already uses diplomatic, economic, information, financial and lawful instruments of national power against many NATO and EU member states to paralyze their decision-making and keep them off-balance. The ethnic minorities abroad, passports, pipelines, security services, (mis)information, bluff, corruption, ambiguity, interpretation of the international law, plausible deniability became the key elements of Russia’s ‘guerrilla geopolitics’ to promote its national interests and apply pressure on the neighbours and partners for the purpose to establish and maintain its hegemony (Galeotti, 2015, Mastriano, 2015, Salhani, 2014).

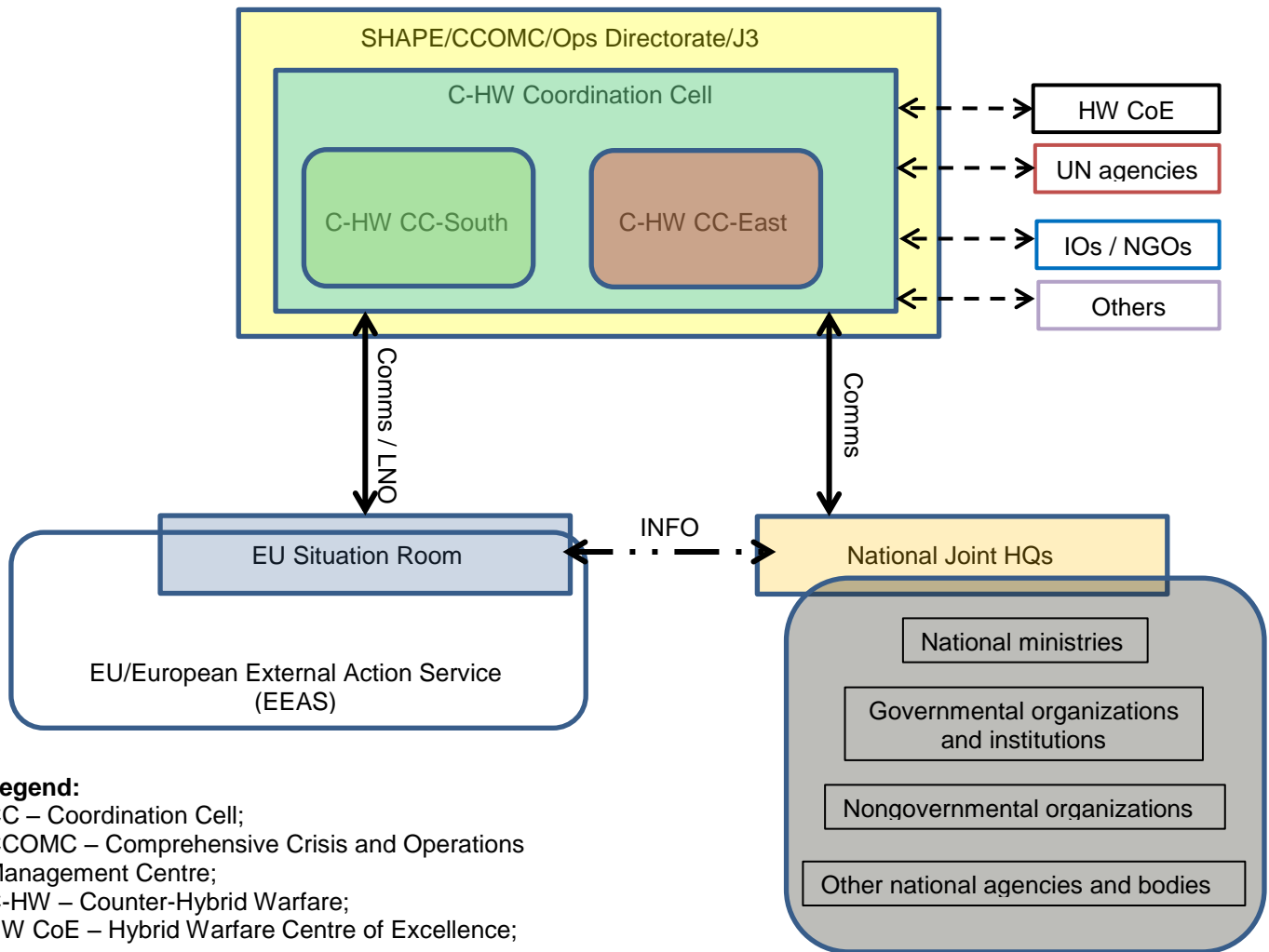
Using the analysis of Hybrid Threats and Russian based State-centric Hybrid Warfare concept, supported by the overview of three Case studies, this essay argues that Alliance Counter-Hybrid Warfare Operating Concept should be based on the Comprehensive Security Approach combining various players and tools available along PMESII-L domains. The effectiveness of this approach will depend on the organizational skills to coordinate public and civic organizations and institutions, officials and ordinary peoples’ involvement at national and multinational levels (Bartkowski, 2015). The education of the members of the international community to recognize and understand the nature of hybrid threats will reduce the effectiveness of Russian propaganda (or any other state actor-aggressor) and a portion of the population with pro-Russian beliefs and will help the development and implementation of the practical response at individual-community-organizational-state levels (Perry, 2015).

The effective comprehensive approach is based on unity of effort of all participants. As lessons identified from other NATO and UN operations shows, it also could be a real challenge in C-HW concept due to the unwillingness of some civil organizations and actors, especially non-governmental, to work together with the military. It will not exclude a possibility of success, however, it will require more time, resources and patience (Aaronson, et al., n.d.).

Annex 1 (Phases and activities within recommended C-HW concept)

Preparation Phase	Deterrence Phase	Defence Phase	
Establishment / activation of C-HW coordination cell within SHAPE/Comprehensive Crisis and Operations Management Centre (CCOMC)			
STRATCOM campaign / INFOOPS (counter-propaganda)			
Intelligence, situational awareness, risk assessment, info sharing with member states			
Establishment / training of NATO high readiness forces	Pre-deployment of NATO troops (VJTF, NRF, SOF)	Article V Ops	
Combined Joint Exercises	Support to target member state with critical capabilities	Force build-up (follow-on forces)	
	Combined Joint Exercises in target state/region		
Education of NATO MIL/CIV personnel at NATO Hybrid Warfare Centre of Excellence	Support to implementation of economic sanctions against aggressor state		
	International cooperation / diplomatic effort to resolve crisis / implementation of Articles II, III and IV		
	Revision of allied legislation to counter known and emerging Hybrid Threats		
Integration of Hybrid Warfare issues into national MIL / CIV education institutions	Alliance Level		
	National Level		
Revision of national legislation to counter Hybrid Threats	Provision of HNS / Combined Exercises (NATO/PfP)		
	International cooperation / diplomatic effort to resolve crisis	Conventional Ops	
Establishment of high readiness forces	Required capabilities building / procurement	Guerrilla Ops in ENY occupied territories	
	Economic development / welfare building / integration of minorities	STRATCOM campaign / INFOOPS (counter-propaganda, PSYOPS, PA)	
Intelligence, situational awareness, risk assessment, info sharing with NATO members	Internal security / border control / CI / COIN	Territorial defence	
	Establishment / activation of C-HW coordination board within JHQ (MIL / CIV representatives)		
Intelligence, situational awareness, risk assessment, info sharing with NATO members			
Establishment / activation of C-HW coordination board within JHQ (MIL / CIV representatives)			
Selection and Training of key personnel for the armed resistance; pre-stocking of weapons/AMMO/MEDKITS		Armed resistance; Insurgency	
Education and training of the society on (Counter)Hybrid Warfare issues		Nonviolent Civilian Defence	

Annex 2 (Organizational introductions within recommended C-HW concept)



For the effective coordination of the allied counter-hybrid effort it is recommended to establish a C-HW Coordination Cell under J3 branch of the Operations Directorate at the Comprehensive Crisis and Operations Management Centre (CCOMC) at SHAPE HQ which is specifically established to ensure the comprehensiveness in NATO's planning and execution of multiple crises and operations simultaneously. A C-HW Coordination Cell should have technical capabilities and expertise to focus on hybrid threats emerging in the East (Russia) and in the South (terrorism). When necessary, this cell would use the competencies and expertise of the HW CoE (as well as other NATO's CoEs), UN agencies, international and nongovernmental organizations. The permanent contact with the national joint headquarters of the member states and with the European Union Situation Room under the European External Action Service

should be warranted by the secure technical communications and through the exchange of liaison personnel when needed.

The EU Situation Room is designed to provide worldwide monitoring and current situation awareness 24/7 and has rapid access to the EU leadership, institutions and bodies which present the broad range of non-military competencies (economic, financial, legal, information, etc.) crucial for the counter-hybrid effort.

The national counter-hybrid effort could be organized through the joint HQs (or their equivalents) involving representatives of the ministries, governmental and nongovernmental organizations, other agencies and bodies.

Bibliography

Aarosan, M., Diessen, S., De Kermabon, Y., Long, M. B. and Miklaucic, M., n.d. NATO Countering the Hybrid Threat. [online] Available at: <https://www.ciaonet.org/attachments/19704/uploads> [Accessed 03 April 2016].

Artman, V.M., 2011. "Passport Politics": Passportization and Territoriality in the De Facto States of Georgia. [online] Available at: https://scholarsbank.uoregon.edu/xmlui/bitstream/handle/1794/11506/Artman_Vincen_t_M_ma2011sp.pdf?sequence=1 [Accessed 03 April 2016].

Bartkowski, M., 2015. Nonviolent Civilian Defence to Counter Russian Hybrid Warfare. [online] Available at: <http://advanced.jhu.edu/academics/graduate-degree-programs/global-security-studies/program-resources/publications/white-paper-maciej-bartkowski/> [Accessed 31 March 2016].

Bartles, C.K., 2016. Getting Gerasimov Right. [online] Available at: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf [Accessed 04 April 2016].

Berzins, J., 2014. Russia's New Generation Warfare in Ukraine: Implications for Latvian Defence Policy. *National Defence Academy of Latvia Center for Security and Strategic Research Policy Paper*, No. 02 (April), p. 1-13.

Charap, S., 2015. The Ghost of Hybrid War. *Survival*. Number 57:6, pp. 51-58.

Coffey, L., Kochis, D., 2015. The Baltic States: The United States Must Be Prepared to Fulfill Its NATO Treaty Obligations. [online] Available at: <http://www.heritage.org/research/reports/2015/09/the-baltic-states-the-united-states-must-be-prepared-to-fulfill-its-nato-treaty-obligations> [Accessed 31 March 2016].

De Larrinaga, N., 2016. Return of the bear. *HIS Jane's Defence Weekly*. 16 March 2016, pp. 22-32.

Department of the US Army, 2010. TC 7-100 Hybrid Threat. [online] Available at: http://www.benning.army.mil/mssp/security%20topics/Potential%20Adversaries/content/pdf/tc7_100.pdf [Accessed 03 April 2016].

Drent, M., 2011. The EU's Comprehensive Approach to Security: A Culture of Coordination? [online] Available at: http://www.clingendael.nl/sites/default/files/20111000_sd_drent_approach.pdf [Accessed 02 April 2016].

European External Action Service, 2015. Food-for-thought paper 'Countering Hybrid Threats'. [online] Available at: <http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf> Accessed 16 March 2016].

Galeotti, M., 2015. 'Hybrid War' and 'Little Green Men': how it works, and how it doesn't. [online] Available at: <http://www.e-ir.info/2015/04/16/hybrid-war-and-little-green-men-how-it-works-and-how-it-doesnt/> [Accessed 31 March 2016].

Gerasimov, V., 2016. The Value of Science is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. [online] Available at: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf [Accessed 04 April 2016].

Giegerich, B., 2015. Workshop Report: Perspectives on Hybrid Warfare. [online] Available at: <http://www.iiss.org/en/iiss%20voices/blogsections/iiss-voices-2015-dda3/july-2632/perspectives-on-hybrid-warfare-cd5e> [Accessed 03 April 2016].

Godwin, Ch., 2016. Hybrid Warfare. Lecture, Baltic Defence College. 17 March 2016.

Hoffman, F.G., 2007. Conflict in the 21st Century: The Rise of Hybrid Wars. [online] Available at: http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf [Accessed 04 April 2016].

Jacobs, A., Lasconjarias G., 2015. NATO's Hybrid Flanks: Handling Unconventional Warfare in the South and the East. In: G. Lasconjarias, J. A. Larsen, ed. 2015. *NATO's Response to Hybrid Threats*. Rome: DeBooks Italia srl. pp. 257-276.

Karagiannis, E., 2014. The Russian Interventions in South Ossetia and Crimea Compared: Military Performance, Legitimacy and Goals. [online] Available at: <http://www.tandfonline.com/doi/abs/10.1080/13523260.2014.963965> / [Accessed 12 October 2015].

Kropaite, Z., 2014. Russia's information war in Lithuania. [online] Available at: <https://euobserver.com/political/125893> [Accessed 01 April 2016].

Ljungman, J., 2014. The Russian information war in Lithuania. [online] Available at: <http://toinformistoinfluence.com/2014/12/10/the-russian-information-war-in-lithuania/> [Accessed 01 April 2016].

Mastriano, D. V., 2015. Five smooth stones: how NATO can deter the 'Goliath' Russian challenge to the Baltics. [online] Available at: <http://smallwarsjournal.com/jrnl/art/five-smooth-stones-how-nato-can-deter-the-%E2%80%9Cgoliath%E2%80%9D-russian-challenge-to-the-baltics> [Accessed 31 March 2016].

McCue, J.J., 2008. Hybrid Wars. [online] Available at: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20080430_art017.pdf [Accessed 04 April 2016].

McDermott, R. N., 2015. Brothers Disunited: Russia's Use of Military Power in Ukraine. [online] Available at: <http://psan.hypotheses.org/1270> [Accessed 24 March 2016].

Morris, V. R., 2015. Leveraging Lietuva: Establishing a 21st Century Nonlinear Warfare Center of Excellence. [online] Available at:

<http://smallwarsjournal.com/jrnl/art/leveraging-lietuva-establishing-a-21st-century-nonlinear-warfare-centre-of-excellence> [Accessed 02 April 2016].

Neneth, W., 2015. Russia's State-centric Hybrid Warfare. [online] Available at: <http://www.diplomaatia.ee/en/article/russias-state-centric-hybrid-warfare/> [Accessed 09 December 2015].

Norberg, J., 2014. The use of Russia's military in the Crimean crisis. [online] Available at: <http://carnegieendowment.org/2014/03/13/use-of-russia-s-military-in-crimean-crisis> [Accessed 24 March 2016].

Pancerovas, D., 2015. Five targets of the Kremlin's propaganda in Lithuania. [online] Available at: <http://www.15min.lt/naujiena/aktualu/karo-zona/5-lietuviski-taikiniai-i-kuriuos-kitamet-taikysis-kremliaus-propaganda-784-474767> [Accessed 01 April 2016].

Perry, B., 2015. Non-Linear Warfare in Ukraine: The Critical Role of Information Operations and Special Operations. [online] Available at: <http://smallwarsjournal.com/jrnl/art/non-linear-warfare-in-ukraine-the-critical-role-of-information-operations-and-special-opera> [Accessed 03 April 2016].

Reisinger, H. and Golts, A., 2014. Russia's Hybrid Warfare: Waging War below the Radar of Traditional Collective Defence. *NATO Defence College*. Research Paper 105. [online] Available at: <http://www.ndc.nato.int/news/news.php?icode=732> [Accessed 03 April 2016].

Russell, M., 2015. *Russia's armed forces: reforms and challenges*. [online] Available at: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554213/EPRS_IDA\(2015\)554213_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/554213/EPRS_IDA(2015)554213_EN.pdf) [Accessed 03 April 2016].

Salhani, C., 2014. Russia's New Weapons: Passports and Pipelines. [online] Available at: <http://oilprice.com/Energy/Energy-General/Russias-New-Weapons-Passports-and-Pipelines.html> [Accessed 19 March 2016].

Sikory, D., 2015. The Fog of Non-linear War: Russia's Strategic Coercion in the Near Abroad. [online] Available at: http://georgianreview.ge/wp-content/uploads/2015/10/DAVID-sikory-pdf_.pdf [Accessed 03 April 2016].

State Security Service of Lithuania, 2016. Threats' assessment to the national security. [online] Available at: <http://www.ekspertai.eu/static/uploads/2014/01/vsd%20gresmes%202015.pdf> [Accessed 02 April 2016].

United States Army Special Operations Command, 2015. SOF Support to Political Warfare. White Paper. [online] Available at: <https://dl.dropboxusercontent.com/u/6891151/Support%20to%20Political%20Warfare%20White%20Paper%20v2.3-RMT%20%2810MAR2015%29%20%20%20.pdf> [Accessed 03 April 2016].

US Army War College, n.d. Project 1704: A U.S. Army War College Analysis of Russian Strategy in Eastern Europe, an Appropriate U.S. Response, and the Implications on U.S. Landpower. [online] Available at: <http://www.strategicstudiesinstitute.army.mil/pdf/files/PUB1274.pdf> [Accessed 02 April 2016].

Votel, J.L., Cleveland, T.C., Connett, T.C., Irwin, W., 2016. Unconventional Warfare in the Gray Zone. *Joint Force Quarterly*. Issue 80, pp. 101-109.

Voyger, M., 2016. Hybrid Warfare and Russian Expansionism in the 'Near Abroad'. Lecture, Baltic Defence College. 17 March 2016.

Wiser, D., 2015. How Russia invaded Ukraine. *The Washington Free Beacon*. [online] Available at: <http://freebeacon.com/national-security/how-russia-invaded-ukraine/> [Accessed 24 March 2016].

Is Russia's hybrid war contagious? Has the world just witnessed the outbreak of a new age of 'peaceful war'?

MAJ Kaspars Miežitis

Sun Tzu stated that 'if enemy is united, cause them to be separated... attack where enemy is unprepared... go forth where enemy will not expect it' (TZU, 2003, p.16). This understanding has unchanged even through time. Moreover those principles are successfully implemented in current warfare and growing effectiveness of available tools has been turned to reach more destructive effects as previously. Today's technological progress has created fertile soil for completely new forms of *multi-modal* activities which can be used as weaponry. One of the ways to describe the complexity and diversity of implemented activities/factors is used the term as hybrid warfare. The term "hybrid" got increased tension when Russia implemented multi-modal activities and methods in Ukraine to annex Crimea, causing shock not just in Ukraine but in the Western world as well. In Ukraine the Russia was able test its strategy and hybrid warfare principles and even more - Western readiness to deal with new format of war. Taking on considerations challenges what could bring hybrid warfare's employment, this paper will focus to the thesis statement: "Russian new generation warfare principles will change world's order durability and currently known war principles in the future". Additionally to strengthen a thesis statement will be used two arguments:

- Properly waged hybrid warfare is the most suitable tool in current weaponry to test country's durability without launching full scale war.
- Concept has proven historical roots and it is successfully tested in Ukraine.

To recognize the essence of hybrid warfare, it is important to understand the meaning of the term "hybrid war" and usage of this term "hybrid warfare".

What is hybrid war? Is it "peaceful war"?

Currently there is different understandings and definitions of hybrid war, even among NATO countries. 'Despite of diversity NATO has adopted the expression "hybrid war" and it is mostly used to characterize warfare which was implemented by Russia in

Crimea. The Wales Summit declaration described “hybrid warfare as a wide range of overt and covert, military, paramilitary and civilian measures... employed in a highly integrated design,” (Podbay, 2012) stating complexity and diversity of hybrid warfare. Additionally there are the European Union earmarked statement that ‘hybrid war is a situation in which a country resorts to the overt use of armed forces against another country or a non-state actor, mixing other means (i.e. economic, political, and diplomatic)’(Pawlak, 2015).

Furthermore the complexity of hybrid war was understood even much earlier before Crimea conflict, for example, in (Murray and Mansoor, 2012, p.321) defined hybrid warfare as:

‘...a conflict involving a combination of conventional military forces and irregulars (guerrillas, insurgents and terrorists), which could include both state and non-state actors, aimed at achieving a common political purpose.’

Moreover understanding of hybrid warfare differs between countries, the Russians are exploring nature of conflict naming it as Russia’s new generation warfare.

‘In 2013. General Valery Gerasimov, the Chief of the Russian General Staff listed main principles of new generation warfare. The core principle is that the world is now in a situation of conflict. He states that “in the 21st century, we have seen a tendency toward blurring the lines between the status of war and peace. He says that the approach of wars has changed as they are no longer declared and, having begun, they move in different and unfamiliar directions. Gerasimov states that the specific abilities will be needed: use of Special Forces linking up with internal opposition groups throughout the target country to create an operating front throughout the entire depth of the enemy’s territory. These actions will be combined with information operations, cyber warfare, legal warfare, economic war and other activities’ (Balasevicius, 2015).

Description of hybrid warfare above is only a short introduction in broad hybrid warfare spectrum, making clear that complexity and diversity become unlimited. Growing world’s technological potential clears limits of coherent action and communication between different instruments of power, widening warfare borders in areas what previously was not considered as part of regular warfare. However, multi modal activities in hybrid warfare and its wide spectre of tools exclude the possibility to clearly state its definition and leads to situations when everything starts to become

hybrid 'as long as it is not limited to a single form and dimension of warfare' (NATO Review magazine, 2015).

Evaluating concept "hybrid war" it is clear that by itself it is not new. Even Russians during the soviet time has implemented some hybrid warfare principles in 1924. 'Back then, assault groups organized by the Soviet intelligence officers, together with underground Estonian communists, attempted to seize power and to subsequently invite regular troops of the Red Army to enter Estonia "for help"' (Maigre, 2015).

Similar principles, but more advanced was implemented by the Soviet Union during Baltic States occupation in 1940. Throughout that time Soviets successfully employed some combination of political, military, economic, social and even information means strengthened with criminal and irregular warfare methods.

For example Historians have divided Latvian occupation process in 1940. into five stages. The first stage was information collection and gathering by soviets. Second implementation of different soviet entertainment and cultural activities like printed books, vinyl records, magazines and organization of different exhibitions to attract population. The third stage was distribution of Bolshevik's ideology mixing with misinformation about soviet and Latvian political systems. Fourth stage was the creation of fake economical support. Fifth was occupation of Latvia and Latvian Armed force destruction (Research of the Commission of the Historians of Latvia, 2003). The result was shocking; Latvia was occupied without significant armoured resistance from Latvian side.

Described above are historical examples showing that the hybrid war concept is not new for Russia even from a historical perspective, rising assumption that it was developed and historically sharpened much earlier as Crimea conflict. However historically devastating wars were not appreciated from any side of involved party and it could develop the impulse for Russia to discover safer manners to wage a war, leading to Hybrid warfare fundamentals. General Gerasimov once stated that 'the effectiveness of "non-military" tools in achieving strategic or political goals in a conflict has exceeded that of weapons' (Kofman and Rojansky, 2015), clearly showing that the new hybrid war concept can become more effective and devastating comparing with conventional military operations. Taking in the sense that the biggest portion of hybrid efforts are conducted by non-military tools, like diplomacy, economy,

information, policy in different domains, it becomes clear that, main struggle is conducted without brutal force involvement and direct threat to military personnel - saving military assets and human lives.

Summarizing all above mentioned, it makes clear that the term hybrid war concept is not a new form of warfare and it can include the multi modal wide range legal and illegal activities to shape one's countries situation in favourable condition where could be implemented other military means. To gain such kind of favourable precondition all implemented activities should intentionally or covertly support expected favourable situation to execute the hybrid war. To understand it deeper let's take a look to concepts how new-generation or hybrid warfare could be executed.

Hybrid warfare's shaping phase: a 'sand pile model' perspective.

Currently there are different concepts created how hybrid warfare could be executed or implemented, orienting all activities to reach not just physically measurable conditions, but even mental and psychological domination over civil population as well. For example András Rácz constructed classification of the way in which hybrid warfare was conducted in Crimea and Eastern Ukraine, describes it as composition of three main phases - Preparatory, Attack and Stabilization phase. Where each phase consists of three sub phases with the list of conducted activities. His concept starts when adversary mapping out the strategic, political, economic, social and infrastructural weaknesses and the vulnerabilities of the target country. This includes establishing of political and cultural organizations loyal to Russia, gaining economic influence, building strong media positions, strengthening separatist movements and other anti-government sentiments, all with the aim of putting pressure on the target government, thereby serving the interests of the Russian state (Rácz, 2015, p.58). Evaluating his listed activities, it is clear that separatist movements and strong anti-government sentiments could be implemented when government is weak and society is suffering of economical insufficiency. Exactly such kind of situation was reached in 2014 'when Ukrainians stood their ground in defence of democracy and rule of law, protesting against government corruption and demanded the closer integration of Ukraine with the European Union' (Maidan, 2015). It leads to the assumption that more, other activities were carried out previously to reach instability in Ukraine. Or,

does Russia just used the window of opportunity to implement hybrid warfare in Ukraine?

One can argue that to shape the country as Ukraine it will be a time consuming process and state as Russia with the lack of strategic thinking (Kolesnikov, 2015) and changing military system (Nichol, 2011) is not able to wage a hybrid warfare which lasts decades. This statement could be truth if we are looking to hybrid war as a long term single military operation.

For example Danish Physicist and Biologist named Per Bak created an idea about the sand pile model. Bak's idea was simply enough, but in the same time complicated, containing multiple layers of complexity and thousands of interacting possibilities that the current understanding is unable to explain. His theory stated that if you piled sand, grain by grain, until it made a cone about the size of your fist, how would you know when that tiny pyramid would have a little avalanche? After all, when the pile got taller, and the sides become steeper, it becomes sure that some of sand would slide off. Could you predict when? Could you predict how much? Simple questions, but terribly complicated in their essence. In addition Bak observed that after some period of time the stack would organize itself into instability, a state in which adding just a single grain of the sand could trigger a large avalanche – or nothing at all. The importance in Bak's idea was that those sand pile cones looked relatively stable and fundamentally build, but in fact were deeply unpredictable (Ramo, 2009, p.48-49).

Similarly, it can reflect on hybrid warfare “mechanism” where cone becomes “country” and all implemented hybrid activities are to be seen “grains of the sand”. Each implemented activity or event is oriented to serve the interests of the Russia representing economic, social, political information and much wider scope of legal activities to shape victim's countries environment in fertile soil for hybrid warfare. Each implemented grain may not have any hostile characteristics by itself; it could be Russian artist concerts, donated history or study books with pro-Russian understanding of events for schools, establishment or support of pro-Russian media and etc. Additionally the target country is creating “sand grains” by itself as well by corruption, unresponsive governance etc. forcing society indirectly set up Russian values higher than their own. In such situation the victim country becomes like sand cone, which looks fundamentally build, like Ukraine's state administration system, but

deeply implemented activities slowly turning the state into instability condition where any following activity/event could trigger regime change, mass riots or movements. All those legal activities or “sand grains” could be implemented mainly by Russian civilian companies, non-government organisations who are pro-Russian oriented. In this shaping phase it does not matter when and what will trigger an avalanche because all activities together are building sand cone where avalanche becomes imminent. The essential in all this shaping process of hybrid war becomes a Russian decision – will it implement hybrid warfare’s scenario when avalanche happens or will it wait for the next, maybe better opportunity. This theory supports events what could have been seen in Ukraine, Estonia and Latvia, where Russia just tried to speed up avalanches in post-Soviet countries testing their readiness to deal with hybrid threats. For example Tallinn’s Bronze Soldier statue riots in 2007. where Russian embassy instructed local extremists and organizers, (RKK ICDS, 2007) giving later possibility to Russian Foreign Minister Sergei Lavrov warn Estonia, that Moscow would "take serious steps" (Spiegel, 2007).

Another example is Riga’s anti-government riots in 2009. where later some of Latvian politicians accused some “Russian’s political forces” of staging the protests in the capital of the Baltic state. Soon those accuses were denied by Russian ambassador in Riga (Sputnik, 2009) calming down tensions till the moment when was found image footage showing that one person participated in Riga and Doneck riots (Цензор.НЕТ, 2014) linking to the assumption that Russian radical groups at least monitored and tested those events. Moreover assessing events in Baltic States we can assume that necessary effects and significant society support was not reached and quickly lowered tensions did not create fertile soil for the implementation of hybrid warfare.

Contrary in Ukraine, where Euromaidan protests in 2014., lead to Ukrainian revolution, rising high tension and society dissatisfaction gathering from 40000 to 100000 protesters - Russia decided to act (Atlantis, 2013). Ukrainian president Yanukovych rejection of a pending EU association agreement, choosing instead to pursue a Russian loan bailout and closer ties with Russia was the trigger point for protests.

From Russian perspective, these protests become a threat to lose their potential Eurasian business space and if protests succeeded, it could pose threat to Russian

authoritative regime, showing to Russian people, that there is another way. To mitigate growing threat Russia implemented hybrid warfare using a multi modal wide range legal and illegal activities already roughly tested in Baltic States.

To sum up all above mentioned events, looking through Per Back sand pile model all those activities precisely resembled sand piles avalanches, encompassing several years of already implemented activities building up a cone of sand and turning it into instability. In Ukraine case cone was much bigger and avalanche more powerful, triggered by pro-Russian oriented President Viktor Yanukovich. Overlooking those avalanches it raises the question was it possible to avoid these events. Well, it is possible to predict how one or two, even hundreds of Russian implemented activities will influence the country, but if those activities become Russian foreign policy, measured in thousands and delivering approaches are changing all the time, it makes impossible for the victim country to measure every little detail. Moreover it turns into a situation that even guess what may happen next becomes impossible, similar how it works in the sand pile model. The result, according to sand pile model is a sand avalanche and when it happens, Russia already has its hybrid war scenario prepared to implement in victim country. However after each avalanche, could it be a riot or mass movement's – victim countries are analysing the results assessing contra strategies, pushing Russian side to discover and adapt new technologies, approaches for more effective implementation for more devastating result, forming again sand pile into the cone. But one can ask, is it so certain that this sand pile model always will work? The answer could be no, if victim's country and its government will be united with strong nationalistic feelings and could maintain high society support. However from Russian perspective, it becomes the portion of hybrid activities and environment shaping to draw victim's country's attention into sand pile grains, forcing it to figure out how grains interact with each other what could be the circumstances, coincidences and other aspects. Moreover, victim country, putting its efforts to figure out thousands of varieties how the sand pile model works wasting its security sources and financial resource which plays on Russian hand, because there is no similar sand pile in the world. Potential victim country instead of competing with Russia should turn its efforts to establish effective and toward a society oriented government system, rising in people strong national strength and identity. In addition, all those activities should be strengthened by effective and modern military and law

enforcement power, spreading away Russian implemented activities without forming grains into a cone shape and turning it within time consuming and dull efforts.

The idea of the sand pile model is to shape one's country in fertile soil for other military means as mass protests, riots, rebellion what later turns into military resistance. The most important in all processes becomes unidentified adversary's militants (without insignia) without clear representation of their country of origin. Similarly, how it happened in Ukraine scenario.

The Russian hybrid war outbreak in Ukraine. Can it be contagious?

Western society was caught by surprise when unknown Russian speaking units appeared in Ukraine and started to "protect" Russian citizens in Crimea and continued military operations in Eastern Ukraine, those activities Kofman and Rojansky distinguish into two distinct phases of operations in Ukraine, the first is the occupation and annexation of Crimea, and the second, invasion of Eastern Ukraine's Donbas industrial region. In those phases Crimea began as a covert military operation, combining ambiguity, disinformation, and the element of surprise at the operational level with more traditional aids such as military invasion (Kofman and Rojansky, 2015).

During the attack phase the key successes for Russians in Ukraine become the ability to blend different means to reach the common goal. Like Russian media, electronicall warfare, psychological operations, economical tools were employed and lead in a coherent way to support military invasion. Russian media conducted aggressive and pro-Russian oriented broadcast causing distorting perception of events among Ukraine people. The misinterpretations of events were broadcasted as well with European and Russian channels significantly overrunning other media who were not influenced by Russian money, reducing the ability among decision makers to act in a fast and assertive way. 'As America's UN ambassador, Samanta Power said "Russia apparently thinks it can convince the world community that up is down and black is white"' (Gedmin, 2014). Additionally misinterpretation of events was mixed with fast, precise military activities in Crimea catching by surprise Ukraine's militaries and limiting their ability to withstand Russian new generation warfare actions. The main objectives in operation become people mind and creation of

uncertainty, spreading unwillingness to resist among Ukrainians. Moreover the unwillingness was reached by effectively using pro-Russian population standing between armed units and Ukrainian's militaries. 'For example, several hundred unarmed protesters seized a Ukrainian naval base at Novofedorivka letting to armed units circle base without resistance' (BBC News, 2014). Furthermore implementing electronic warfare and cutting communication channels at military bases, Ukraine units did not get any order or clear guidelines from Kiev. Questionable was armoured unit appearance, because units were without insignia and Russia just later admitted that Russian regular armed forces were involved in Crimea. However, when the conflict escalated and Western world started to respond with financial and economic sanctions (EU news room, 2016), Russia targeted Europeans vulnerability of gas import (Chyong and Tcherneva, 2015), clearly warning western countries about consequences (EurActiv, 2014).

These executed offensive operations and vision of new generation warfare relatively were covered much earlier in Russia's 2010 Military Doctrine. Where characteristic features of contemporary conflicts were presented like:

- 'Integration of military force and forces and resources of non-military character;
- The intensification of the role of information warfare.

Additionally features of modern military conflicts were mentioned like:

- The presence of broad range of military-political, economic, strategic, and other objectives;
- The prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the use of military force' (The Military Doctrine of the Russian Federation, 2010).

Are those listed points providing insight into hybrid war? Definitely, yes and representing changed Russian perception how war should be waged. Moreover, this doctrine is approved for the period through 2020, giving understanding that Russian's intent is to develop more capable military how it was known so far. All above listed, clearly indicate that Russia will develop hybrid war tools and melt them with non-military character creating combatant power without clear membership to country of

origin, rising possibility to execute more devastating new generation warfare in the future.

Taking look to other countries' experience, it becomes clear that 'Russian new generation warfare principles starting to appear in Middle East conflicts and some of characteristics have been used in North Africa as well' (Chekinov and Bogdanov, n/a, p. 14), identifying hybrid warfare as a beginning of new "military age", bringing other country's attention toward the possibility to cheat international law and test current world order durability.

Is Russian hybrid warfare adoptable to test NATO and its Article V?

The one of the most powerful peace supporter in the world is NATO with its collective defence module. According to Article V, attack against one Ally shall be considered as an attack against all Allies, triggering individual or collective defence toward adversary. Additionally, Article III states, that each country separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack (Lillian Goldman Law library, 2008.).

Assessing NATO's Articles V and III, it is clear that decision to help one Ally will be made by each Nation's politicians who will become the target auditory in the hybrid war scenario. Moreover, some of the NATO's countries are not so successful to develop their own military capabilities that could raise the doubt for defence necessity and decrease the willingness to sacrifice any other country's military units in case of attack. Even NATO Articles by them self opens door for uncertainty and discussion for other NATO member countries. This means that in case of aggression there could be conducted strong information operations using media capabilities around the world to put in doubt decision makers. Some of the source could be Sputnik or Russia Today — or RT as it has rebranded itself since 2009. It has a growing budget and President Putin himself have intervened to protect it against cuts. The network now claims a worldwide audience of 700 million and extends it every day (O'Sullivan, 2014). Showing intentionally that media field is important and well supported by Russians government findings, playing a significant role in Russia's strategy.

Significant moment to test Article V, becomes Russian policy toward neighbour countries, stubbornly targeting their national interests and values using the sand pile

model. By creating instability and implementing pro-Russian oriented activities, using civilian companies and NGOs, they may gain slow movement toward population diversity and potential friction between local national and pro-Russian oriented groups. All activities may be conducted without direct involvement of any kind of official Russian government institutions. This assumption strengthens statement by Gerasimov during a conference in Russian Academy of Military Science; 'that Russia should develop a strategy how to answer Western "soft power" where regular force actions are unacceptable by targeting adversary's country without occupy its territory' (Нагорных , 2016). In addition, there could be used economical tools to speed up situation worsening in neighbour countries or as a warning tool toward other European nations to calm tensions and gain temporary indecisiveness. All those actions could be strengthened by covertly infiltrated "volunteers", retired special force representatives, *Kazak* units, like riot organisers and participants mixing them with local pro-Russian activists. Such kind of cocktail will blur the line between kinetic and non-kinetic actions, letting Russia to keep its unchanged status internationally without losing its face. Never less it will put the advantage in Russian hands, because for NATO it could become impossible to trigger article V and define where attack starts and where it turns from intra-state conflict into inter-state conflict.

All above mentioned shows that Russia by executing hybrid warfare strategy against NATO countries could challenge its cohesion and validity of its article V. Moreover well planned Russian hybrid activities by their modularity and diversity could become challenging for NATO if timely counter measures are not taken.

Evaluating all mentioned hybrid warfare aspects in the essay, it becomes clear that today's technology development and dependence of economic and natural resources influence war waging principles, drawing countries into new multimodal activity research. Russian implemented hybrid war in Ukraine opened door for new war waging approach, which concept can become contagious to other countries and implemented as a tool to test current world order. In hybrid activities there is no clear border where hostility starts and when it turns into inter-state conflict, because according to sand pile model, taken actions may not hold any hostile or planned characteristic by itself. Moreover the temptation becomes ability for authoritarian countries like Russia conduct hostilities by other countries citizens' hands without direct involvement of their troops and without losing its face on international arena. Considering potential challenges NATO should develop clear crisis response

scenarios were each member country unmistakably understood the signals of hybrid activities and has common clearly stated red line beyond which defence becomes collective activity. In addition, hybrid warfare by itself becomes a new war waging principle which already has thrown down the gauntlet to today's international law and the current world order.

Bibliography:

Atlantis, 06.12.2013. Ukraine's Threat to Putin. [online] Available at: <http://www.theatlantic.com/international/archive/2013/12/ukraines-threat-to-putin/282103/> [Accessed 27 February 2016].

Balasevicius T., 11.10.2015. Russia's "New Generation War" and Its Implications for the Arctic. [online] Available at: <http://mackenzieinstitute.com/russias-new-generation-war-implications-arctic/> [Accessed 2 February 2016].

BBC News, 22.03.2014. Russian troops have stormed a Ukrainian airbase in Crimea throwing stun grenades and firing automatic weapons in the air. [online] Available at: <http://www.bbc.com/news/world-europe-26698754> [Accessed 9 March 2016].

Chekinov S.G. and Bogdanov S.A., n/a. The Nature and Content of a New-Generation War. [online] Available at: http://www.eastviewpress.com/Files/MT_FROM%20THE%20CURRENT%20ISSUE_No.4_2013.pdf [Accessed 14 March 2016].

Chyong C.K. and Tcherneva V., 17.03.2015. Europe's vulnerability on Russian gas. [online] Available at: http://www.ecfr.eu/article/commentary_europes_vulnerability_on_russian_gas [Accessed 9 March 2016].

Cooper R. J., 2009. The Age of the unthinkable. New York, Boston, London: Little, Brown and Company. Page 48-49.

EurActiv, 11.09.2014. Moscow limits German and Polish gas flows as 'warning'. [online] Available at: <http://www.euractiv.com/section/global-europe/news/moscow-limits-german-and-polish-gas-flows-as-warning/> [Accessed 9 March 2016].

European Union news room, 18.03.2016. EU sanctions against Russia over Ukraine crisis. [online] Available at: http://europa.eu/newsroom/highlights/special-coverage/eu_sanctions/index_en.htm [Accessed 9 March 2016].

Gedmin J., 2014. Beyond Crimea: What Vladimir Putin Really Wants? [online] Available at: <http://www.worldaffairsjournal.org/article/beyond-crimea-what-vladimir-putin-really-wants> [Accessed 8 March 2016].

Kofman M. and Rojansky M., 2015. Closer look at Russia's "Hybrid War" [online] Available at: <https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf> [Accessed 8 March 2016].

Kolesnikov A., 09.09.2015. The Russian Regime in 2015: All Tactics, No Strategy. [online] Available at: http://carnegie.ru/2015/09/09/russian-regime-in-2015-all-tactics-no-strategy/ih3t_ [Accessed 23 February 2016]

Lillian Goldman Law library, 2008. NATO Treaty; April 4, 1949. [online] Available at: http://avalon.law.yale.edu/20th_century/nato.asp#art3 [Accessed 15 March 2016].

Maidan, 2015. EuroMaidan (2013-2014). [online] Available at: <http://world.maidan.org.ua/category/civic-campaigns/euromaidan-2013-2014> [Accessed 23 February 2016]

Maigre M., 2015. Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO. [online] Available at: www.gmfus.org/file/4272/download [Accessed 18 November 2015].

NATO Review magazine, 2015. Hybrid war – does it even exist? [online] Available at: <http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm> [Accessed 18 November 2015].

Nichol J., 24.08.2011. Russian Military Reform and Defense Policy. [online] Available at: <https://www.fas.org/sgp/crs/row/R42006.pdf> [Accessed 23 February 2016].

O'Sullivan J., 06.12.2014. Russia Today is Putin's weapon of mass deception. Will it work in Britain? [online] Available at: <http://www.spectator.co.uk/2014/12/the-truth-about-russia-today-is-that-it-is-putins-mouthpiece/> [Accessed 15 March 2016].

Pawlak P., 2015. Understanding hybrid threats. [online] Available at: <http://epthinktank.eu/2015/06/24/understanding-hybrid-threats/> [Accessed 2 February 2016]

Podbay, 2012. NATO Review: Hybrid War – Hybrid Response? [online] Available at: <http://podbay.fm/show/950410144/e/1418242051?autostart=1> [Accessed 16 January 2016].

Rácz A., 2015. Russia's Hybrid War in Ukraine, Breaking the Enemy's Ability to Resist. Helsinki: The Finnish Institute of International Affairs, page 58. [online] Available at: <http://www.isn.ethz.ch/Digital-Library/Publications/Detail/?lang=en&id=191590> [Accessed 17 January 2016]

Research of the Commission of the Historians of Latvia 2003., Totalitarian occupation regimes in Latvia in 1940-1964. Volume 13. Riga: Institute of Latvian History, 2004. [online] Available at: http://www.president.lv/images/modules/items/PDF/item_1618_Vesturnieku_komisijas_raksti_13_sejums.pdf [Accessed 17 January 2016].

RKK ICDS publication, 11.05.2007. Russia's Involvement in the Tallinn Disturbances. [online] Available at: <http://www.icds.ee/publications/article/russias-involvement-in-the-tallinn-disturbances/> [Accessed 23 February 2016].

Spiegel, 27.04.2007. Deadly Riots in Tallinn: Soviet Memorial Causes Rift between Estonia and Russia. [online] Available at: <http://www.spiegel.de/international/europe/deadly-riots-in-tallinn-soviet-memorial-causes-rift-between-estonia-and-russia-a-479809.html> [Accessed 23 February 2016].

Sputnik, 20.02.2009. Ambassador denies Russian involvement in Riga clashes in Jan. [online] Available at: <http://sputniknews.com/world/20090220/120232559.html> [Accessed 24 February 2016].

The Military Doctrine of the Russian Federation, 05.02.2010. Approved by Russian Federation presidential edict. [online] Available at: http://carnegieendowment.org/files/2010russia_military_doctrine.pdf [Accessed 9 March 2016].

TZU, S., Art of War. Translated by Ralph D.S. 2003. Philadelphia, London: Running Press.

Williamson M. and Mansoor P., 2012. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present, Cambridge: Cambridge University Press, p. 321.

Нагорных И., 01.03.2016. "Цветным революциям" ответят по законам гибридных войн. [online] Available at: <http://www.kommersant.ru/doc/2927168> [Accessed 17 March 2016].

Цензор.НЕТ, 15.03.2014. Один и тот же российский "турист" участвовал в беспорядках в Риге в 2009-м, и в Донецке в 2014-м. ФОТОфакт. [online] Available at: http://censor.net.ua/photo_news/275927/odin_i_tot_je_rossiyiskiyi_turist_uchastvoval_v_besporyadkah_v_rige_v_2009m_i_v_donetske_v_2014m_fotofakt [Accessed 24 February 2016].

Higher Command Studies Course (HCSC)

Can small- and medium-sized states have grand strategies?

LTC Armin Wagner

Introduction: The David Example

‘Meanwhile, the Philistine, with his shield bearer in front of him, kept coming closer to David. He looked David over and saw that he was only a boy, ruddy and handsome, and he despised him. [...] David ran quickly toward the battle line to meet him. Reaching into his bag and taking out a stone, he slung it and struck the Philistine on the forehead. The stone sank into his forehead, and he fell face down on the ground. So David triumphed over the Philistine with a sling and a stone; without a sword in his hand he struck down the Philistine and killed him’ (1 Sam 17:41 - 17:50).

In one of the most famous scenes of the *Old Testament*, a lightly dressed small shepherd boy wins against ‘a champion’ who was ‘over nine feet tall’ with a ‘bronze helmet on his head’ and ‘a coat of scale armour’ (1 Sam 17:4 – 17:5). Prominent evidence of world literature – the Holy Bible – tells us that the small can defeat the big, the raider the regular, the outsider the favourite. ‘Greatness’, this may be the lesson of that ancient story, is not about size and appearance, but about ideas and performance. The same might be said about world politics.

Might the same be really said about world politics? Most states of the world are not ‘Great Powers’, no ‘Goliaths’, but small- or medium-sized. This paper tries to find an answer to the following questions: (1) Are there strategies that help such small- and medium-sized states to survive in international politics? (2) Is there something like a ‘Lilliputians’ choice’ for the minors to craft own grand strategies?

Our discussion starts with questioning what we can understand as ‘grand strategy’ – in difference to the more common term of ‘military strategy’. Whereas we have a clear understanding of the meaning of ‘policy’, ‘politics’ and ‘polity’, ‘strategy’ keeps more in the darker shade of pale. Though we are not going to write an encyclopaedia on formal definitions, we also have to ask what characterizes small- and medium-sized states. Following that, we will compare different strategic baselines in search for starting points to develop grand strategies. We do not elaborate on the situation of the Baltic States in particular. Neither the question we work on nor our theory-driven line of argumentation urges us to do so. Moreover, the situation of the Baltic States

was examined under that specific aspect just recently (Nilsons, 2015, pp. 150-153; see also Molis 2006; Paulauskas 2006).

Heading on this way, the link between ‘grand strategy’ and the all-overarching dimension of politics is still missing: ‘power’; in our case especially in relation to the questioned ‘size’ of states. The importance of the realist’s category of power is also accepted by scholars of liberalism, institutionalism and even constructivism – they just have a different understanding of the matter.

David’s fight against Goliath is partly proof of the realist theory, partly not: According to most of their representatives, only Great Powers rule the game – and win the fight. The victory of the small is not anticipated. However, the use of force as a means of struggle between states (here: between the Philistine’s and the Israelite’s) is within the explanation scheme of the realist school. Our hypothesis is that the minors can be policy-makers, not only policy-takers; actors, not only factors. Simply said, they can have a grand strategy. Nevertheless, the use of direct force or coercion usually is an inappropriate means for them.

We will frame the way to verify or falsify this hypothesis systematically with theoretical substance – what we are primarily interested in – and by some empirical evidence (with short EXAMPLES). Eventually, we will see that the cosmos of world literature offside the Holy Bible supports our answer figuratively.

The Secrets of Strategy

Much was written and said about strategy. While it is quite clear that its origins lie in the military field, today every societal domain seems to develop its very own strategy (and, additionally, its own selling ‘narrative’). Sport offers a lot of colourful examples. Take Formula One: Mercedes and Ferrari, McLaren and Williams do not simply compete in races; already the choice of different wheels according to the weather conditions and the set-up of the cars are not considered anymore as a simple question of technology or of racing tactics, but one of a declared ‘wheel strategy’. But not every strategy leads to world championship or is a strategy at all.

Many masters have thought about classic, i.e. military strategy. In a widely agreed canon, Sun Tzu represents the beginnings, leading to the grandmasters Clausewitz

and Jomini and further to Liddell Hart and J.F.C. Fuller (for details see Paret, 1986; Handel, 2001; Bartholomees, 2012). Some thinkers may be considered as post-modern strategists, to name just Edward Luttwak and Martin Van Creveld, or Colin S. Gray and Hew Strachan. But are they strategist or do they merely write about the idea and history of strategy, as did Lawrence Freedman in his latest work (Freedman, 2013)?²⁴

Most of military strategists, aware of the interplay of politics and war as well as between human nature, (mass) psychology and war, considered elements of grand strategy in their theories. Clausewitz spoke of the ‘remarkable trinity’ of war, within government, military and the people are influencing each other. He saw neither ‘purely military evaluation of a great issue, nor of a purely military scheme to solve it’, and underlined quite famously that ‘war in itself does not suspend political intercourse or change it into something entirely different’ (Quoted by Jablonsky, 2012, p. 4).

Military strategy, therefore, is part of something bigger. This ‘bigger’ we may name ‘grand strategy’ (on the term, also in comparison with ‘national’, ‘major’ and ‘minor’ strategy, see Layton, 2012). Williamson Murray teaches us that ‘grand strategy demands an intertwining of political, social, and economic realities with military power’ and, moreover, ‘a deep understanding of the past’ and ‘a comprehensive and realistic understanding of the present’ (Murray, 2011, p. 5). History pays tribute to a grand strategy as well as the impact of geography (Gray, 1999 a); the domestic and societal environment influences strategy-making very deeply; and culture counts as well as ideology. The (constructed) worldviews pour into the (real-world related) strategy draft. Grand strategy – its making, prevailing and persisting – is not only about hard facts and skills; it is ‘a willingness to challenge one’s own assumptions and the myths and truisms of one’s own culture’ (Murray, 2011, p. 6). To stay in accordance with the values and beliefs of the own culture (or nation), grand strategy needs ‘a proper ethical and legal basis’ (Melvin, 2012, p. 21).

At the same time and foremost, grand strategy is directed to the adversary outside, the neighbouring states, international politics, and has to keep in mind that change

²⁴ A graduate of history studies may call himself a historian; but is a graduate of philosophy a philosopher? This question seems very much the same for writers on strategy.

constitutes the world. Uncertainties about attitudes of third players are most relevant for the creation and constant redefinition of every strategy (Rostoks, 2010, pp. 95-98). On this basis, we see that ‘the essence of grand strategy is its integrative nature’ (Layton, 2012, p. 58).

The before said as a framework in mind, we follow Basil H. Liddell Hart`s definition as developed in his famous book on *Strategy* – with the one major exception, that we do not consider ‘grand strategy’ as a requirement of wartime only, but at peacetime as well; especially in a time, when war and peace are not necessarily two different states of action anymore but could float in a ‘hybrid’ condition. Liddell Hart wrote:

‘[T]he term “grand strategy” serves to bring out the sense of “policy in execution”. For the role of grand strategy [...] is to coordinate all the resources of a nation, or a band of nations, towards the attainment of the political object of the war [our approach: of the state] – the goal defined by fundamental policy’ (Liddell Hart, 1954 [1941], quoted by Bartholomees, 2012, p. 14).

Finally, in this short attempt to make the term productive, it should have become clear that grand strategy always requires further development – a *product* and a *process* at the same time, or, according to Hew Strachan: ‘as much a way of thinking as a way of doing’ (Strachan, 2011, p. 1281). Like deterrence, grand strategy may have worked yesterday, which does not mean that it will work tomorrow in ‘a word of flux’ (Gray, 2000, p. 259; quotation: Murray, 2011, p. 11). Considering the past, we resume, grand strategy is directed towards future. We therefore add to the above stated definition the following outlook:

‘Grand strategy try to shape the future in a certain sequence into a preferred construct that displays the desired orderliness and stability’ (Layton, 2012, p. 59; see also Strachan, 2011, p. 1296).

In this broader concept, military strategy is ‘the bridge that relates military power to political purpose’ (Gray, 1999 b, p. 17). The military strategy has to serve the grand strategy, not the opposite. To give a well-known EXAMPLE: When Germany entered First World War, there was only a military strategy, not a ‘grand’ one, and consequently no independent political choice: To avoid war at two fronts (what eventually happened and was mastered relatively well by the Germans at the Eastern and clearly badly at the Western Front), in case of war declaration France had to be attacked immediately to redirect the German troops directly afterwards to East

Prussia to defend against Russia. No German grand strategy had preserved wiser solutions, and politics was bound to a short-sighted military strategy. The original role of military strategy, demonstrated by this example of failure, is to submit military advice in the political context, but not to take over comprehensive strategic or political responsibility.

Grand strategy and military strategy have in common that they become operational in the system of ends (objectives), ways (concepts) and means (resources), or simpler: 'This is where we are going, here is the plan and this is how we will carry it out' (Elliott, 2015, p. 148; also Jablonsky, 2012, p. 3). But what distinguishes both spheres deeply is that grand strategies today are designed to keep state and nation out of risk; state actors tend to be defensive and reactive, whereas on the contrary the 'old school' generals have learned that a military strategy has to be decisive to lead to victory, therefore needs proactive initiative accepting uncertainties and risks (Strachan, 2011, p. 1284, 1287).

The Implications of Power and Size

Despite this reversal in the character of grand and military strategy, one understanding should be shared by the strategists of all schools: 'Where we are going', and what the plan might be, should not be born out of wishful thinking. The analytical device to match reality is *power*. There are other categories that influence theorists (and practitioners) of international politics, like *security*, *sovereignty* or *legitimacy*; but each of them fall under the insight that 'all politics is power politics in the sense that all politics involves power. This is not to say that politics is *only* about power' (Baldwin, 2002, p. 236 [italics in the original]; see also Mearsheimer, 2001, p. 12).

Power as an analytical device needs an explanation in itself. Theory on it has walked two different avenues: power seen as a property, and power seen as a relation. Regarding power as a property, some states are superior to others due to their geographical size, number of population, size of gross domestic product, or of armed forces size. SuffICIENTLY, such resources can be met only by a few international players at eye's level. Without any access to 'power' in this perspective, no argument then would support the assumption that the minor players in world politics can have a

grand strategy at all – they simply lack these kinds of ‘size’ and would therefore be powerless at all. That would exclude all but less than a dozen of the 193 UN member-states from the game. Such a disparagement would question not only the analytical skills of the term ‘small state’ – why to use it, then? – but also the relevance of nation states in international politics. Fortunately for our argumentation and the minor states, the property of power is not necessarily identical with its successful conduct. The development of the political landscape with more and more public interventions sets limitations of mistrust and blame on Great Powers’ options to show aggressiveness and use of force (Rostoks, 2010, pp. 88, 99).

It might be useful to remember the 1922 definition from Sociologist Max Weber, according to which power is ‘the opportunity to have one’s will prevail within a social relationship, also against resistance, no matter what this opportunity is based on’ (quoted and translated by Berenskoetter, 2007, p. 4). This Weberian understanding, though not originally speaking of international relations, is backing the ‘soft power’ school of institutionalism (fundamental: Keohane and Nye, 2011 [1977]; Nye, 2004): ‘[P]revail within a social relationship [...] no matter what this opportunity is based on’, leads exactly to the power-as-relation approach, which is the feasible way to understand ‘power’ as a more common good, achievable for the small-sized as well as for the big ones’ (Keohane, 1969, p. 298). Indeed, even the size of forces itself seems less relevant than the local military balance: troop deployments and dispositions, alert levels, fighting experience and the willingness to fight might be comparatively more decisive than pure head counts (Sim, 2007, endnote 22).

Seen that way, which patterns or standards could set the difference between the dozen giants from the hundreds Lilliput’s – or to deny exactly that divide? No Einstein of International Relations has ever come up with a general relativity theory of world politics; as in nearly every field of political science, no single agreed definition of ‘small states’ and ‘medium-sized states’ exists. The realist school, that categorized states mostly on ‘hard’ size items, has been challenged at the latest since the 1960s, when the question whether a state is ‘system-determining’, ‘system-influencing’ or ‘system-affecting’ became yardstick. First, behavioural patterns, adopted from a flourishing US research on psychology and sociology of the previous decade, reached the discipline of International Relations – attention was drawn in particular to actions and attitudes of small states in international organisations and

in political situations that required the capability of balancing different positions (Keohane, 1969, pp. 293-295, 298-303; Wilson, 2008, pp. 115-116, 120-121.). Second, as such political contributions and the resulting standing of states were difficult to measure, in addition to behaviourism the category of perception now played into theory and therefore also constructivist positions. In both the behavioural and perceptive perspective, not the 'hard terms' alone matter in the execution of power, but the calling of international institutions, the knowledge of actors and the perceptions of states' capabilities (Rostoks, 2010, p. 192). Power 'materializes' itself via these capabilities and via influence: how the actor handles his power in a certain situation under certain circumstances. 'If capability is defined as the potential power to affect others more than one is affected by others, it is no longer a property of a single actor'; or, more figurative: 'If the name of the game is bridge, the person with the good poker hand may be in big trouble' (Baldwin, 2002, p. 247, 251).

Up to here, it can be summarized that in a 'soft power' approach as developed above, 'size' becomes a question not only of fixed data. 'Smallness' (and, consequently, also 'greatness') then is mainly a matter of situation, opportunity and negotiation. A state has and realizes that it has limited capacities in a certain situation: it is 'small' in that domain (and in that moment); it has, maybe at the same time, well-balanced capabilities in another field and is 'medium-sized' in that respective; and it may have overwhelming capacities in a third discipline, being able 'to play bridge' with the big ones. Vatican, for EXAMPLE, not a Great Power in the realist sense, has no military power and cannot compete in a military duel with any armed state, but has moral influence especially in the Catholic World; Switzerland, mostly because of its geographical conditions, seems well equipped to defend itself by conventional military means, while aggregating its influence and wealth only out of its role as a key bank district; Luxembourg will not win any tank battle and is not world leader in moral matters, but as a powerful finance trading place has the capability to interact in European economy at high level (Rostoks, 2010, 94, 96; Carlsnaes, 2007, p. 13). Great Powers can also benefit from power understood as a relation, insofar they may use soft tools to follow their interest: For EXAMPLE, institutions like the British Council, the Institut français or the Goethe-Institut are designed to spread cultural understanding (and, doing so, indirect: influence) in their host nations.

Adopting this conceptualisation of 'size' in relation to 'power', we decide at this point of our argumentation to leave the distinction between 'small-' and 'medium-sized' states behind us. Instead, we are going to speak of the 'minors' or generally of 'smaller states'. Interestingly enough, this approach is in an indirect way supported by the progressive thinker of offensive realism, who only differentiates between the 'Great Powers' seeking to achieve hegemony in the international system and all other states that are not capable of playing in that league, whether they are in earlier definitions 'mini', 'small', 'medium' or 'secondary' (Mearsheimer, 2001, pp. 21, 362-363). Our working assumption of 'smaller states' implicitly accepts that there are states that are 'larger' or even 'great' in almost all fields in the shared perception of international actors.

The Choice of the Minors

Great Powers' might is a resource and obligation at the same time: It inherits the burdens of greatness and the risks of erosion. Smaller states can tacitly benefit from the shortfalls of Great Powers' politics, its stalemates and paralysis, and exploit the parameters of international politics (Wilkinson, 1985, p. 115; Wilson, 2008, p. 122; Rostoks 94, 99). Generally spoken, there are a couple of factors that may strengthen smaller states in international relations, among them: geographical location and climatic dimension; international law and international organisations as watchdogs; acclamatory limitation on a regional focus or a low, unattractive level of development; the preparedness for sacrifice; strong allies or in contrary a policy of neutrality; the image problem of Great Powers outing aggressive action in public (Paterson, 1969, pp. 120-122; Keohane, 1969, pp. 291-294). For each smaller state, only a few of these factors will be available. It is from utmost importance to identify them to adopt an own grand strategy.

But what leads to a successful grand strategy? Is there any rule of wisdom? It seems that at least three key aspects are important (Wivel, 2010, pp. 24-25):

- (1) The political substance of the smaller states strategy must be relevant for other actors; a contribution to a commonly recognised item is asked for rather than pushing one's own, completely different agenda;

- (2) the more vital the issue is, the less relevant may be the part of smaller states – in other words: smaller states gain more influence in political fields that are not top-level and should focus there;
- (3) smaller states can position themselves as honest brokers, between bigger rivals, namely in such fields where no other actor suspects hidden interests of the minor.

Thus said, theory based on empirical research offers different strategy designs. The following table gives a survey which basic strategy guidance is on the market. These baselines themselves do not formulate grand strategy at all relevant subfields of a countries' policy, but give underlying direction for the central strategic course. In a second step we are going to assess the results and concentrate on those baselines which give assets for smaller states.

<i>Strategy baseline</i>	<i>Relevance</i>	<i>Reference(s)</i>
Use or threat of force, direct coercion (War/Bait and Bleed/ Bloodletting/ Blackmail)	Relying on violence or coercive power may lead to short-term success; promises no survival in the long run and may lead to 'blame and shame'; usually not available for smaller states.	Mearsheimer, 2001, pp. 147-155
Self-Defence	Independent strategy; avoids being mastered by others; needs strategic circumstances that promise success.	Orvik, 1973, p. 228
External Balancing	A balanced state of affairs, guaranteed by Great Powers; usually positive for their partners.	Keohane, 1969, p. 300; Mearsheimer, 2001, pp. 156-157
Buck-Passing	Shifting the international burden to another state, while staying at the sideline. A 'free-ride', also a possible	Mearsheimer, 2001, pp. 157-163

	choice inside alliances.	
Bandwagoning	Joining a powerful opponent and conceding power to gain a bigger share of all common policy efforts.	Mearsheimer, 2001, pp. 160-163
Seeking Shelter	Becoming member of an alliance to borrow power, security and protection in a group of shared interests on partial costs of independence.	Keohane, 1969, p. 301-303; Orvik, 1973, p. 228
Binding	Creating and strengthening of international governance by international rules and institutions.	Keohane, 1969, p. 297; Keohane/Nye, 2011 [1977], pp. 23-37; Wilson, 2008, p. 114, 122; Wivel, 2010, p. 16
Defence against Help	Convincing a Great Power that the smaller state can defend against all possible third aggressors and do not need help.	Orvik, 1973, pp. 228-230
Hiding (Neutrality/Nonalignment/ Appeasement)	Avoiding conflicts intentionally; staying out of trouble by staying out of sight.	Karsh, 2011 [1988], pp. 37-42; Keohane, 1969, pp. 291-292; Wivel, 2010, pp. 15-16;

In evaluation of the different strategic baselines offered,

- the *use or threat of force* or *direct coercion* usually is beyond the opportunities of smaller states; Great Powers may choose these strategies. There are some exceptions: for EXAMPLE the fight of the Vietminh against the French, and of

the Vietcong against the Americans – typical wars of the period of decolonisation and its aftermath, backed-up by a (hidden) bigger ally and, in the American case, by public opinion in the opponent`s country. (North Korea today is not a proof: It has manoeuvred itself in the role of a world outlaw, completely isolated from international politics and economy.)

- *Self-defence* is a best practice but needs to face preconditions that only very few states will meet. The best-known EXAMPLE for a smaller state that is following this strategy is Israel (which has a nuclear option as last resort), another one is Taiwan.
- *Defence against help* messages to the potentially threatening Great Power in a credible way that the messenger state is capable to defend itself against all other countries around (except the Great Power) and needs no assistance by that Great Power. This is an ambitious and complex approach, successfully used for EXAMPLE by Finland and Sweden towards the Soviet Union during the Cold War and failed by Norway in 1940, when Oslo aimed on convincing the British (that were assumed as possible rival in the North Sea) that it was able to defend itself and overlooked that the Germans were the true challenger. Like self-defence, it needs very special geographical and/or historical circumstances.
- *External Balancing* may produce a favourable international setting for smaller states when Great Powers are occupied with balancing the world system. Small states may benefit from the specific combination of competition and consensus. A good EXAMPLE could be seen in the policy of the Kingdom of Sardinia: It benefitted from the Vienna Congress 1815 and not only got back Savoy, Piedmont and Nice out of the bankrupt`s estate of Napoleonic France, but additionally Genoa. But external balancing is, nevertheless, not a way to be gone by own resources and means, because it is negotiated mainly by the Great Powers.
- *Buck-passing* and *bandwagoning* are opportunistic baselines, at first glance a good choice for ‘free-rides’, which finally lead away from a grand strategy, due to the reduced and subordinated chance to actively design the own foreign policy. The consequence of the British Appeasement Policy in 1938, for EXAMPLE, was that the responsibility (the buck) of major warfare against Nazi Germany was passed to Soviet Russia, while at the same time France jumped

on the British bandwagon that seemed to offer a solution to escape armed conflict with Berlin. For smaller states both baselines are strategic calculations that rely on the mercy of the Great Power that is addressed.

- *Seeking shelter* is a very reasonable way to go for a minor since millennia. In an alliance, smaller states benefit from the aggregation of power and the promotion of international order exercised by the alliance members. Inside the alliance, the junior partners have duties, but are able to influence the grand strategy of the alliance and can develop national strategies especially on fields like development policy, energy policy, environmental policy and domestic policy. Nevertheless, alliances reduce independent strategy making in the core domains of foreign and security policy. Looking at the EXEMPLARY Cold War alliances, Western European countries went very well in joining the umbrella of North Atlantic Treaty Organization, which was/is a body of negotiations. On the contrary, in the Warsaw Pact the single Eastern European state actors strictly had to follow the strategic outline of the dominating Great Power. In the current political situation, the Kremlin Policy towards its neighbours make NATO membership a good deal for the geographically exposed Baltic States, where the strategic advantages of having 25 partners outweigh the limitations of independent strategy making.
- *Hiding* strategies aim on the preservation of state autonomy. Among the hiding options, *nonalignment* and *appeasement* are very much related to certain historical moments. Nonalignment (Bandung, 1955) was not simply a policy of neutrality, but looked – without bigger success – on becoming a more or less equal third power next to USA and USSR. Appeasement ('Peace for our time', 1938) lost all its reputation and credibility when the appeaser sacrificed sovereignty of Czechoslovakia on behalf of a superficial, friable peace with the dictator Adolf Hitler. *Neutrality*, in contrast, is a sophisticated concept, and, in a way, the bigger brother of defence against help. Neutrality is not a strategy that can be adopted in an occurring threat; its credibility depends very much of its long-term proof and strict performance. Its balance sheet is controversial: For EXAMPLE, out of six neutral countries in Second World War, the Finnish and Norwegian grand strategies of neutrality collapsed, while Ireland, Switzerland, Spain and Sweden managed to stay neutral. During the Cold War, Switzerland and, geographically more exposed, Finland played the neutrality

card in a very successful manner. Such a success gives evidence for the capability of a state to develop an independent grand strategy. Nevertheless, it remains a major problem of neutrality that it limits the room for political manoeuvre up to self-abandonment in case that the foreign opponent changes its acceptance of that declared neutrality. Though neutrality is the only suitable hiding option, finally this strategic baseline makes smaller states more a subject than an object of politics.

- *Binding* reconciles soft power tools with the concept of power as a relation. Soft power instruments are law and justice, decision-making rules, values and attitudes. Attraction and persuasion rather than force and coercion are basic concepts. International organisations are in the centre of political doing. Smaller states should be aware of their own limited capabilities and focus on launching and supporting initiatives, acting as mediator and build issue-related coalitions. The emphasis of international calibre in world politics back-up the relevance of smaller states by the inherent formal equality of players, by internationally organized security offers and by shared capacities to restrain Great Powers. Even the pure perception of being part of the international process and having a systemic role in world politics is important for the smaller states position (Keohane, 1969, p. 294, 297; Nye, 2004; Wilson, 2008, p. 114; Wivels, 2010, p. 26). The Benelux countries in the initial phase of what now is the European Union might be an EXAMPLE, or today the Netherlands as host of important international courts (while being member of NATO alliance at the same time).

Among these selected strategy baselines usually Seeking Shelter, Binding and Hiding seem to be most reasonable for smaller states. Each of these three options has its advantages and disadvantages, and which to choose is very much dependent on the situation of the respective country. The connectedness of single countries policies, regional organisations and international institutions may favour a certain mix of concepts: Both alliance membership and empowerment of international regimes of world order – seeking shelter and binding – are not contradicting or itself-excluding strategies, but a rational entanglement. Alliance membership is the one appropriate strategy to follow under conditions of threat. Binding appears an ‘elegant’ and smart-thought strategy for smaller states in a certain ‘comfort’ zone of international politics that opens way to an independent grand strategy. Nevertheless, a strategy based on

soft power tools is not starry-eyed idealism; like for hard power, for soft power the national well-being is the political purpose.

This is central: The different strategic baselines presented above have to be improved by knowledge of the strengthening factors and under consideration of the three key aspects mentioned above – that means, in a realistic assessment of the own situation. Only then they stand the proof with regard to the question of our introduction: if there is a ‘Lilliputians’ choice’ for the minors in international policy to craft own grand strategies and, as a consequence, act independently in world arena.

Conclusion: The Mowgli Approach

In this paper, we have argued that the ‘smallness’ of smaller states is perceptual and contextual, not static but variant – different states have different power options, related to particular conditions. We have further underlined that the ‘notion of relativity’ (Carlsnaes, 2007, p. 13) is a chance for smaller states in international politics in regards to the traditional categories of ‘size’ and ‘power’. Important precondition is the states’ ability to self-assess realistically their respective capabilities and to obey some key aspects of strategy-making. In this view, smaller states are able to follow their own political ends on their own strategic ways and finally craft ‘grand strategies’, under certain circumstances with restrictions in the fields of foreign and security policy.

Far from being fixed in a comprehensive definition and due to its fluent character, any strategy does not produce eternal verities or provide physical regularities. It was once compared with a French peasant soup: ‘a mixture of items thrown into the pot over the course of a week and then eaten, for which no recipe can possibly exist’ (Murray, 2011, p. 9). Even more challenging than to describe what ‘grand strategy’ accurately means, is to work on it in a consistent manner. As a baseline for that undertaking, among a number of options discussed by scholars we have suggested that seeking shelter (alliance membership), hiding (neutrality) and binding (promoting international governance) are the most suitable ones. Joining an alliance might be best choice in most cases; hiding requires a pronounced credibility; binding needs larger efforts to retain in international politics, but opens way for a relatively

independent grand strategy. *In praxi*, elements of the presented strategic baselines will often be mixed.

Dependent from the theoretical approach and its practical derivation, smaller states are not out of bounds in international politics. Their ways and means to achieve the ends of survival and influence differ from Great Powers. Soft power may suit them better than hard power. Little shepherd boy David used cleverness and force to win over Goliath. Nowadays, the knowledge of the international environment and the ability to find partners in an uncertain world are requested by the minors:

‘Mowgli stood upright - the fire pot in his hands. [...] He flung the fire pot on the ground, and some of the red coals lit a tuft of dried moss that flared up, as all the Council [of the wolves] drew back in terror before the leaping flames. Mowgli thrust his dead branch into the fire till the twigs lit and crackled, and whirled it above his head among the cowering wolves. “Thou art the master”, said Bagheera in an undertone.’ (Kipling, 2008 [1894/95], pp. 30-31).

Rudyard Kipling`s founding Mowgli has learned to adapt himself to the laws of the Indian forest. He understood the attitudes of its animal inhabitants, the benefits of using fire and to ally with Great Powers Baloo the bear and Bagheera the panther against his enemy Shere Khan the tiger. Such a Mowgli smart-tool based grand strategy could help the smaller states to influence and to benefit from the international system and to guarantee the single state actor its survival in the wilderness of world jungle.

Bibliography

Baldwin, David A. 2002. Power and International Relations. In: [eds.] Walter Carlsnaes, Thomas Risse and Beth A. Simmons. Handbook of International Relations. Los Angeles et al.: SAGE, 2002.

Bartholomees, J. Boone. 2012. A Survey of the Theory of Strategy. In: [ed.] J. Boone Bartholomees. US Army War College Guide to National Security Issues. Volume I: Theory of War and Strategy. Carlisle, PA: Strategic Studies Institute, 2012.

Berenskoetter, Felix. 2007. Thinking About Power. In: [eds.] Felix Berenskoetter and Michael Williams. *Power in World Politics*. London/New York: Routledge, 2007.

Carlsnaes, Walter. 2007. How Should We Study the Foreign Policies of Small European States? In: *Nação and Defesa*. Autumn/Winter, 2007, Vol. 118, 3.

Elliott, Christopher L. 2015. *High Command. British Military Leadership in the Iraq and Afghanistan Wars*. London: C. Hurst & Co, 2015.

Freedman, Lawrence. 2013. *Strategy. A History*. Oxford: Oxford University Press, 2013.

Gray, Colin S. 1999 a. Inescapable Geography. In: *Journal of Strategic Studies*, June/September 1999, Vol. 22, 2-3.

Gray, Colin S. 1999 b. *Modern Strategy*. Oxford: Oxford University Press, 1999.

Gray, Colin S. 2000. Deterrence in the 21st century. In: *Comparative Strategy*, July/September, 2000, Vol. 19, 3.

Handel, Michael I. 2001 [1992]. *Masters of War. Classic Strategic Thought*. London: Frank Cass, 2001 [3rd edition; first published in 1992].

Holy Bible. 1992. *New International Version*. Colorado Springs et al.: International Bible Society, 1992 [for this print].

Jablonsky, David. 2012. Why is Strategy Difficult? In: [ed.] J. Boone Bartholomees. *US Army War College Guide to National Security Issues. Volume I: Theory of War and Strategy*. Carlisle, PA: Strategic Studies Institute, 2012.

Karsh, Efraim. 2011 [1988]. *Neutrality and Small States*. London/New York: Routledge, 2011 [Reprint; first published 1988].

Keohane, Robert O. 1969. Lilliputians' Dilemmas: Small States in International Politics. In: *International Organization*. March, 1969, Vol. 23, 2.

Keohane, Robert O. and Nye, Joseph S. 2011 [1977]. *Power and Interdependence. World Politics in Transition*. Boston: Longman, 2011 [4th edition; first published in 1977].

Kipling, Rudyard. 2008 [1894/1895]. *The Jungle Books*. Oxford: Oxford University Press, 2008 [Reprint; first published 1894/1895].

Layton, Peter. 2012. The Idea of Grand Strategy. In: *RUSI Journal*. August, 2012, Vol. 157, 4.

Liddell Hart, Basil Henry. 1954 [1941]. *Strategy. The Indirect Approach*. London: Faber & Faber, 1954 [3rd edition; first published in 1941].

Mearsheimer, John J. 2001. *The Tragedy of Great Power Politics*. New York/London: W.W. Norton & Company, 2001.

Melvin, Mungo. 2012. Soldiers, Strategy and Statesmen. In: *RUSI Journal*. February, 2012, Vol. 157, 1.

Molis, Arunas. 2006. The Role and Interests of Small States in Developing European Security and Defence Policy. In: *Baltic Security and Defence Review*. 2006, Vol. 8.

Murray, Williamson. 2011. Thoughts on Grand Strategy. In: [eds.] Williamson Murray, Richard Hart Sinnreich and James Lacy. *The Shaping of Grand Strategy: Policy, Diplomacy and War*. Cambridge: Cambridge University Press, 2011.

Nilsons, Martins. 2015. Can small- and medium-sized states have grand strategies? In: *Ad Securitatem. The best essays written by students at the Baltic Defence College during 2014/15*. Tartu: Baltic Defence College.

Nye, Joseph S. 2004. *Soft Power. The Means of Success in World Politics*. New York: Public Affairs Press, 2004.

Ørvik, Nils. 1973. Defence Against Help – A Strategy for Small States. In: *Survival. Global Politics and Strategy*. September/October, 1973, Vol. 15, 5.

Paret, Peter [ed.]. 1986. *Makers of Modern Strategy from Machiavelli to the Nuclear Age*. Princeton: Princeton University Press, 1986.

Paterson, William E. 1969. Small States in International Politics. In: *Cooperation and Conflict*. March, 1969, Vol. 4, 1.

Paulauskas, Kestutis. 2006. Yesterday Came Suddenly: The Brave New Security Agenda of the Baltic States. In: [eds.] Heli Tiirmaa-Klaar and Tiago Marques. Global Security and Regional Security Challenges: A Baltic Outlook. Tallinn: Tallinn University Press, 2006.

Rostoks, Toms. 2010. Small States, Power, International Change and the Impact of Uncertainty. In: [eds.] Robert Steinmetz and Anders Wivel. Small States in Europe: Challenges and Opportunities. Farnham: Ashgate, 2010.

Sim, Harold. 2007. Is the Concept of Deterrence as a Key Survival Strategy for Small States Fundamentally Flawed? In: Pointer: Journal of the Singapore Armed Forces. Spring 2007, Vol. 33, 2.

Strachan, Hew. 2011. Strategy and Contingency. In: International Affairs. November, 2011, Vol. 87, 6.

Wilkinson, David. 1985. Spykman and Geopolitics. In: [eds.] Ciro E. Zoppo and Charles Zorgbibe. On Geopolitics: Classical and Nuclear. Dordrecht: Martinus Nijhoff Publishers, 1985.

Wilson, Ernest J. Hard Power, Soft Power, Smart Power. In: The Annals of the American Academy of Political and Social Science. March, 2008, Vol. 616, 1.

Wivel, Anders. 2010. From Small State to Smart State: Devising a Strategy for Influence in the European Union. In: [eds.] Robert Steinmetz and Anders Wivel. Small States in Europe: Challenges and Opportunities. Farnham: Ashgate, 2010.

Can it ever be ethical to deliberately kill enemy non-combatants during an armed conflict?

LTC Michael Christensen

Introduction.

This paper is concerned with the intersection between law, ethics and realities on the battlefield as formulated in the Just War Tradition, in relation to deliberately targeting non-combatants. The very notion of targeting non-combatants will in the mind of many immediately trigger a response. I have very unscientifically recently asked a couple of handfuls of my colleagues, if they thought that killing non-combatants in war could be ethically justified. All of them are accomplished academics and officers with operational experience, and all of them replied with and unequivocal *no*. From many of them the answer came as an immediate response almost like a reflex. I must say that their reply confirmed my anticipation and also my own opinion. So is it really that simple? Is it in all cases unethical to target non-combatants in war? This paper will investigate into that and provide nuances to both the question itself and to the before mentioned *no*. It will argue that it indeed is not at all that simple. The paper will show that one can formulate morality arguments for deliberately targeting non-combatants if the conditions are right. But at the same time under the same conditions one could formulate morally founded arguments against targeting non-combatants. This ambiguity reflects quite well the different positions on this very philosophical topic, where accomplished scholars continue the discussion from their respective points of view. By using the relevant key principles of the *Jus in Bello* theory the paper will uncover some of the morality considerations to the key question embedded in the papers title.

Framework and limitations.

Just War tradition builds on knowledge gained over more than two millennia. It is in general best described as condensed knowledge of ethical and morality nature. A number of different sources have fed into this tradition over time, both religious (mostly Christian) and secular, both philosophical work and experiences obtained by waging war, from statecraft and from the development of political theory as well as

international law. Just War thinkers have had a variety of approaches and also viewpoints of what role the tradition should play. Dominantly are the views on statecraft and on ethical issues related to every day life and to waging war. Especially the ethical discourse on waging war has a long and proud tradition of influencing the evolution of the tradition, an evolution that continues today. The Cold War proxy war in Vietnam was a sort of catalyst for new thoughts on the tradition and especially the post Cold War period, where thinking on war distanced itself from the inherent doomsday nature of the weapons of mass destruction of the Cold War, have spawned a number of contributors to the tradition. This paper will not account for the lively development of the tradition, nor all its many great thinkers and the different schools they have spawned. Rather it zooms in on the ethical and morality reasoning related to war. Broadly the tradition branches out in two directions related to war. One is *Jus ad Bellum*, which I would translate into “when is it just to wage war” the other is *Jus in Bello*, that translates into “how we justly wage war”. Both branches a hugely important and offers ethical and morality considerations. The so-called orthodox view describes independency between the two. The *Jus ad Bellum* is in this tradition a strict political matter. In other words, the military has nothing to do with why we go to war, including if it is just or not, regardless of for instance situations where senior members of the military have a political role. As an example of what that entails is, that although a state have initiated an unjust war (for the seven *Jus ad Bellum* just war criteria, see Frowe. 2011, p.50) the soldiers fighting the war carry no specific ethical or morality burden because of it, hence they can still fight justly (pending their conduct of course). Others reject that notion fully and places full responsibility on the soldiers for engaging in an unjust war; hence they are by fighting an unjust war *per se* unjust in their *Jus in Bello* actions (McMahan. 2006). McMahan’s considerations on Just and Unjust Wars will be addressed in this paper. This will further allow and justify focussing primarily on the *Jus in Bello* framework when determining the justness and morality of the conduct of war. The *Jus in Bello* framework rests primarily on four pillars: *non-combatant* versus *combatant*, *discrimination*, *necessity* and *proportionality* and lastly *prisoners of war* and combatants *hors de combat*. The first three pillars relate to this paper and needs to be understood in more detail, hence they will be addressed in order to formulate morality arguments for and against deliberately targeting civilians.

As the essay suggests it is concerned about *non-combatants* as opposed to *combatants*. Others would use the terms *civilians* and *soldiers*. This essay will adopt these two recognized sets of terms and use them as synonyms for each other (similar approach is adopted by James Johnson (Johnson. 1999, pp. 239-240).

In the paper *ethics* and *morality* and *ethical* and *morally* are treated as synonyms.

Relationship between law and ethics

A lawyer once described the law to me as the wall you can play up against in order to find out whether an action was right or wrong. I agree with that notion, however for the full understanding of it, I believe we must addwhether an action was right or wrong *according to the law*. Why this addition? Well, we must remind us selves that the law as it is codified in various states or internationally in protocols and conventions is an attempt to provide a framework that makes sense of numerous individual behavioural patterns and interpretations of situations, leading to a chosen action. It provides us with an understanding of what is right and wrong by providing a yardstick that actions can be measured against. Law is not fixed though; it changes back and forth and evolves serving the end its writers see fit. It is a human construct.

Ethics and morality are something else. It is there regardless of what the law prescribe, as a convention. It simply “is what it is” as McMahan puts it (McMahan 2008, p. 35). This means that although something is permissible by law it can at the same time be morally wrong. In some countries it is legal to slap your child across the face at the same time most people would nowadays find it morally problematic.

Law and morality is nonetheless connected, insofar they influence each other. A great deal of morality consideration is vested in the law and the treaties we abide by when waging war today. Some times that influence is happening in small doses leading to a slow evolution of law and sometimes the influence is quite dramatic leading to a small revolution in the codification of law. Allow me to give an example:

During the Second World War Denmark was invaded and occupied by Germany. The sitting government adopted a policy of corporation with the occupying state in an attempt to minimize and contain the destruction of the state and its citizens. Following the policy of the government and in full compliance with the law, citizens and companies engaged in trade and commerce with the occupying state. Some were very successful in their effort and created substantial societal and economical wealth. After the conclusion of the war and the defeat of the occupying state the situation changed dramatically. Some of the before mentioned citizens and companies were tried and convicted for supporting the occupying state.

What had changed? Not the morality, I would say. Cooperating with the occupying state was throughout the occupation regarded immoral and unethical, but the law serving the end of appeasement, somehow masked its unethical sides. If the unethical masking is in fact the societal and political norms prevailing at a given time, it only naturally follows that a change in those norms will change the masking even up to the point where the masking falls apart all together. I could be argued that was the case in the Danish example. This supports the argument of morality as a convention. Maybe “it is what it is” when it functions, as McMahan suggests; however the Danish example indicates the convention to be volatile and changeable.

Just and Unjust Wars

The modern Just War thinker, Jeff McMahan has forwarded a string of arguments that goes against the orthodox independency view between *Jus Ad Bellum* and the *Jus in Bello* thoughts. The key idea of the orthodox Just War thinkers on combatants is that they are without guilt/responsibility for decisions on waging war. The leadership of their nation’s *Jus ad Bellum* conduct/behaviour does in other words not burden them. So when war commences both opposing parties start with a clean slate and with equal rights. McMahan sees this differently. He argues, that if your country initiates an unjust war its combatants will regardless of their *in Bello* conduct fight unjustly and immorally. Since the end is unjust all actions leading to that end are inherently unjust and immoral. In fact he argues, all citizens, non-combatants as well as combatants have a collective and/or individual responsibility for their

government's unjust initiation of war. The degree of responsibility may well be higher or lower, he admits, however those who contribute in one-way or another to the sustainment of their nation and its war waging ability, have a responsibility. This he argues makes them liable for a morally founded intentional attack in very extreme cases. (McMahan 2009, pp. 221-231). I can follow his argumentation and from a theoretical point of view the causality is intact. As he admits, the practical application of the idea is very limited and I concur with that. Though I do not fully reject his thoughts, I believe we part ways on two accounts. Firstly I am not convinced that the very starting point is right. Though I largely subscribe to the orthodox view regarding the division between *Jus ad Bellum* and *Jus in Bello*, I recognize the notion that being a citizen of a state carries some responsibility and guilt. I just do not see that that responsibility and guilt can be carried through to a war situation and causing civilians to become morally justified targets. Supporters of McMahan's position could then argue that that is why combatants and non-combatants belonging to a state that initiates an unjust war, must actively and persistently stop fighting and stop supporting the state until the unjust actions have stopped. A beautiful idea indeed, but hardly a realistic one, I would say. Secondly, I believe that McMahan does not pay enough attention to the possibility that both sides of a conflict regard themselves as being on morally solid grounds and fighting a just war. Following this logic and McMahan's argumentation both sides could interpret the degree of guilt and liability to find justification for intentionally targeting each other's population, and in doing so, not limit themselves to the very extreme cases that McMahan puts forward. If spinning out of control, a total war scenario that morality and law in the first place should prevent because of its unlimited destruction potential could be the reality. So in conclusion: McMahan's idea of responsibility and guilt in the *Jus ad Bellum* conduct of a nation waging an unjust war to be carried forward into *Jus in Bello* thereby providing argument for the *Jus in Bello* actions to be immoral all together, carries some logic. However that this should entail that non-combatants carry enough responsibility/guilt for the unjust actions to make them morally justified targets, is taking the argument too far. The extreme cases forwarded by McMahan, although being logically sound, opens up for interpretation of the degree of guilt and liability that could be exaggerated. This could lead into an escalation in the deliberate targeting of civilians.

Jus in Bello framework

The *Jus in Bello* tradition draws on considerations that just war theorists have had in relation to defence of your self (self-defence) and defence of others (other-defence) and on how one could morally apply force when waging war. The thinking and the discussions of which many found its way into rules and later on into law served the same purpose, namely to limit the destructions of war. Experiences from especially medieval wars and the wars of the last century have given evidence to unimaginable destruction towards property, soldiers and especially civilians. It is those thoughts and experiences that are put together into the *Jus in Bello* framework. The framework rests on the before mentioned pillars. They are mutually reinforcing and interconnected. They form up a framework designed to provide clarity and guidance when waging war in an attempt to limit the very destructiveness of war. The framework is not a recipe though, however the individual components can serve as steppingstones when deciding if actions are morally permissible (and to some extent legally permissible). The challenge with the steppingstones is that they are questionable. They are not black or white but all shades of grey. The steppingstones being questionable call for answers. When waging wars some of these answers need to be provided fast and decisions need to be taken on the lowest tactical levels up to the strategic levels and in many cases by single individuals. Without the pressure of combat we will look at the morality side and ambiguity of the *Jus in Bello* pillars. (Further on the *Jus in Bello*, see Frowe. 2011, pp. 95-101).

Combatants and non-combatants

Knowing who is a combatant and who is a non-combatant is imperative both from an orthodox just war morally point of view and from a legal one. Common for both are that it is *not* morally and *not* legal to target non-combatants intentionally. In other words without distinguishing between the two we cannot morally or legally determine if a military target is legitimate or not. So what is in fact the difference between being a non-combatant and a combatant? That difference between the two is much debated and the positions on the topic are widespread. From one extreme it is argued that if a

nation wage war, all its subjects are combatants (as argued by Augustine in Frowe. 2011, p. 152), to the other extreme where pacifists argue for a total rejection of the use of force against combatants and non-combatants all together. One could ask, “Why all this discussion, isn’t it clearly defined?” Well maybe so. I would argue that it is when we look at the legal side of the case. According to the Geneva Convention a combatant can only qualify as such by meeting the following four criteria (Frowe 2011, p.101):

- Be a part of a hierarchical Group, with a recognisable chain of command
- Wear a distinctive emblem, which is visible.
- Bear arms openly.
- Adhere to the rules of *Jus in Bello* as laid down in the convention.

The fourth criteria was later rewritten in an additional Protocol to the Geneva convention in order to address the nature in which guerrilla warfare was conducted, where combatants blend into to general population and in doing so does not wear uniform and emblems that clearly makes it possible to distinct them for non-combatants. In such situations when they participate in deployments to engagements in which they will take part as well as the engagement it self, they must bear arms openly and in doing so will maintain their combatant status (Frowe. 2011, p. 102).

That is all fine from a legal point of view, but from a morality point of view there are arguments for defining being a combatant differently. Collective guilt is one argument. It stems as mentioned above from the early thinking of Augustine and basically paints with a broad brush. It claims that the citizens of a country that wage war carries guilt or responsibility, hence there are no morality grounds for distinction between non-combatants and combatants. When this argumentation was formulated ordinary citizens had very little influence on the politics applied by the sitting ruler, who in many states had absolute powers, hence it carries little weight, I believe. It could be argued though that Augustine’s thoughts carry more weight in a modern democratic society where individuals have much more direct influence on who is leading their country and therefore more responsibility for the actions taken. But as I see it there is still no grounds for adopting the argument, because in reality, or in war if you like, there is no way one could distinguish between who voted for the sitting government and who did not.

Hugo Grotius, later formulated the distinction between non-combatants and combatants that Augustine's argumentation lacks. Not only did he formulate his thoughts on a clear distinction between *Jus ad Bellum* and *Jus in Bello* but he also codified the morality distinction between those who belong to armed forces (combatants) and those who do not (non-combatants). His argument to the former was that being a part of an armed force you forfeit the right not to be killed therefore it is both legally and morally just to do so. The right *not* to be killed remains intact for a non-combatant; hence it is morally unjust to kill one. A continuation of Grotius thoughts relates to posing a threat. The initial intention was to even further narrowing down the group of actors that morally could be regarded as combatants so that only those posing a threat are actual combatants. That rationale could also be applied to non-combatants in an argument for broadening that group, hence make the group of morally permissible targets greater. You can trace the thoughts back to the idea of self-defence (for further on self-defence see Frowe. 2011, pp.9-26), that broadly stipulates, that it is morally permissible and just to retaliate on an attack, even up to the point of applying lethal force should the situation call for it (proportionality and necessity criteria applies). So the argument is that by posing a threat it becomes morally permissible to attack even non-combatants. That of course immediately raises the issue of what constitutes a threat and who determines what is a threat. Using an example taken from Stephen Deakin (Deakin.2011), where a patrol behind enemy lines is being spotted by a local goat herder. Fearing that the goat herder will alarm the nearby garrison of their presence, which inevitably will lead to their capture or maybe death, the patrol is facing a morality dilemma or question if you like. Is it given the circumstances morally permissible to kill the herder? If so, then all the civilians the patrol believes to have spotted them could expect to be killed. You could hardly argue that the herder should he in fact alarm the garrison *de facto* becomes a combatant, however it could be argued that his action poses a threat and the severe consequences of it can provide some kind of morality justification for them taking action. As with self-defence the actions could be tailored to the situation, following the principle of proportionality. Currently according to the laws of war, no harm is to be inflicted on non-combatants, so even in our herder example it would be unjust to knock him unconscious. This very definite line is being contested not only morally as above, but also from a legal point of view. A softening, although not allowing killing of non-combatants, is being suggested with the introduction of quite

sophisticated non-lethal weapons (NLW). In our herder example the employment of such a weapon could save the lives of both parties and the action could be standing on a solid legal ground as well as a morality one (further on NLW see Deakin.2011.).

Legitimate targets

Above we determined what a combatant is. By doing so we should then know who could then legally and morally be targeted. That being said there is no precise overlap between a person being identified as a combatant and the person then in the eyes of the law is a legitimate target. Doctors and clergy personnel are examples of combatants that are not legitimate targets. The same goes for combatants *hors de combat*. The idea of those not taking “active” part in the fighting *a la* the *hors de combat* category has spawned a whole array of philosophical and morality thought even further narrowing down the scope of legitimate targets (as an example see Walzer’s example of “The naked soldier” in Walzer. 2006, pp. 138-143). It goes the other way as well as Frowe points out “But even those politicians without military roots or affiliation can be legitimate targets if they are instrumental in the orchestrating of the war” (Frowe. 2011, p. 103). As one can see the lines become more and more blurred. Not only between the two principles of combatant/non-combatant and legitimate targets but also between law and morality. George Mavrodes provides a viewpoint by revisiting the relationship between law and ethics. Basically he argues that the immunity of non-combatants has developed into law on the wrong assumption that it is a morality fact that non-combatants cannot be intentionally targeted. This is significant. It is so because he reminds us that both morality and law are means to limit the damage and deaths caused by war. He offers an argument that kind of sets the morality free from this “damage-minimizing-straightjacket” and thereby he allows us to apply a somewhat more pure look on morality. After all how do we morally distinguish between a farmer that from his land overlook the ocean and who in the time of war reports on enemy ship movements and thereby allows them to be targeted and between the engineer that has developed techniques for making precision ammunition at his factory for his countries army to use in war. Are they not equally involved as the uniformed soldier firing his rifle? I would say that they are involved to such degree that it probably is morally justified to target them.

Frowe mention a number of other just war thinkers that have tried to provide arguments on who is a legitimate target and who is not (Frowe. 2011, pp. 151-158). None of them with much conviction I would say.

Necessity

In armed conflict the application of military force must meet the condition of necessity, which implies that the application has to create a military advantage. Military advantage is somewhat difficult to identify. As an example, I believe that most people see the necessity, legality and morally permissibility of destroying an enemy battle tank charging towards you. Then try and recall Walzer's "Naked soldier" example I referred to earlier. Is it morally permissible to kill the naked soldier taking a bath well away from the battle? Is it necessary? The lines become blurred. If we throw civilians into the equation, maybe even more so. Let us look at a classic example of a weapons factory with a thousand men strong civilian workforce and which production provides a significant contribution to its country's ability to wage war. International law can specify this as a legitimate military target allowing us to blow it up even though we kill a lot of civilians, which is generally regarded as a morally flawed act. They are merely collateral damage. This then constitutes a dilemma between morality and law. To bridge this dilemma the Doctrine of Double Effect (DDE) has been used. Like the principles of necessity and proportionality the Doctrine of Double Effect (DDE) goes way back to thoughts on self-defence (Frowe. 2011, pp. 19-27). The doctrine provides a possible explanation to the morality dilemma we are all too aware of namely that non-combatants are killed in war, even though it is morally impermissible and unlawful to kill them. The DDE basically rests on the notion that there is a distinct ethical difference between a military action that intentionally kills non-combatants and one that kills non-combatants unintentionally. Emphasis is on the *intention*, on the *end* that your actions are to achieve. Put shortly, if you intentionally destroy a legitimate military target, like the factory from before, where some innocent non-combatants happen to be killed, your action is morally permissible. However if your intention were to kill the non-combatants and not destroy the factory, it would be morally impermissible. Going back to the factory example. Lets say that the know how that is behind the production

activities in the factory rests on ten engineers that work in an office environment ten kilometres away from the factory. Since targeting them provides a military advantage similar to that of blowing up the factory, the necessity criterion is met. That the casualty number by bombing the factory could be well above the ten dead engineers can provide a morality argument for choosing that option. In this example I would argue that it can be morally justified to target civilians, because it is a choice between two options both involving civilian casualties. The DDE allegedly provides morally justification in the factory bombing case since it absorbs all the dead civilians as collateral damage because the intention in the first place was *not* to kill them but to destroy the factory. I would argue that this example challenges the actual DDE application to real life situations. The transfer of military necessity first from the factory and then to the engineers opens up for even further transfers, like to the electricity plant supporting the factory, or the water plan etc. etc. This of course, as in the case of defining combatants, holds the potential of spinning out of control and cause more harm than good.

To sum it up, although I am in no way arguing that a decision to target civilians that contribute to the war effort should be taken without careful consideration, including morality considerations, I can find morality arguments for the engineers and workers putting themselves in a position where they forfeit their right “not to be attacked” because they engage directly in the support of the war effort with such significance that it becomes necessary to target and kill them.

Proportionality

The last of the *Jus in Bello* criteria is proportionality. It entails that; “The harm that one inflicts must be proportionate to the good that is protected, and must be the least harmful means available of achieving the good” (Frowe. 2011, p. 107). In other words it aims at controlling the extent of force application in war in order to minimize suffering and destruction. The criteria raise morality questions to military actions like the dropping of the two nuclear bombs in the end of The Second World War. The American rationale was that the bombing was what it would take to get the Japanese to surrender and thereby avoid a prolonged war, that was likely to cost the lives thousands and thousands of American soldiers. So the morality question the

Americans was facing was: “Is it okay to kill Japanese civilian (and some soldiers of course) in order to save our own boys?” Most just war thinkers of course believe that the non-combatant lives counts in the calculation of proportionality (Frowe. 2011, p. 108) and we have previously discussed that civilians have not waived their right not to be killed while most think that soldiers by their very profession have forfeited their right not to be killed. So how can you morally justify the bombings? Well we can’t, can we? Unless of course, we start playing with numbers. Let us say that 200.000 civilians died in the bombing, but the prolonged war was estimated to reach a death toll of 1.000.0000 American and Japanese soldiers and civilians, a 1:5 ratio. So if you set aside the above-mentioned rights, the sheer numbers lays grounds for a morally justification, provided though that the approach is the only solution presenting itself (McMahan.2009, pp. 226-231). I would argue that this was probably not the case. The arguments follow along the ones proposed by McMahan against the decision to drop the bombs (McMahan. 2009, pp. 128-130). I would add further that boiling down attacks against non-combatants in order to save combatants as a mathematical 1:1 ratio for finding morally justification is based on shaky grounds, giving the very difference between the two as argued previously. On the other hand I expect that it would be morally accepted by most that one single non-combatant could be killed if it saves 5000 combatants in an imaginable scenario. So proportions matter (for further on this see Walzer. 2006, pp. 263-268). This kind of rationale ties into the thoughts on Supreme Emergency, where the consequences of not acting are unimaginable – even more unthinkable than what one proposes to do (Frowe. 2011, p. 97). A rationale I would argue builds on self-defence rights and thoughts, just blown up in scale (see Walzer. 2006, pp. 251-262).

Conclusion

I believe that I have put forward morality arguments for adopting a broader understanding of who can be legitimately targeted up to the point that there are arguments for deliberately killing civilians, like the farmer spotting ships or the herder telling on the patrol. This argumentation is along the lines of what I have seen referred to as the “Boxing Match” model. If you enter the ring you can expect to be hit by your opponent. The ring in this argumentation is not a geographically outlined

area, but is to be regarded in a broader action related context, where ones actions contribute directly to the war effort (McMahan.2009, pp.51-57). Actions the civilians take are key I believe if we are to establishing understanding on the morally permissibility for killing them. Just being citizens in a war waging country does not quite justify for them loosing their right *not* to be killed, although it might flaw their innocence. This line of arguments are linked to being combatant or non-combatant Regarding being a legitimate target, George Mavrodes have put forward strong arguments that could open up for a greater morally acceptance of targeting the civilian elements of the war effort even though they have a more distant and less decisive part to play in the war effort. After all how decisive is an individual rifleman's contribution?

Mavrodes argumentation ties into the necessity discussion where we saw that law and morality in the factory example provide a weak causal argument and link between the two. The DDE are not fully bridging the two and providing strong morality justification with its single focus on intent, although I admit that the DDE can serve a purpose as a sort of morality compass in its pure form.

I have found no strong arguments for deliberately killing non-combatants from the principle of proportionality except maybe in cases of Supreme Emergency. Here the case of the nuclear bombing showed as was the case with other principles that number matters, at least insofar that they can strengthen or weaken the morality argumentation.

So to sum it up, I cannot say with any rock solid causal argumentation that we should never deliberately kill civilians in armed conflict. In fact I have provided some logically linked arguments that could morally explain or even justify that we intentionally kill civilians. However, I do have a sincere doubt about the arguments, since they are so intimately linked to someone's subjective judgement, perception and interpretation of fundamental components in the arguments, like threat, necessity, proportionality numbers, guilt and involvement. This is I suppose a fundamental problem with ethics in general. The doubt leads me to conclude that although we isolated can find causal morally justifiable arguments for deliberately killing civilians in armed conflict we need it to remain illegal. The reason for this follows the above mentioned subjective element, leading to a fear of opening up Pandora's Box and that the targeting of civilians will spin out of control. The ingrown retaliatory dynamics of war provides strong arguments for that this will indeed happen.

Select biography

UN Security Council Resolution 1674 [Online] [Cited: 01 April 2016.]

<http://www.un.org/press/en/2006/sc8710.doc.htm>

Deakin, Stephen. 2014. Naked Soldiers and the Principle of Discrimination.

Journal of Military Ethics, 2014 Vol. 13, No. 4. [Online] [Cited: 04 May 2016.]

<http://www.tandfonline.com/doi/full/10.1080/15027570.2014.991507>

Chan, David K. 2012. Just war, non-combatant immunity, and the concept of Supreme Emergency. *Journal of Military Ethics*, 2012 Vol. 11, No. 4. [Online] [Cited: 04 May 2016.]

<http://www.tandfonline.com/doi/full/10.1080/15027570.2012.758399>

Deakin, Stephen. 2011. Wise men and Shepards: A case for taking non-lethal action against civilians who discover hiding soldiers. *Journal of Military Ethics*, 2011 Vol. 10, No. 2. [Online] [Cited: 04 May 2016.]

<http://www.tandfonline.com/doi/full/10.1080/15027570.2011.593713>

Gade, Emily Kalah. 2010. Defining the Non-Combatant: How do we Determine Who is Worthy of Protection in Violent Conflict? *Journal of Military Ethics*, 2010 Vol. 9, No. 3. [Online] [Cited: 04 May 2016.]

<http://www.tandfonline.com/doi/full/10.1080/15027570.2010.510863>

Just and Unjust Killing. [Online] [Cited: 04 May 2016.]

<http://www.tandfonline.com/doi/full/10.1080/15027570802573203>

Mavrodes, George. 1975. Conventions and the Morality of War. *Philosophy and Public Affairs*, 1975 Vol. 4, No. 3. 1975, pp. 117-131. [Online] [Cited: 01 May 2016.]

<http://www.sps.sdu.edu.cn/sps60/cms/attachment/080528093246.pdf>

McMahan, Jeff. 2006. *On the Moral Equality of combatants*. [Online] [Cited: 04 May 2016.]

http://philosophy.rutgers.edu/joomlatools-files/docman-files/Moral_Equality_of_Combatants.pdf

Mayer, Chris. 2007. Nonlethal Weapons and Noncombatant Immunity: Is it Permissible to Target Noncombatants? *Journal of Military Ethics*, 2007 Vol. 6, No. 3. [Online] [Cited: 04 May 2016.]

<http://www.tandfonline.com/doi/full/10.1080/15027570701539552>

Coleman, Stephen. 2013. *Military Ethics: An Introduction with Case Studies*. Oxford: Oxford University Press, 2013. pp. 148-161.

Downes, Alexander B. 2008. *Targeting Civilians in War*. Ithaca: Cornell University Press, 2008.

Frowe, Helen. 2011. *The Ethics of War and Peace: An Introduction*. London: Routledge, 2011.

Frowe, Helen. 2011. Self-defence and the Principle of Non-Combatant Immunity. *Journal of Moral Philosophy*. 2011, Vol. 8, 4. [Online] [Cited: 01 April 2016.] [[Link](#)]

Frowe, Helen. 2014. Non-Combatant Liability in War. [eds.] Helen Frowe and Gerald Lang. *How We Fight: Ethics in War*. Oxford: Oxford University Press, 2014.

Hartle, Anthony E. 2004. *Moral Issues in Military Decision Making*. Lawrence, Kansas: University Press of Kansas, 2004. pp. 149-180.

Kaldor, Mary. 1998. *New and Old Wars, Organized Violence in a Global Era*. Cambridge: Polity Press.

Mckeogh, Colm. 2002. *Innocent Civilians, the Morality of Killing in War*. Palgrave Macmillan, 2002.

McMahan, Jeff. 2008. *The Morality of War and the Law of War*, in David Rodinand Henry Shue (eds), *Just and Unjust Warriors*. Oxford: Oxford University Press, 2008.

McMahan, Jeff. 2009. *Killing in War*. Oxford: Oxford University Press, 2009.

Murphy, Jeffrie G. 1986. Killing of the Innocent. [Ed.] Malham M. Wakin. *War, Morality and the Military Profession*. Boulder, Colorado: Westview Press, 1986, pp. 341-364.

Turner Johnson, James. 1999. *Morality and Contemporary Warfare*. New Haven, Massachusetts: Yale University Press, 1999, pp. 119-158.

Walzer, Michael. 2006. *Just and Unjust Wars*. New York City, New York: Basic Books, 2006, pp. 138-175.

Can the forward deployment of armed forces extend and entrench regional security?

Mr Karolis Aleksa

Introduction

History leaves no doubt on the importance of the forward bases to the great powers' foreign policy. Up to the beginning of the World War II forward bases were acquired through colonization and conquest (Harkavy, 2007, p. 92) and used by great powers for a variety of purposes, mainly to protect economic interests, conquest new territories, control and extend colonies and compete against each other. Therefore, it was hard to expect they could serve well to ensure regional security by preventing security dilemmas in the region to turn into the military conflicts.

The period after the World War II was marked by several important changes in respect to the role of forward bases to regional security. Firstly, U.S. has taken a global lead to confront expansion of Soviet influence in the regions outside of the Soviet control. Secondly, U.S. was given an access by different countries to establish or maintain forward bases in order to deter communist military aggression (Krepinevich, Work, 2007, p. 105). Thirdly, a communist attack on U.S. forward base could trigger a U.S. nuclear response, escalating into nuclear strikes' exchanges. That has built a basis for an extended deterrence during the Cold War period.

Despite the fact that the U.S. was successful in deterring the communist military aggression against its allies and partners during Cold War time, a question of credibility of extended deterrence was always present. For example, a search for credible deterrence against Soviets during the decades of Cold War has shifted NATO strategy focus from nuclear towards more conventional deterrence (Huntington, 1983/84, p. 32). Thus, it can be argued that a question of deterrence credibility is a key in understanding if the forward deployed armed forces can extend and entrench regional security. It means that forward deployed forces may contribute to regional security if they can achieve their task, which is defined by a particular strategy of deterrence, and are in the right mixture with other important elements of deterrence. However, the challenge in the third decade of the post-Cold War era to ensure a credible deterrence seems no smaller than in the Cold War, especially as the great

powers, including U.S., are unwilling to contemplate nuclear escalation strategy when they are not directly threatened by nuclear weapons (Morgan, Paul, 2009, p. 259, 264-265). Such change has put a huge pressure on the conventional side of deterrence and specifically on the forward deployed forces.

In order to examine the statement that forward deployed armed forces can extend and entrench regional security two cases will be explored: U.S. against China in the East China Sea and NATO against Russia in the Baltics. Both cases have been chosen because of recent Russia and China's assertiveness and aggressiveness, which in response requires credible deterrence. Conventional deterrence theory will serve as a theoretical background for an analysis by providing variables, which will help to illustrate the most important aspects of two case studies.

1. Conventional deterrence and forward deployed armed forces

Deterrence theory offers one of the best available theoretical frameworks to explain the relationship between forward deployed armed forces and regional security as it explores the impact of conventional and nuclear weapons role in ensuring different layers of security (national, regional and global). Since forward deployed forces are generally represented by conventional forces (with few exceptions), the conventional deterrence theory will be used to provide a theoretical background.

Deterrence is a strategy to convince an opponent to abstain from an action he was probably planning to take (Gray, 2003, p. 13; Freedman, 2004, p. 26). As it is evident, deterrence is a relationship between the deterrer and the deteree, however, the success or failure of deterrence depends largely on the latter. Nonetheless, the deterrer in his disposition has a set of measures, which can lead a deterrence strategy to success. Both conventional and nuclear deterrence theories agree that this set includes political will, capabilities and communication. Political will usually reflects the importance of national interest: the more important national interest is at stake, the stronger political will is expected to appear to defend it. For example, security of free democratic world was at the heart of U.S. national interests during the Cold War, therefore, U.S. had a strong political will to defend it against the Soviets. A rock solid political will gives a straight way to build necessary capabilities against opponent but

the main challenge is to choose a strategy of using the armed forces for the deterrence. Based on the planned role for the armed forces, conventional deterrence theory proposes two different strategies: deterrence by denial (defeat) and deterrence by punishment. The former strategy is centered on denying the opponent to achieve a quick military victory and other objectives related to military offensive. Such a strategy may succeed because an opponent will probably try to avoid long exhausting conflict, which in the end offers little opportunity to achieve goals associated with military offensive (Mearsheimer, 1985, p. 158; Gerson, 2009, p. 37). Deterrence by punishment strategy puts emphasis on retaliatory actions in the event of opponent's military intervention. Retaliatory actions may directed to seize the territory of invader or to strike invader's forces and/or military infrastructure with the long-range conventional capabilities (Guertner, 1992, p. 9; Gerson, 2009, p. 32). In addition to these strategies, Samuel Huntington points to the third possible course of action, which requires to place some forces against the opponent in order to increase uncertainty and possible costs of invasion (Huntington, 1983/84, 35-36). This strategy falls short of denying opponent's objectives so it can hardly be considered as a real alternative to strategies of denial and punishment. Implementation of these strategies largely falls on the forward deployed armed forces when the deterrer has no land (and maritime) border with the deteree. The choosing of conventional deterrence strategy is influenced by the existing local military balance. When forward deployed armed forces of the deterrer is clearly inferior in numbers against the armed forces of deteree, the former is more likely to pick the strategy of punishment. Nevertheless, even a big advantage in numbers does not guarantee a quick victory for the deteree because the deterrer may be able to reinforce rapidly his forward deployed forces, and his forces may be qualitatively superior. However, historical experience shows that even superior forces of deterrer can not ensure the success of conventional deterrence (Betts, 1985, p. 155, p. 167-169; Huntington, 1983/84, p. 38). Such seeming instability of conventional deterrence can be partly addressed by well-designed and implemented communication. Communication is much more important in the conventional deterrence than in nuclear deterrence because in the case of the later the nuclear weapons speak for themselves: every decision-maker understands the destructiveness of the nuclear strikes. In case of conventional deterrence, communication has to include a verbal messaging of commitment to a particular conventional deterrence strategy as well as to demonstrate capacity to implement it

by conducting military exercises (Stone, 2012, p. 116-117). In addition to the described three very important elements of conventional deterrence, one has to include a role of an ally. When the forward deployed forces are located in the territory of an ally, the latter's strong contribution in sharing the burden will have an impact for developing and maintaining a more effective deterrence (Guertner, 1992, p. 6-7). If the deterrer is attentive to all important elements for conventional deterrence, it can expect it to be a credible one.

On the other hand, that does not mean a credible deterrence will be a successful in the end. It is the deteree who decides to take or not to take an action. While the deterrer may think the deteree has to act rationally as confronted against credible deterrence, however, the national interests, beliefs, strategic culture of the deteree may dictate it to act differently, but not without a reason (Gray, 2003, p. 21; Freedman, 2004, p. 49). Also, military doctrine and military planning of the deteree may tempt the latter to conduct offensive military campaign. For example, Soviet military planning against allies in Europe was based on the offensive scenario, so inevitably it added an uncertainty to the belief that conventional deterrence will survive (Huntington, 1983/84, p. 43; Mearsheimer, 1985, p. 158). Both factors can reinforce each other: if the deteree believes the window of opportunity is closing to achieve its vital national interest, and it has an offensive military doctrine in place, then it is a much bigger possibility to experience a failure of conventional deterrence.

The elements of conventional deterrence, which were recently described, form a theoretical background to start analysis of the two case studies. Specifically, in the analysis of deterrer side (U.S./NATO), the variables of political will, national interest, capabilities (forward deployed armed forces), communication and burden sharing with an ally/allies will be explored. On the deteree side (China and Russia), political will, national interest and military doctrine have been chosen as the variables.

2. U.S. versus China in the East China Sea

The analysis of U.S. and China deterrence relationship in the East China Sea, centered on the Senkaku/Diaoyu islands, offers a possibility to explore a pressing security issue. It can be argued that if China will decide in the future to test the U.S.

deterrence, it will focus on the Senkaku/Diaoyu islands. There is a less probability of U.S. direct military involvement in the South China Sea because U.S. is not prepared to guarantee extended deterrence for its allies and partners on the basis of contested waters. Taiwan's scenario, which is usually a favourite in exploring the U.S. and China deterrence relationship, seems also less relevant as the U.S. is not opposed to a peaceful reunification of both China's, especially if it is based on independent Taiwan's decision.

2.1. China as a potential aggressor

Territorial integrity is one of the most important national interests of China as it believes that some territories (for example, Taiwan, Senkaku/Diaoyu islands) belong to China. Chinese government's White Paper on Diaoyu islands claims these islands to be an ancient Chinese territory at least since the XIV-XV centuries, which only in the end of XIX century were conquered by Japan. In addition, White Paper calls Japanese administration of these islands illegal and leaves no doubt that China is determined to bring them back under its control (Information Office of the State Council of the People's Republic of China, 2012). China's Ministry of Foreign Affairs on a case-by-case basis emphasizes China's rights to the Senkaku/Diaoyu islands, and mentions China's determination to solve this issue peacefully (Embassy of the People's Republic of China in the Republic of South Africa, 2012). China demonstrates a strong political will to protect its national interest related to the Senkaku/Diaoyu islands. Since 2012 China's coast guard and fishery-law enforcement ships regularly and in confrontation with the Japanese vessels have been entering the Senkaku/Diaoyu waters, which is a sovereign Japanese territory (Department of Defense, United States of America, 2015). Moreover, China has established Air Defence Identification Zone in the East China Sea, claiming control of the airspace over the Senkaku/Diaoyu islands.

China's recent military strategy reflects an increased importance of the maritime dimension. It declares that Chinese navy tasks in the nearest future will expand to include the protection of open seas (USNI News, 2015). In fact, the core of Chinese military planning is directed to prepare for the military conflict in the maritime domain. While increasing its assertiveness in the maritime domain, China confirms

its adherence to the strategic defence concept, which includes concepts of operational and tactical offense. According to the China's military strategy (which in fact keeps consistency in the post-Cold War period), Chinese military forces must be able to win local wars. Therefore, it can be argued that such military planning philosophy is deeply permeated by offensive ideas (Solomon, 2013, p. 122-123). China's impressive modernization of naval capabilities in the post-Cold War time has already provided some power projection capabilities in the maritime domain (Huxley and Schreer, 2015, p. 128-129). For example, it is estimated that China already may be capable of executing amphibious operations on a smaller scale, which may allow it to seize control of small islands (O'Rourke, 2016, p. 38). Moreover, since 2013 China is building a military facility in the Nanji island, which is only a 300 km away from the Senkaku/Diayou islands. There is an evidence that such a military base will host the Chinese helicopters with anti-submarine warfare capabilities, and also may host a rapid reaction force in the nearest future (Wood, 2015; Keck, 2015). Such Chinese actions only deepen uncertainty concerning the Chinese publicly stated commitment to solve the Senkaku/Diayou islands issue peacefully.

2.2. U.S. as a provider of extended deterrence to Japan

U.S. has the long standing political, security and economic interests in the Asia-Pacific region. They are best embodied in the U.S. policy to ensure its access to Asian market and prevent the rise of regional hegemon (Castro, 1994, p. 343-344). The emergence of democratic regimes during the Cold War in some parts of Asia-Pacific has added a normative aspect to the U.S. interests as well: for example, U.S. was even more committed to ensure the defence of Taiwan as the later transformed into the democratic regime. U.S. political and security interests in the region are mainly protected by the bilateral alliances and partnerships with Japan, South Korea, Australia, Philippines, Thailand and other countries in the region. An alliance with Japan is the most important, therefore, the U.S. is deeply committed to contribute in ensuring the security of Japan. In the context of increasing confrontation between Japan and China over the Senkaku/Diayou islands, the U.S. openly and clearly expressed recognition the Senkaku/Diayou islands being a part of Japanese territory. Also, the U.S. has declared it will confront any unilateral move to change the current administration of these islands (Asia-Pacific Maritime Security Strategy, 2015, p. 6).

U.S. determination to defend Japan is also reflected in the renewed U.S.-Japan defence guidelines, which shows a formal U.S. commitment together with Japan oppose any attack against the later (The Guidelines for Japan-U.S. Defence Cooperation, 2015).

The developments of Chinese military capabilities and the nature of its military doctrine give an idea that one of the most likely scenario, which could be chosen by China in the East China Sea, is a surprise attack on the Senkaku/Diayou islands, expecting to achieve a *fait accompli* by establishing its control over these islands. Such scenario drives the U.S. to lean towards the conventional deterrence strategy of denial. Forward deployed armed forces have a special role in the implementation of this strategy. In fact, forward deployed armed forces of the U.S. in Asia-Pacific had been playing a significant role against the Soviets and its allies since the early years of the Cold War (Jackson, 1987, p. 67-68), so today for the U.S. is a challenge to adjust its forward posture in facing a new threat (Erickson and Mikolay, 2006, p. 72).

Based on the assumption that the first U.S. reaction to a potential China's aggression against the Senkaku/Diayou islands would mainly come from the forward deployed forces in Okinawa (Japan) and Guam (U.S. territory), it is necessary to take a glance at these forces in particular. U.S. forward based forces in Japan are quite large (about 53000 soldiers) and Guam hosts approximately 6000 U.S. soldiers (Kan, 2014, p. 1; Chanlet-Avery and Rinehart, 2016). More than one third of the U.S. forward based force in Japan is represented by the U.S. Marine Corps, which is basically a rapid reaction force. Even though the U.S. Marine Corps and other U.S. forces in Japan would probably be involved in the hostilities centered on Taiwan and North Korea as well, nevertheless they appear as a big force, which is capable to counteract a potential Chinese aggression against the Senkaku/Diayou islands. A scenario of a surprise Chinese attack requires enhanced maritime surveillance capabilities. By deploying or planning to deploy the most modern platforms such as P8A maritime surveillance aircrafts and MQ-4C unmanned aerial system the U.S. will lessen the risk of facing a surprise in the Western Pacific (Asia-Pacific Maritime Security Strategy, 2015, p. 21). A strong U.S. naval presence nearby the Senkaku/Diayou islands is also required in order not to allow China to secure naval area before an attack. In general the U.S. plans to increase its naval presence in the Pacific theater by 30 percent till year 2020. The U.S. has already replaced aircraft carrier George Washington with a

more modern aircraft carrier Ronald Reagan, which is ported in Japan, and deployed an additional attack submarine in Guam base. Also, the U.S. plans to deploy in Japan two additional Aegis-capable destroyers by 2017, and three DDG-1000 destroyers later (LaGrone, 2014; Sisk 2016). The third set of capabilities that the U.S. needs to counter the potential contingency are related to rapid reaction. These capabilities will be strengthened as the U.S. will deploy a number of tilt rotor aircrafts and the most modern amphibious assault ship in Japan by 2020-2021, and a Joint high speed vessel in Guam base by the end of 2018 (Asia-Pacific Maritime Security Strategy, 2015, p. 20).

Japan's role in deterring China, and if deterrence fails, in defending its own territory is very important for the U.S. However, since the new defence guidelines were signed in 2015 it is not only about burden sharing in defending Japan. Japan has made a huge shift in its policy by committing to participate in defending the U.S. as well if an armed attack against the later occurs (The Guidelines for Japan-U.S. Defence Cooperation, 2015). This is a very powerful message to the U.S., showing Japan's will to share burden in defending the U.S. On its part, Japan is implementing a set of measures, which are directed to enhance defence of Senkaku/Diayou islands. These include increasing surveillance capabilities in the areas around Senkaku/Diayou (a radar station in Yonaguni island), creation of amphibious rapid reaction brigade and adding a new fighter squadron to defend airspace over Senkaku/Diayou islands. Moreover, Japan declared its military concept on how it will deter an attack on its islands, and if the deterrence will fail, how it will recapture them (Defence of Japan, 2015, p. 227-228). It is also important to mention that Japan will share the costs of relocating 5000 U.S. marines from Okinawa to Guam base. A relocation move, even if triggered by Okinawa population, will make the U.S. forward posture in the Western Pacific more flexible, dispersed and so probably add more credibility to deterrence (Chanlet-Avery and Rinehart, 2016, p. 1).

It is no surprise that Japan being a very important ally, the U.S. is not failing to communicate to China its will to defend Japan. U.S. president Barack Obama and his state and defence secretaries regularly expressed U.S. position to defend Japan's territory, including the Senkaku/Diayou islands (The Washington Post, 2014; Kan, 2014, p. 19). Joint U.S. and Japan's military exercises, especially focused on different

amphibious operations (for example, Iron Fist 2016), add power to a regular verbal communication (Fuentes, 2016).

2.3. Preliminary insights: U.S. forward deployed forces and security in the East China Sea

U.S. forward deployed forces in Japan, Guam make a strong contribution in deterring a potential Chinese attack on the Japanese administered Senkaku/Diayou islands. The U.S. abstain from strengthening the forward posture in the context of ongoing rapid China's military modernization, its activities in the East China Sea could convince China to attack the Senkaku/Diayou islands. On the other hand, while the U.S. forward deployed forces is a very important element to the deterrence strategy against China, alone it cannot bring credibility to this strategy. Other elements such as U.S. national interest, political will, communication and burden sharing with Japan in concert with the forward deployed forces give such credibility to conventional deterrence strategy, and thus enhance regional security.

3. NATO versus Russia in the Baltics

Nowadays there are only a few analysts, who disregard a potential Russian threat to the NATO's eastern flank, especially the Baltic countries. Also, many security and defence experts would agree that the U.S. role in developing the NATO answer to Russian threat is a crucial one, an understanding based on the major U.S. role in the Alliance and its forward military posture in Europe. Therefore, this case study will be limited to include only Baltic countries from eastern NATO flank, and there will be a focus on both NATO and U.S. response to Russia.

3.1. Russia as a potential aggressor

Russia was never satisfied with the NATO expansion into the Baltic states, though, even if uneasy, it has accepted that as an unavoidable process (Kramer, 2002, p. 16-17). Nonetheless, Russia has been questioning the legality of Baltic states' existence for several recent years. For example, Lithuanian authorities started to receive official Russian requests to prosecute Lithuanians who refused to serve in the Soviet army

after Lithuania has declared its independence in 1990 (Molin, 2014). Such trend is also reflected by the request of two Russian parliamentarians submitted to Russian General Prosecutor's Office to investigate if recognition of Baltic states' was legal (BBC, 2015). Another trend, which is worrying Baltic countries, is Russia's chosen policy to protect its citizens and ethnic Russians living abroad by force (The Washington Post, 2014). This policy has been used by Russia to justify its military interventions in Georgia and Ukraine. In addition to these developments, Russia harshly criticizes the U.S. and NATO military activities near its borders, and seeks to undermine their role in ensuring security of Europe. Therefore, a strong Russian political will to change the status quo in its neighbourhood, if needed, by force presents a big challenge specifically to the Baltic countries, and NATO in general.

Russian military doctrine leaves no doubt that U.S. and NATO represent the main military risks. However, it does not present the modus operandi of Russian armed forces against potential opponents, except that Russia may use nuclear weapons in defending itself against devastating conventional attack (The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland, 2014). The Russian approach to war is better represented by the so-called Gerasimov doctrine, which proposes to combine nonmilitary and military measures to wage a war (Bartles, 2016, p. 34). Military exercises Zapad and other snap exercises show a real face of potential Russian military measures. For instance, in the exercises Zapad 2009 and Zapad 2013 Russia played offensive scenarios against the Baltic countries and Poland, preparing to conduct large scale combined arms operations and use a tactical nuclear weapon (The Jamestown Foundation, 2015, p. 5-7; Van Herpen, 2011). Recently Russia has enhanced its capacity to implement such scenarios, for example by establishing a helicopter base near the border of Latvia, recreating the 1st tank army in the Western military district and strengthening A2/AD capabilities around Kaliningrad district (Sputnik News, 2014; Novichkov, 2016). In principle, that gives an evidence of Russian preparation to invade the Baltic countries.

3.2. NATO as a deterrent

NATO is a cornerstone of the European and transatlantic security, providing collective defence guarantees to its members. For this reason every member of an

Alliance has a national interest to preserve it. The future of the Alliance much depends on the U.S., which is a global power and the strongest NATO country. Since the end of the World War II the U.S. has been giving no reason to doubt its commitment to the security of Europe. In the context of Russian military aggression against Ukraine the U.S. repeated its adherence to Article 5 of Washington Treaty and declared its determination to strengthen alliance with Europe (The White House, 2015, p. 25). Moreover, before the NATO Wales summit the U.S. President Barack Obama in his Tallinn speech said that defending Estonia, Latvia and Lithuania is no less important than to defend Germany, France or United Kingdom (The White House, 2014). The U.S. decisions in April 2014 to strengthen the NATO's Baltic Air Policing mission by sending fighters jets and by deploying an army company on a rotational basis in each Baltic country was a prove of the U.S. interest in the security of its Baltic allies. In addition, NATO agreed to strengthen security of its allies in the eastern flank by approving assurance and adaptation measures, which include increased military presence in the eastern part of Alliance, enhancement of NATO Response Force and creation of new Allied rapid reaction force (NATO, 2014). As part of the assurance measures NATO has continuously deployed company-size military units in the Baltic countries alongside the U.S. army companies (NATO, 2015).

Russian military thinking permits to expect a scenario of Russian military intervention to complete an occupation of the Baltic countries, thus forcing the NATO to face a *fait accompli* situation (Colby and Solomon, 2015, p. 22-24; Stoicescu and Praks, 2016, p. 23-24). There is an ongoing debate regarding the strategy of conventional deterrence to be applied to counter such a scenario. Theory of conventional deterrence argues that combination of strategies of denial and punishment make a conventional deterrence stronger (Gerson, 2009, p. 37). Even if it is so, the current discussions among the NATO allies show that the strategy of denial will be a basis to confront a potential scenario. In the implementation of this strategy there will be important two elements: forward deployed forces in the Baltic countries and the planned reinforcement of these forces in case of war with Russia from the territory of other NATO countries. A perfect interplay of both elements would deny a Russian military operation to overrun the Baltic countries. In this case the role of the forward deployed forces is even more important as a big part of reinforcements will most likely arrive from other forward deployed U.S. forces in Europe. In

strengthening forward military presence in the eastern NATO flank, the U.S. has decided to continuously rotate an armored brigade since 2017 in addition to two brigades, which are located in Europe. Also, U.S. plans to expand prepositioning of equipment in eastern NATO allies in 2017, which would allow to reinforce the forward deployed U.S. forces in the Baltic and other eastern NATO allies more quickly in case of Russian invasion. Land component will be supplemented by the U.S. naval presence in the Baltic Sea and by increased capabilities of intelligence, surveillance and reconnaissance (Office of the Under Secretary of Defense, 2016). It is highly possible, if not certain yet, that the U.S. land component in the Baltic countries will become a part of NATO battalion-size military unit to be deployed in each Baltic country after the decisions at the NATO Warsaw summit (Holehouse, 2016). NATO has been planning that forward deployed forces in the Baltic countries and other NATO members in the east will be supported by three multinational brigade-size military units coming from the Very High Readiness Joint Task Force (VJTF) and NATO Response Force (SHAPE, 2016). Later, as defence operation of the Baltic countries evolves, more follow-on forces may come to support. It seems that the U.S. and NATO decisions in the nearest future may increase the forward deployed force in the Baltic countries and Poland up to 2 brigades, which is in the line with the proposals from different think tanks (Hicks and Conley, 2016, p. 12; Stoicescu and Praks, 2016, p. 27-31). There is a believe that such forward deployed forces supported by rapid reaction and follow-on force may deny a quick Russian military victory.

Baltic states appear committed to do whatever it takes in sharing a burden with their NATO allies. With Estonia already spending slightly more than 2 percent of GDP, Latvia and Lithuania plan to reach target of 2 percent by 2018-2020. For example, Lithuania has already more than doubled its defence spending in real terms since 2013 (Caffrey, 2015). In order to complete manning of its military units and increase a depleted reserve force, Lithuania has reinstalled a conscription. Moreover, Lithuania established the second army brigade in 2016, which will become fully operational in early 2020s (Ministry of National Defence of the Republic of Lithuania, 2015). Baltic countries are also increasing their warfighting capacity by speeding up acquisition of infantry fighting vehicles, self-propelled artillery, anti-tank and short-range air defence systems. Furthermore, Baltic states provide a host nation support in relation to NATO Baltic Air Policing mission, prepositioning of U.S.

military equipment, functioning of the NATO Force Integration Units and military exercises with NATO allies.

There is no doubt that the communication from the U.S. and NATO to Russia regarding the defence of the Baltic countries is very strong. One can find a powerful wording from the high U.S. officials, including U.S. president, and NATO foreign and defence ministers. On another hand, NATO and the U.S. has increased the size and frequency of military exercises in the Baltic countries and Poland (The Guardian, 2015). In addition, the large-scale military exercises are started to be executed in the region by the U.S. such as Anakonda 2016 in Poland, which is a clear warning to Russia.

3.3. Preliminary insights: NATO and U.S. forward deployed forces and security of the Baltic countries

Forward deployed forces of U.S. and other NATO allies in the Baltic countries play a very significant role in deterring Russia. Even now, still waiting for the decisions to reinforce forward deployment of NATO forces in the Baltic countries, it is hard to imagine Russian military intervention in the Baltics as the military units of U.S. and other NATO allies continuously rotate in the Baltics. Also, other elements of deterrence are perfectly in place: a political will of U.S. and NATO to defend Baltic allies is strong, being well-communicated to Russia, and Baltic countries put a huge effort to lessen the costs to the U.S. and other NATO allies associated with their military presence in the Baltics.

Conclusions

China and Russia are two regional powers, which are working against the status quo in the regions of East China Sea and Eastern Europe respectively. At first instance it seems that China's challenge to the security of East China Sea is more dangerous than Russia's to the security of the Baltic countries. China believes the Senkaku/Diayou islands to be a part of its territory and is pushing military to prepare for reinstalling Chinese control of these islands meanwhile Russia does not claim Baltic countries to be a part of Russian territory. On another hand Russia seeks to change the security

architecture of Europe, and the Baltic countries may provide a perfect pretext. Russian opportunism, reflected in eastern Ukraine and Syria, shows that such a scenario could be the case.

Security in the East China Sea and Eastern Europe largely depends on the efforts to deter China and Russia from their potential actions. Only a credible deterrence can provide a higher prospect to succeed in preventing Chinese and Russian military interventions. In both cases the deterrer (NATO and/or U.S.) leaves no doubt he has a vital interest and a strong political will to ensure security of Senkaku/Diayou islands and/or the Baltic countries. Also, the deterrer is making a great effort to communicate to the potential aggressor the seriousness of his commitment to deterrence. Forward deployed armed forces are given a big role to complete the build-up of credible deterrence. Analysis of both cases reveals the ongoing strengthening of forward deployed armed forces, which are tasked to deny possibility of quick Chinese and Russian military victories. There is a hard discussion regarding the size of forward deployed armed forces, especially in the Baltic and other eastern NATO allies. However, having a historic experience of conventional deterrence failures even with strong defences, the deterrer has at least to avoid deploying too weak forward forces, which may provide an incentive to exploit opportunity. Analysis of current forward deployed forces postures and the plans to strengthen them show the deterrer will not make such a mistake. In addition, the rapid reaction and follow-on forces greatly enhance a chance to deny execution of potential Chinese and Russian military operation. On another hand, NATO and/or U.S. has to continuously evaluate the situation on the ground, taking into the account changes in the local military balance, military modernization of Russian and Chinese forces, and evolving beliefs of these countries, which may require to adapt the posture of forward deployed forces. Deep commitment from allies (Baltic countries, Japan) to share the burden of deterrence significantly eases the change in forward posture, and so contributes to credible deterrence.

Finally, based on the analysis of two cases, it can be concluded that the forward deployed armed forces play a very significant role in preventing regional conflicts. Even in case of deterrence failure, the forward deployed armed forces would be one of the essential instruments to restore regional security by defeating an opponent and

helping to build a new deterrence. Nonetheless, the credibility of deterrence depends only on a right balance between the forward deployed armed forces and other elements of deterrence such as a political will, communication and a burden-sharing with allies.

Bibliography

Asia-Pacific Maritime Security Strategy. 2015. The Asia-Pacific Maritime Security Strategy: Achieving U.S. National Security Objectives in a Changing Environment. [Online]. [Cited: 27 April 2016.] http://www.defense.gov/Portals/1/Documents/pubs/NDAA%20A-P_Maritime_Security_Strategy-08142015-1300-FINALFORMAT.PDF.

Bartles, Charles K. 2016. Getting Gerasimov Right. *Military Review*. January-February 2016. [Online]. [Cited: 28 April 2016.] http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art009.pdf.

BBC. 2015. Russia examines 1991 recognition of Baltic independence. [Online]. 30 June 2015. [Cited: 28 April 2016.] <http://www.bbc.com/news/world-europe-33325842>.

Betts, Richard K. 1985. Conventional Deterrence: Predictable Uncertainty and Policy Confidence. *World Politics*. January, 1985, Vol. 37, 2.

Caffrey, Craig. 2015. Lithuania plans 35% increase in 2016 defence budget. [Online]. 1 October 2015. [Cited: 29 April 2016.] <http://www.janes.com/article/54928/lithuania-plans-35-increase-in-2016-defence-budget>.

Castro, Renato De. 1994. U.S. Grand Strategy in Post-Cold War Asia-Pacific. *Contemporary Southeast Asia*. December, 1994, Vol. 16, 3.

Chanlett-Avery, Emma and Rinehart, Ian E. 2016. The U.S. Military Presence in Okinawa and the Futenma Base Controversy. [Online]. 20 January 2016. [Cited: 27 April 2016.] <https://www.fas.org/sgp/crs/natsec/R42645.pdf>.

Colby, Elbridge and Solomon, Jonathan. 2015. Facing Russia: Conventional Defence and Deterrence in Europe. *Survival*. December 2015-January 2016, Vol. 57, 6.

Defense of Japan. 2015. Defense of Japan (Annual White Paper). [Online]. [Cited: 28 April 2016.] http://www.mod.go.jp/e/publ/w_paper/2015.html.

Department of Defense, United States of America. 2015. Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015. [Online] 2015. [Cited: 27 April 2016.] http://www.defense.gov/Portals/1/Documents/pubs/2015_China_Military_Power_Report.pdf.

Embassy of the People's Republic of China in the Republic of South Africa. 2012. Foreign Ministry Spokesperson Hong Lei's Remarks on Japanese Politician's Erroneous Comments. [Online] 2012. [Cited: 27 April 2016.] <http://www.chinese-embassy.org.za/eng/fyrth/t978143.htm>.

Erickson, Andrew S. and Mikolay, Justin D. 2006. A Place and a Base: Guam and the American Presence in East Asia. [eds.] Carnes Lord. Reposturing the Force: US Overseas Presence in the Twenty-first Century. Newport, Rhode Island: Naval War College Press, 2006.

Freedman, Lawrence. 2004. *Deterrence*. Cambridge: Polity Press, 2004.

Fuentes, Gidget. 2016. U.S. Marines Teach Japanese Forces How to Fight From the Sea in Expanded Iron Fist Exercise. [Online]. 25 January 2016. [Cited: 27 April 2016.] <https://news.usni.org/2016/01/25/u-s-marines-teach-japanese-forces-how-to-fight-from-the-sea-in-expanded-iron-fist-exercise>.

Gerson, Michael S. 2009. Conventional Deterrence in the Second Nuclear Age. *Parameters*. Autumn 2009. [Cited: 25 April 2016.] <http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/09autumn/gerson.pdf>.

Gray, Colin S. 2003. *Maintaining Effective Deterrence*. Carlisle, Pennsylvania: Strategic Studies Institute, 2003.

Guertner, Gary L. 1992. Deterrence and Conventional Military Forces. [cited: 26 April 2016.] <http://www.dtic.mil/dtic/tr/fulltext/u2/a251476.pdf>.

Harkavy, Robert E. 2007. *Strategic Basing and the Great Powers, 1200-2000*. Abingdon: Routledge, 2007.

Information Office of the State Council of the People's Republic of China. 2012. Diaoyu Dao, an Inherent Territory of China. [Online] 2012. [Cited: 27 April 2016.] http://www.china.org.cn/government/whitepaper/node_7168681.htm.

Herpen, Marcel H. Van. 2011. Russia's Embrace of Tactical Nuclear Weapons: Its Negative Impact On U.S. Proposals For Nuclear Arms Reductions. [Online]. September, 2011. [Cited: 28 April 2016.] http://www.cicerofoundation.org/lectures/Marcel_H_Van_Herpen_RUSSIA_EMBRACE_OF_TACTICAL_NUCLEAR_WEAPONS.pdf.

Hicks, Kathleen H. and Conley, Heather A. 2016. Evaluating Future U.S. Army Force Posture in Europe. Phase I Report. [Online]. February 2016. [Cited: 29 April 2016.] http://csis.org/files/publication/160203_Hicks_ArmyForcePosture_Web.pdf.

Huhley, Tim and Schreer, Benjamin. 2015. Standing up to China. *Survival*. December 2015-January 2016, Vol. 57, 6.

Holehouse, Matthew. 2016. Nato may deploy thousands of troops in Europe to ward off Russia. [Online]. 10 February 2016. [Cited: 28 April 2016.] <http://www.telegraph.co.uk/news/uknews/defence/12149403/Nato-may-deploy-thousands-of-troops-in-Europe-to-ward-off-Russia.html>.

Huntington, Samuel P. 1983/1984. Conventional Deterrence and Conventional Retaliation in Europe. *International Security*. Winter, 1983/1984, Vol. 8, 3.

Jackson, Karl D. 1987. U.S. Military Assistance to Asia Facing Cuts. *Contemporary Southeast Asia*. June, 1987, Vol. 9, 1.

Kan, Shirley A. 2014. Guam: U.S. Defense Deployments. [Online]. 26 November 2014. [Cited: 27 April 2016.] <https://www.fas.org/sgp/crs/row/RS22570.pdf>.

Keck, Zachary. 2015. Confirmed: China is Building a Military Base Near Japan. [Online]. 26 January 2015. [Cited: 27 April 2016] <http://nationalinterest.org/blog/the-buzz/confirmed-china-building-military-base-near-japan-12120>.

Kramer, Mark. 2002. NATO, the Baltic States, and Russia: A Framework for Enlargement. [Online]. February 2002. [Cited: 27 April 2016.] http://csis.org/files/media/csis/pubs/ruseur_wp_019.pdf.

Krepinevich, Andrew and Work, Robert. 2007. The US Global Defence Posture and the Second Transoceanic Era. Washington, DC: Centre for Strategic and Budgetary Assessments, 2007.

LaGrone, Sam. 2014. Navy Moving Two Additional BMD Destroyers to Japan. [Online]. 17 October 2014. [Cited: 27 April 2016.] <https://news.usni.org/2014/10/17/navy-moving-two-additional-bmd-destroyers-japan>.

Mearsheimer, John J. 1985. Prospects for Conventional Deterrence in Europe. *Bulletin of Atomic Scientists*. August 1985. [Cited: 25 April 2016.] <http://mearsheimer.uchicago.edu/pdfs/A0009.pdf>.

Ministry of National Defence of the Republic of Lithuania. 2015. A new brigade named Žemaitija is established within the Lithuanian Armed Forces in Western Lithuania. [Online]. 31 December 2015. [Cited: 29 April 2016.] http://www.kam.lt/en/news_1098/current_issues/a_new_brigade_named_zemaitija_is_established_within_the_lithuanian_armed_forces_in_western_lithuania.html

Molin, Anna. 2014. Russia Seeks Investigation of Lithuanian Red Army Deserter: Many Lithuanians in Soviet Army Deserted After Lithuania Declaration of Independence. [Online]. 8 September 2014. [Cited: 27 April 2016.] <http://www.wsj.com/articles/russia-seeks-investigation-of-lithuanian-red-army-deserter-1410191086>.

Morgan, Patrick M. and Paul, T.V. 2009. Deterrence among Great Powers in an Era of Globalization. [eds.] T.V.Paul, Patrick M.Morgan, and James J.Wirtz. *Complex*

Deterrence: Strategy in the Global Age. Chicago: The University of Chicago Press, 2009.

NATO. 2014. Wales Summit Declaration. [Online]. 5 September 2014. [Cited: 28 April 2016.] http://www.nato.int/cps/en/natohq/official_texts_112964.htm.

NATO. 2015. NATO's Readiness Action Plan. [Online]. October 2015. [Cited: 28 April 2016.] http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_12/20151130_1512-factsheet_rap_en.pdf.

Novichkov, Nikolai. 2016. Russia completes reformation of 1st Guards Tank Army. [Online]. 9 February 2016. [Cited: 28 April 2016.] <http://www.janes.com/article/57828/russia-completes-reformation-of-1st-guards-tank-army>.

Office of the Under Secretary of Defense. 2016. European Reassurance Initiative. [Online]. February 2016. [Cited: 29 April 2016.] http://comptroller.defense.gov/Portals/45/Documents/defbudget/fy2017/FY2017_ERI_J-Book.pdf.

O'Rourke, Ronald. 2016. China Naval Modernization: Implications for U.S. Navy Capabilities. [Online] 31 March 2016. [Cited: 27 April 2016.] <https://www.fas.org/sgp/crs/row/RL33153.pdf>.

SHAPE. 2016. Fact Sheet. [Online]. January 2016. [Cited: 29 April 2016.] <https://www.shape.nato.int/page349011837>.

Sisk, Richard. 2016. All Three Zumwalt Class Destroyers to be Assigned to Pacific: Carter. [Online]. 8 April 2016. [Cited: 27 April 2016.] <http://www.military.com/daily-news/2016/04/08/all-three-zumwalt-class-destroyers-assigned-to-pacific-carter.html>.

Solomon, Jonathon F. 2013. Demystifying Conventional Deterrence: Great-Power Conflict and East Asian Peace. *Strategic Studies Quarterly*. Winter 2013. [Cited: 27 April 2016.] http://www.au.af.mil/au/ssq/digital/pdf/winter_13/2013winter-Solomon.pdf.

Sputnik News. 2014. Russia Starts Combat Helicopter Training Flights on Baltic Border. [Online]. 30 April 2014. [Cited: 28 April 2016.] <http://sputniknews.com/military/20140430/189494181/Russia-Starts-Combat-Helicopter-Training-Flights-on-Baltic.html#ixzz47neivdJD>.

Stoicescu, Kalev and Praks, Henrik. 2016. Strengthening the Strategic Balance in the Baltic Sea Area. [Online]. March 2016. [Cited: 28 April 2016.] [http://www.icds.ee/fileadmin/media/icds.ee/failid/Kalev_Stoicescu_Henrik_Praks - Strengthening the Strategic Balance in the Baltic Sea Area.pdf](http://www.icds.ee/fileadmin/media/icds.ee/failid/Kalev_Stoicescu_Henrik_Praks_-_Strengthening_the_Strategic_Balance_in_the_Baltic_Sea_Area.pdf).

Stone, John. 2012. Conventional Deterrence and the Challenge of Credibility. *Contemporary Security Policy*. April, 2012, Vol. 33, 1.

The Embassy of the Russian Federation to the United Kingdom of Great Britain and Northern Ireland. 2014. The Military Doctrine of the Russian Federation. [Online]. 29 June 2015. [Cited: 29 April 2016.] <http://rusemb.org.uk/press/2029>.

The Guardian. 2015. NATO shows its teeth to Russia with elaborate Baltic training exercise. [Online]. 17 June 2015. [Cited: 29 April 2016.] <http://www.theguardian.com/world/2015/jun/17/nato-russia-elaborate-training-exercise-dangerous-signal>.

The Guidelines for Japan-U.S. Defence Cooperation. 2015. [Online]. 27 April 2015. [Cited: 28 April 2016.] http://www.mod.go.jp/e/d_act/anpo/shishin_20150427e.html.

The Jamestown Foundation. 2015. [eds.] Liudas Zdanavičius and Matthew Czekaj. Russia's Zapad 2013 Military Exercise: Lessons for Baltic Regional Security. [Online]. [Cited: 28 April 2016.] [http://www.jamestown.org/uploads/media/Zapad_2013 - Full online final.pdf](http://www.jamestown.org/uploads/media/Zapad_2013_-_Full_online_final.pdf).

The Washington Post. 2014. Transcript: Putin says Russia will protect the rights of Russians abroad. [Online]. 18 March 2014. [Cited: 27 April 2016.] https://www.washingtonpost.com/world/transcript-putin-says-russia-will-protect-the-rights-of-russians-abroad/2014/03/18/432a1e60-ae99-11e3-a49e-76adc9210f19_story.html.

The White House. 2014. Remarks by President Obama to the People of Estonia. [Online]. 3 September 2014. [Cited: 28 April 2016.] <https://www.whitehouse.gov/the-press-office/2014/09/03/remarks-president-obama-people-estonia>.

The White House. 2015. National Security Strategy. [Online]. February 2015. [Cited: 28 April 2016.] https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf.

USNI News. 2015. Document: China's Military Strategy. [Online] 2015. [Cited: 27 April 2016.] <https://news.usni.org/2015/05/26/document-chinas-military-strategy>.

Wood, Peter. 2015. China Plays Helo Card to Shift Military Balance in East China Sea Dispute. [Online] 6 March 2015. [Cited: 27 April 2016.] [http://www.jamestown.org/single/?tx_ttnews\[tt_news\]=43621&tx_ttnews\[backPid\]=7&cHash=675ecb61e1dc0413c0687ffa0966832a#.Vx4rp3rIjzw](http://www.jamestown.org/single/?tx_ttnews[tt_news]=43621&tx_ttnews[backPid]=7&cHash=675ecb61e1dc0413c0687ffa0966832a#.Vx4rp3rIjzw)