# Baltic States - How to React to "New Warfare" in the Context of the Article V?

**Tomáš Čižik**[1]

**Abstract**
Hybrid warfare represents new security challenge for whole Europe. However, hybrid warfare cannot be considered as new phenomenon, Russian aggressive exercise of hybrid warfare (annexation of Crimean Peninsula) took all European states by surprise. It consists of effective combination of tools, such as, information warfare, psychological operations, cyber operations and use of special forces. Russian hybrid warfare is designed to directly challenge the cornerstone of the North Atlantic Treaty Alliance, the Article V., because it combines conventional and unconventional measures, which are difficult to predict and counter. NATO and EU member states are forced to develop new capabilities, to build new infrastructure and to strengthen the eastern boundary of the Alliance to successfully deter potential Russian aggression in its close neighbourhood. It is also very important to build inner resilience of the member states against Russian propaganda that has massively spread throughout Eastern and Central Europe.

**Key words:** hybrid warfare, propaganda, NATO, Russia, security

## INTRODUCTION

Russian "hybrid" warfare has deeply influenced the whole European security architecture. Russia is now increasingly focused on less conventional (asymmetric) military capabilities that are considerably more difficult for NATO to deter or counter. Asymmetric tactics of Russian Federation include – cyber-attacks against state infrastructure networks and websites; information operations including wide-spread dissemination of false information; propaganda and psychological operations; and so-called "little green men", soldiers without insignia or official affiliations (SOF operations). Such tactics were used in Estonia (2007), Georgia (2008) and Ukraine (2014). This represents a new security challenge for NATO, mainly in the Baltic states, with considerable Russian-speaking population. "Officials and residents [of Baltic states] alike fear that after annexing Crimea and assisting a rebellion in the east of the country that is steadily undermining its government in Kiev, Moscow may soon turn its eye to other states where a sizeable minority is ethnically or linguistically Russian" (Sabet-Parry 2015).

Russia can use same tactics in the Baltics as it used in Georgia or Ukraine to

[1] Mgr. Tomáš Čižik, Centre for European and North Atlantic Affairs (CENAA), Tolstého 9, 811 06 Bratislava, e-mail: cizik@cenaa.org

test NATO and the threshold of Article V. It is very important to find a consensus within the Alliance on how to react, or what measures should NATO take to counter the Russian threat and possible aggression on its member states. A study of UK Defence Committee says that "risk of a conventional assault remained low – but warned over methods as cyber-attacks and the use of irregular militias" (UK Defence Committee 2014). In he last 15 years NATO has been focused mainly on foreign operations and did not invest too much attention to territorial defence, because after the end of the Cold War and the dissolution of the Soviet Union there was no direct military threat for NATO in Europe and because Russia was considered as partner. Russia has clearly different objectives that EU and NATO have believed. According to the Economist (2015) Putin's "overarching aim is to divide and neuter that alliance, fracture its collective approach to security, and resist and roll back its advances". All actions that were taken by President Putin in last three years was aimed against the EU and NATO member states, to hamper mutual cooperation and reaching consensus among states, to undermine the trust of general population to state and European institutions, national political elites and to democratic system. Kremlin has undeniably developed very effective set of asymmetric tools, which allow easy interference into internal affairs of states without any massive investment into hard power. Hybrid warfare allowed Putin to shift from the use of hard power or military to the use of so-called "soft power". "Soft-power" according to Joseph Nye (2004) is "the ability of a country to persuade others to do what it wants without force or coercion". The definition of Joseph Nye has a positive meaning and it means the power of attraction (European Union can be used as a best example of the exercise of "soft power" for example). On the other side, Kremlin gave the term "soft power" different, negative meaning. "In the Russian context, however, "soft power" is often used in a different way to denote the ability of an actor to wield power of non-military, non-traditional ways, such as through disgruntled minority groups, media outlets, the entertainment industry and the domestic political system of another country" (Winnerstig, 2015).

This article will focus on the short definition of hybrid warfare and its tools and possible non-conventional solutions that NATO had and should implement to become more deterring and better prepared for Russian aggressive actions. It is clear that hybrid war cannot be faced only by conventional measures. However, it is questionable if NATO is the most appropriate organization, which should react on all aspects of hybrid warfare.

## 1 HYBRID WARFARE

At first, it is necessary to define what hybrid warfare is and what tools it is using. Nowadays, hybrid warfare is mostly associated with the Russo-Ukrainian war. The definition of hybrid warfare according to Hunter and Pernik (2015) is as follows: "sophisticated campaigns that combine low-level conventional and special operations; offensive cyber and space actions; and psychological operations that use social and traditional media to influence popular perception and international opinion". Hybrid war is not a new concept, it was part of conflicts hundreds years ago,[2] but currently, the information era and new technologies creates very specific environment, where hybrid tactics are very useful and effective. Hybrid warfare comprises the use of special forces, information warfare, cyber warfare and psychological warfare besides the conventional way of fighting. These four elements of hybrid war are used in certain order to reach the desired results or to establish favorable political, military and economic conditions that are in favor of an attacker. Hybrid warfare relies mostly on unconventional tools (soft power) and it cannot be considered a war between two conventional armies. One of those unconventional tools are "hybrid forces". "Hybrid force is a military organization that employs a combination of conventional and unconventional organizations, equipment, and techniques in a unique environment designed to achieve synergistic strategic effects" (Harel and Issacharof 2008; cf. McCulloh and Johnson 2013).

Russian hybrid tactics that are used in Ukraine can result in significant difficulties for NATO member states conventional armies, because it is mostly oriented toward a symmetrical way of fighting or use of conventional tools to defend it members. Annexation of Crimea by Russian Federation took everybody by surprise. Firstly, because nobody expected such military offensive in European territory and secondly, because Russia behaved as partner state all the time. However, Russian behavior became more and more aggressive since 2014, but nobody took is seriously (except Baltic states and Poland, who always warned of Russian behavior. "It started at Munich Security Conference in 2007, where Vladimir Putin said that "Russia should play and increasingly active role in world affairs" (The Washington Post, 2007), it follows by "the suspension of the implementation of the Treaty on Conventional Armed Forces in Europe in 2007, Russian "peacekeeping mission" in Abkhazia followed by the Russian intervention to Abkhazia and South Ossetia in 2008, large military exercises on Russia's western borders near Georgia and Ukraine, or multiple incursions against the air sovereignty of many NATO member states, which continues to

[2] Origins of hybrid warfare can be traced back to the age of Antiquity.

this day at high rates" (Čižik, 2015a). Analyses of the Russian hybrid warfare approach during Crimea annexation shows that "Russia has found a 'new art of war' that made up for shortcomings in its conventional capabilities and, if repeated, could pose a considerable threat to states in the West" (Jones 2014, Renz and Smith 2016).

The origins of Russian hybrid warfare can be traced back to 2013, when Valerii Gerasimov. Russian Chief of the General Staff published his article.

NATO, at this moment, is simply not fully prepared to deal with the hybrid warfare and there is a need for development of a new set of capabilities to strengthen the Alliance. On the other side, the Alliance did not stand inactive and many steps were states. To sum up, how Russia sees hybrid warfare, we can use following definition: "Russian view of modern warfare is based on the idea that the main battlespace is the mind and, as a result, new-generation wars are to be dominated by information and psychological warfare, in order to achieve superiority in troops and weapons control, morally and psychologically depressing the enemy's armed forces personnel and civil population" (Berzins 2014).

### 1.1 Information warfare

Without a doubt, Russia has long-standing experience with the dissemination of propaganda. First, propaganda in Russia was used to spread the ideology of Marxism-Leninism and later became the tool of choice in the competition with the United States during the Cold War. Since the dissolution of the Soviet Union, propaganda in Russia has taken a step back and ceased to be relied on to such an extend as was the case during the Cold War. Nevertheless, ever since the annexation of the Crimea by the Russian Federation in March 2014, it has made resurgence, with its dissemination reaching gigantic proportions and the greatest concentration of activity registered by the states of Central Europe, the Baltics and the Ukraine (Krivoruchko 2015). Even though the political elites in the countries concerned do not seem to devote much attention to these propaganda activities, from a long-term perspective it represents a rather dangerous phenomenon, which requires maximum attention. The question that remains is what makes the Russian propaganda so effective, what are its goals, and what can be done to defend against it. According to Saifetdinov (cf. Franke 2015) information warfare "needs to be continuously conducted in peacetime, in periods of escalating threats, and in wartime with all available forces and as a way to act against the information objects of the opposing side and to defend one's own from similar actions". Russia is conducting so-called offensive information warfare that is composed of these five elements: "electronic warfare,

psychological operations, deception, physical attack on information processes and information attack in information processes" (Nichiporuk 2002, 188). In case of Russia, the main goals of information warfare are the spreading of misleading information, brainwashing of the population and destabilization of society, as well as influencing the strategic decisions of other countries. Information warfare is the most efficient tool that Russia is currently using against NATO and EU member states. Currently, Russian government invests much more attention and finances into propaganda campaigns than just a few years ago. "Since 2005, the Russian government has increased the channel's [Russia Today] annual budget more than tenfold, from $30 million (€22,6 million) to over $300 million" (Bidder 2015). More detailed information about Russian investments into state media are provided by DELFI (2015) - "the budget for the RT agency (formerly Russia Today) in the period 2007-2015 was approximately 120 million USD, reaching its height over 2013-2014 with 400 million USD. Sputnik News in conjunction with Ria Novosti have a combined operating budget of 200 million USD per year, not to mention the local media involved in the spreading of propaganda".

Russia is focusing on three main areas: "internally and externally focused media with a substantial online presence; […] use of social media and online fora as a force multiplier to ensure Russian narratives achieve broad reach and penetration; language skills, in order to engage with target audiences on a broad front in their own language" (Giles 2015). Moreover, it is important to note that Russian propaganda is spread in national languages and is tailor-made for specific countries and regions. This makes messages created in Russia by professionals more powerful, because it is easier for people to get the information in language that they understand without the necessity of translation. Another Russia's great advantage is the inability of western countries to effectively fight against this propaganda because they are limited by freedom of expression. However, in April 2015 Lithuania as the only state banned Russian TV station RTR for three months for repeatedly broadcasted myths and propaganda (Čižik 2016).

According to Euromaidanpress (2015) the Russian federal budget for Russia Today TV station in 2015 has increased by 41%. Also, TV Novosti got 15.38 billion rubles (approximately 250 million eur). Altogether, in 2015 Russia investmented into media increased by approximately 250%. Russia has always used propaganda, but this increase in investment is also proof of Russian intentions. Russian government also employs so-called "trolls" whose main goal is to flood the internet and social media with lies or misinformation and to influence the public opinion in the West. "Trolls manage several social media accounts under different nicknames, [and they are] attracted by relatively high monthly salaries of 40,000 to 50,000 rubles ($800 to $1000) (CTVNews,

2015). To compare, for Russia work thousands of trolls and investments into propaganda is up to billion rubles, and on the other side is NATO and its tens of employees in NATO Public Diplomacy Division and limited investments (The Guardian 2015). Without significant changes inside the EU and NATO, it will not be possible to stop Putin's trolls. Moreover, the consumers of propaganda are also Russian citizens, who have no other source of information than media that are owned by the Russian government.

Psychological warfare is an inseparable part of Russia's information warfare, even though information warfare is not limited only to psychological operations. In 2000 the first Russian Information Security Doctrine was approved that "laid out tasks for improving [Russian] electronic and intelligence combat abilities to include elements to counter propaganda" (Hunter and Pernik 2015). "Russia operates under the supposition that regime security and national security are one and the same" (Franke 2015, 19-20). So definitely, Russia is aware of the effectiveness of psychological and information warfare. The main goal of psychological warfare is to identify enemy's weaknesses and hit the opponent where it hurts. "The main objective is to reduce the necessity for deploying hard military power to the minimum necessary, making the opponent's military and civil population support the attacker to the detriment of their own government and country" (Berzins 2014).

### 1.2 Cyber-attacks

Russia is considered as a state with great cyber capabilities (UK Defence Committee 2014). As proof of these capabilities can serve the cyber-attacks on Estonia in 2007 or Georgia in 2008. In 2007, "several of Estonia's banks, schools, media networks and government departments were disabled by sustained attack on their computer networks" (UK Defence Committee 2014). Russia possesses the capability to effectively cripple a state and achieve key strategic goals even before it will be registered what is going on. "The majority of Russian attacks in cyberspace have been psychological in nature" (Berzins 2014). The same cyber-attacks can be used again on one of NATO member states, which poses a question if NATO will be able to defend its networks, because it still has not developed effective defence against cyber-attacks. NATO has developed NATO Computer Incident Response Capability (NCIRC) that should protect the Alliance's networks. The question remains whether this protection will be able to counter or defend against cyber-attacks coming from Russia, while Russia clearly has much more experience with information warfare and cyber-attacks than NATO member states. Wales Summit also incorporated cyber-attacks into

Article V of the Washington Treaty, but each cyber-attack on a member state will be considered individually. Incorporation of cyber-attacks into Article V is definitely a positive step forward, which allows states to invoke Article V not only in case of armed attack.[3] However, consideration of such an attack will take some time, and without effective defence it can cause significant material losses or serious infrastructure damages. It is important to note that each state should develop its own set of defence capabilities that should also include cyber defence. Currently there is discussion if NATO should protect only its own networks or protect also the networks of its member states. 14th May 2008 saw the opening of NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, which should successfully counter threats in the area of cyber security.

### 1.3 Special forces

Special forces fulfils very specific roles in hybrid warfare. Ukrainian war is the best example. The annexation of Crimea was accompanied by the "appearance of "little green men" who occupied key buildings including political and communications headquarters and laid siege to Ukrainian armed forces. However, those little green men were not wearing Russian uniforms or visible Russian insignia, but they "all wore the latest Russian kit and drove military vehicles with official plates" (UK Defence Committee 2014). Moreover, separatists are equipped with modern Russian military equipment and many of them have clear ties with Russian state security forces (FSB). Russia still has not admitted that there are Russian troops in Ukrainian territory, despite clear evidence to the contrary. On August 2014, NATO has released satellite images of Russian combat troops inside Ukraine.[4] Latest estimates say that "12,000 Russian troops are operating inside" Ukraine (Urban 2015). Additional evidence of Russian involvement in Ukraine could be a decree signed by Putin, which is "making a state secret of any information about losses of Russian troops "during special operations" in peacetime" (UNIAN 2015). Denying Russian presence in Ukraine is also a part of information warfare. Russia employed special forces mainly for their ability to effectively operate on foreign territory in small numbers.

## 2 IMPLICATIONS FOR NATO

So why is hybrid warfare so challenging for the Alliance? The same scenario that happened in Ukraine can be used in any one of NATO member states, most probably one of the Baltic states. Estonian city Narva, which lies only 300 meters

[3] The decision, which attack will be covered by Article V is still based on consensus of member states.
[4] See: http://www.nato.int/cps/en/natohq/news_112193.htm

from Russian border, can become Russia's next target to test NATO reaction. In Narva lives Russian minority, the same as for example in Crimea, so Putin could potentially test the same scenario in this Estonian city.

The invocation of article V demands clear evidence that an armed attack was conducted against one of the NATO member state, but in the current situation when the possibility that "little green men" will besiege governmental buildings in one of the NATO member state or other than conventional armed attack will be undertaken against the member state makes the invocation of Article V even more challenging. The same principle applies in case of information and psychological warfare or cyber-attacks. These attacks are intended to damage, weaken or confuse the opponent and NATO does not have a clear strategy on how to face them. As a response, the Alliance has strengthened its military presence in Central and Eastern Europe and the Baltic states, announced the creation of NATO Very High Readiness Joint Task Force, many of NATO member states announced that they will increase their defence spending, but these conventional measures cannot stop Russia in its hybrid tactics (Čižik and Novák 2014, 92-93). Moreover, new NATO Force Integration Units (NFIU) was established in a number of NATO member states (Slovakia, Hungary, Bulgaria, Estonia, Latvia, Lithuania, Poland and Romania, which should facilitate the deployment of NATO high-readiness forces to the region "in a rapid manner and prepare for subsequent operations if required" (NATO 2015). NATO should develop also some unconventional methods, which will be able to deter or counter Russian actions.

It has to be said that NATO cannot do so alone − without cooperation within the Alliance and with partners this task will be impossible. Viable partners in this undertaking for NATO can be the EU and NORDEFCO[5] given that most of the NATO member states are also members of EU and vice-versa. Joint efforts of these two organizations to stop or slow Russia could work very well. Economic power of the European Union together with the political and military power of NATO can serve as an effective deterrent to Russia.

Russia will rely on hybrid warfare because its military cannot defeat the militaries of NATO member states. Therefore, unconventional tools used by Russia are aimed at the weakest points of the Alliance and EU (Ondrejcsák 2015). So, where are the limits of NATO facing hybrid warfare?

[5] NORDEFCO is the best example of regional defense cooperation and is composed of five Nordic countries and its homepage says that "mutually reinforcing cooperation in capability development can be achieved without negative influence on participating countries' different foreign and security policy orientation and membership obligation in NATO, the EU and the UN" (NORDEFCO, n.d.). It is a brilliant example of how cooperation between states should look.

First, the biggest limit of NATO is the internal division within the Alliance regarding Russia. For Baltic states and Poland Russia represents long-term and imminent threat. On the contrary, the relations of Central European political elites to Russia and President Putin are more ambiguous and disunited. In addition, Germany is behaving very carefully, when military or hard-power measures against Russia are discussed. Germany relies mostly on its economic power and diplomacy, while the Baltic states are asking for more troops and weapons. Moreover, Russian information warfare is successfully dividing NATO members states even more.

Second, internal division hampers reaching consensus and decision making of the Alliance and EU. NATO and EU[6] are based on consensus and Putin is fully aware of this situation and it puts him in an advantageous position. Discussions about important issues always take some time to work through and significantly prolong the reaction time of the actors involved. Moreover, cooperation between NATO and EU member states is negatively influenced by their internal disagreements and disagreements between Turkey, Cyprus and Greece.

Third, inconsistency in policies of Central and Eastern European states (approval of the sanctions at the NATO and EU level, but their criticism on the national level) support the Russian propaganda that is very effective in those countries (Ondrejcsák 2015). "The overall impact of the Russian information warfare on Central Europe is multiplied also by ambiguity of high-level politicians towards Russia. Ambiguity in this case means the incompatibility of domestic and international politics of Central European countries or unwillingness to label Russian Federation as an aggressor responsible for violations of international law and threat for European security architecture. Inconsistent statements of top politicians only contribute to the further division of the population towards official policy of the country. To be specific, open critics of sanctions that were imposed on Russian Federation by European Union by Róbert Fico, Prime Minister of Slovak Republic on domestic level just few hours afterwards they were unanimously approved by all EU member states in Brussels does not shed a positive light on Slovakia as a reliable partner" (Čižik, 2017).

Fourth, absence of common tool, approach or agency that will be able to counter or mitigate Russian propaganda. For example, in Central Europe Russian propaganda works very well, mainly if it is supported by local politicians and disseminated by alternative media in combination with Russian 'trolls'. What compounds the problem further is that in many states there are missing strategies to carry out the fight against propaganda. Moreover, many states do not consider propaganda as an imminent threat and do not take any measures to

[6] Consensus in EU is necessary only in the field of security.

protect its citizens (Slovakia or Hungary for example). Absence of strategies also negatively influences the cooperation between states. Successful anti-propaganda campaign should start in schools, also because education can be a good remedy to conspiracy theories. Education also strengthens inner resilience of states and their citizens who are then less vulnerable vis-à-vis information warfare, disinformation campaigns, conspiracy theories and hoaxes. On European Union level was established East StratCom Task Force, which main aim is to address Russia's ongoing disinformation campaigns. Its activity consists of 3 main objectives: effective communication and promotion of EU policies towards Eastern Neighbourhood; strengthening the overall media environment in the Eastern Neighbourhood and in EU Member States, including support for media freedom and strengthening independent media; and improved EU capacity to forecast, address and respond to disinformation activities by external actors (EEAS, 2015).

## 3 NATO UNCONVENTIONAL MEASURES

Hybrid warfare is a very complex challenge for NATO. It is composed of conventional and unconventional measures. To deal with it successfully requires the application of complex solutions – a mixture of effective conventional deterrence and unconventional measures that will allow NATO to act, not to react. "As a part of a cohesive response to these challenges, and in order to deter or defend against state or non-state actors employing hybrid warfare, NATO, and its members, and partner states must be able to develop, implement and adapt strategies combining diplomatic, military, informational, economic and law-enforcement efforts" (The Military Balance 2015).

First of all it is necessary to unify the voices within the Alliance. NATO must take a strong position and send this message also outside the Alliance. As it is, there are too many voices inside the Alliance, which have to come to a consensus to take action, but on the other hand there is Russia with only one voice, the voice of Vladimir Putin. Russia is an imminent threat and all member states have to come to terms with it and advocate strong opposition against Russian actions. The main problem lies in that for some states Russia does not represent an imminent threat, and there is a lack of common clear evaluation of the threat that Russia represents for NATO. Therefore, common communication strategy should be developed to alleviate and shorten the reaction time of the Alliance. As long as the reaction within the Alliance will not be clear and unified, the answer will be still weak and ambiguous. Common communication strategy will set the way how certain actions taken by Russia will be evaluated and communicated.

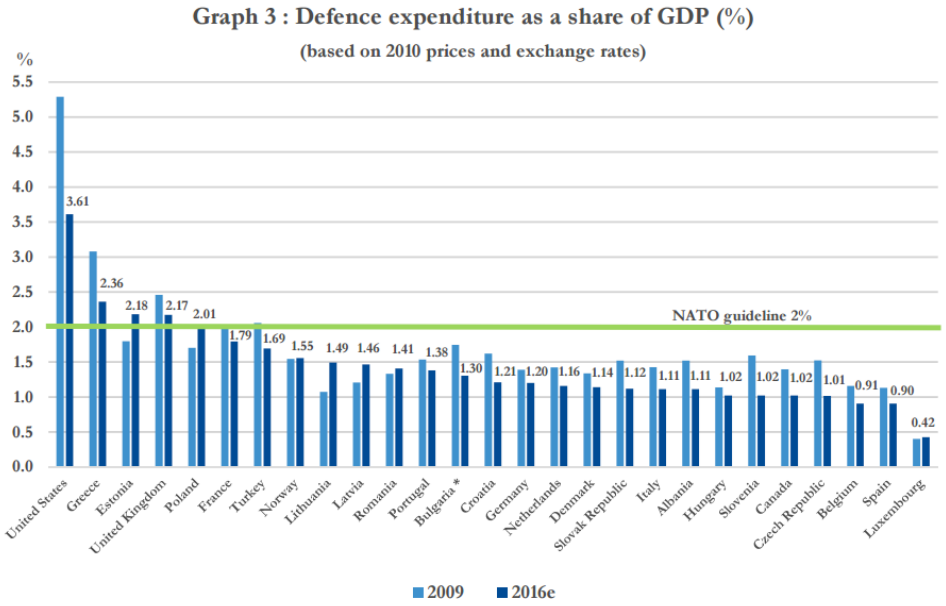
One of the biggest challenges for NATO and the EU is Russian propaganda. There is a discussion underway whether the reaction should be in the way of counter-propaganda or via developing a new concept how to minimize the damages or even challenge Russia on its own territory. Needless to say, counter-propaganda would be the worst option. One of the possible solutions is the creation of a common media agency that will be jointly financed and managed. It will broadcast verified facts about Russian actions in Russian language to Russia and the neighbouring states with significant Russian minority (Belarus, Ukraine or the Baltic states). It is important to challenge Russia on its own territory and to offer to its citizens an alternative source of information, thus weakening Putin's position at home. This is especially so because "Propaganda is too pervasive. About 90 percent of Russians get news from national television and the segment of Russians who are critical don't watch the news at all" (Pszczel 2015). Public relation and communication experts were working on an operation to counter Russian propaganda to be completed by June 2015. This fully-fledged plan should "develop and EU narrative through key messages, articles, op-eds, factsheets, infographics, including material in Russian language (EurActiv 2015). However, there is still the distinct possibility that these channels will have poor viewership, due to the perception that they are run by western companies.

Hybrid warfare also challenges the Article V of Washington Treaty. Therefore, it is necessary to set concrete conditions when it is to be invoked. In case of the Russian test of NATO reaction to "little green men" sent to the territory of its member states or cyber-attack it will allow for immediate response. There is "a low likelihood of a Russian conventional attack on a Baltic state. However, NATO has an obligation under the Article 5 to protect Baltics as NATO Member States" (UK Defence Committee 2014). There have to be clear rules when the Alliance should react without protracted discussion or negotiations between member states. Clearly defined conditions and fast response can successfully deter Russia from testing the cornerstone of the Alliance. The speeding up of NATO reaction can be partially solved by increasing of the autonomy of commanders in deciding when to respond to an attack. Currently, NATO can respond only after the approval of the North Atlantic Council (NAC), which can take hours before the final approval. Greater autonomy of commanders (to a certain level) will definitely increase the capability of the Alliance to deter Russia.

Low or better said slowly rising defense budgets of member states are also contributing to the inability of NATO to deter Russia or defend itself against hybrid warfare. Currently only five states spend 2% or more of their GDP on defense (Poland, Estonia, Greece, United States and United Kingdom) (NATO 2017). This negative trend has to be reversed. After the annexation of Crimea

many member states committed to increasing their defense spending. “Poland aims to increase the defence spending to the 2% by the year 2016 and to go even beyond this commitment. Latvia and Lithuania have pledged to reach the 2 percent target by the year 2020. Romania has promised to increase its defence spending gradually until 2016. Czech government has said it aims to reverse the trend of declining defence spending” (Croft 2014; cf. Čižik and Novák 2014). Slovakia also announced that its defence expenditures will reach the 1.6% mark of GDP by 2020. In 2016, the defence spending of Slovak Republic reached 1,12 % of GDP, so there can be seen slow growth, however it is very questionable, if Slovakia will be able to spend 1,6 % of GDP on defence in 2020[7]. However, both President and Prime Minister Slovakia expressed that our commitments will be fulfilled without any doubts. Without considerable political will within the Alliance it will prove impossible to successfully deter Russia.

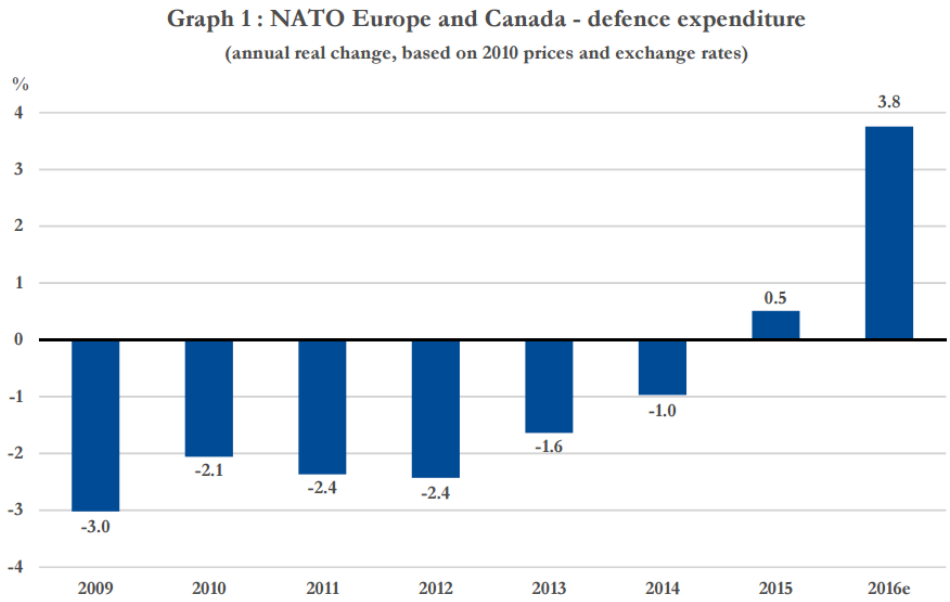
**Table 1:** Defence expenditures of NATO member states as a share of GDP




Source: NATO (2017)

[7] Slovak government allocated finances to acquire new Blackhawk helicopters, which will increase the Slovak defense spending by 0.1% in 2017. Nevertheless, these additional expenditures cannot be considered as part of the plan of Slovak government to increase the overall defense spending.

**Table 2:** NATO Europe and Canada – Defence expenditure




Source: NATO (2017)

Cyber attacks are yet another big challenge for the Alliance. "While there is certainly espionage and low-level conflict in cyberspace, most experts would agree that we have yet to see the first real "cyber war". According to Vixie we are now living in a new "state of affairs", where every nation state or company has to defend itself against adversary, which can be domestic or foreign (International Centre for Defence and Security 2015). Information sharing between military and civilian authorities within the nation states and within the Alliance is crucial to develop effective defence against the cyber attacks. However, development of critical infrastructure protection will be also crucial for this task. Without strong cyber capabilities NATO will be unable to defend its own networks and networks of its member states. According to International Centre for Defence and Security (2015) there is "complete lack of existing international law governing foreign electronic intelligence gathering". NATO Wales Summit brought some important steps in this regard moving forward, namely due to incorporation of cyber-attacks into Article V. Thus, also hybrid attack on any of NATO member state can invoke Article V, which will nevertheless in the end always depend on the decision of member states.

## CONCLUSION

According to many experts, hybrid warfare and asymmetrical way of fighting will now prevail in interstate and intrastate conflicts. Best proof of this is Afghanistan, where asymmetric warfare significantly influenced the military presence of the United States and NATO. Although both actors possess the best military equipment, they were unable to defeat Taliban, mainly due to the asymmetric tactics employed. The main advantage of hybrid and asymmetric warfare is that it is aimed against the weakest points of the adversary. Hybrid warfare is now extensively used in the territory of Ukraine by Russian forces and was also used during the annexation of Crimea. Due to increased reliance of Russia on this model of fighting, hybrid warfare constitutes a new challenge for the Alliance. In order to address it, NATO has to undertake some necessary measures to become again able to deter potential adversaries, just as it has during the Cold War. However, now the political situation is different and NATO has to adapt to it.

It is important to find a strong voice within the Alliance and strengthen its core the same as during the Cold War. Since the establishment of NATO in 1949 it successfully guarantees security for all its members. Over the years, there were many challenges that the Alliance had to address, but all of them were always solved successfully. Now hybrid warfare is another challenge NATO is facing as Russia has taken action to unilaterally change the whole European security architecture, a surprise move for which nobody was prepared. Prior to that Russia was considered as the partner of the Alliance. Facing this new reality, NATO should develop effective mixture of conventional and unconventional measures as soon as possible to become again resolute and ready to defend all its members in any situation.

First steps were already taken with the incorporation of cyber-attacks into Article V, development of new rapid reaction forces, improvements in defence spending of NATO member states or with the establishment of seven NATO Force Integration Units. Moving forward, it will be important for NATO member states to decide to what extent hybrid threats will be addresses solely by NATO and where other organization should be involved. There is no doubt hybrid warfare represents a complex issue which also calls for comprehensive countermeasures. Although, it will be necessary to strengthen the conventional capabilities of individual NATO member states, also development of brand new capabilities should be high on the agenda that will allow NATO to cope with the hybrid threat more effectively. As with everything, these new capabilities will demand more resources and willingness of states to commit to making the required investments.

## REFERENCES


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*. Available from: http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx. [Accessed November 12, 2015].

BIDDER, B 2015, 'Russia Today: Putin's Weapon in the War of Images', *Spiegel Online*, 13 August. Available from: http://www.spiegel.de/international/business/putin-fights-war-of-images-and-propaganda-with-russia-today-channel-a-916162.html. [Accessed June 12, 2015].

ČIŽIK, T & NOVÁK, P 2014, 'North Atlantic Treaty Alliance' in R. Ondrejcsák (ed), *Introduction to Security Studies*, pp. 85-114. Centre for European and North Atlantic Affairs, Bratislava.

ČIŽIK, T 2015, 'Najsilnejšia zbraň Ruska - propaganda' *Denník N*. 18 May. Available from: https://dennikn.sk/135672/najsilnejsia-zbran-ruska-propaganda/. [Accessed January 7, 2016].

ČIŽIK, T 2015a, 'Implications for Security and Defence Cooperation of the Nordic-Baltic Region Following the Annexation of Crimea by Russian Federation'. In Róbert Ondrejcsák and Grygoryi Perepelytsia (eds.). *Ukraine, Central Europe and the Future of European Security*. Bratislava: Centre for European and North Atlantic Affairs. pp. 66-87.

ČIŽIK, T 2017, 'Russian Information Warfare in Central Europe'. In Tomáš Čižik (ed.). *Information Warfare – New Security Challenge for Europe.* Bratislava: Centre for European and North Atlantic Affairs.

DELFI. 2015. 'Kremlin's millions: How Russia funds NGOs in Baltics (3).' Available from:
http://en.delfi.lt/nordic-baltic/kremlins-millions-how-russia-funds-ngos-in-baltics.d?id=68908408. [Accessed September 4, 2016].

'Russian "troll factory" flooding Internet with propaganda' 2015, *CTVNews*, 29 May. Available at: http://www.ctvnews.ca/sci-tech/russian-troll-factory-flooding-internet-with-propaganda-1.2396874. [Accessed May 27, 2015].

'Putin's war on the West' 2015, *Economist,* 14 February, Available from: http://www.economist.com/news/leaders/21643189-ukraine-suffers-it-time-recognise-gravity-russian-threatand-counter. [Accessed June 14, 2015].

'Question and Aswers about the EAST StratCom Task Force' 2015, *European Union External Action Service*. Available from: http://collections.internetmemory.org/haeu/content/20160313172652/http://eeas.europa.eu/top_stories/2015/261115_stratcom-east_qanda_en.htm. [Accessed March 22, 2017].

‘EU launches operation to counter Russian propaganda’ 2015, *EurActiv.* 20 March. Available from: http://www.euractiv.com/sections/global-europe/eu-launches-operation-counter-russian-propaganda-313099. [Accessed May 23, 2015].

‘Russia to increase propaganda media budget by 250%’ 2015, *Euromaidanpress.* 23 September. Available from: http://euromaidanpress.com/2014/09/23/russia-to-increase-budget-by-2-2-times-for-its-main-propagandists-russia-today-and-dmitry-kiseliov/. [Accessed May 27, 2015].

FRANKE, U 2015, *War by Non-Military Means: Understanding Russian Information Warfare.* Available from: http://foi.se/Global/Press%20och%20nyheter/War%20by%20non-military%20means.pdf. [Accessed May 14, 2015].

GILES, K 2015, ‘Russia’s Hybrid Warfare: a Success in Propaganda’. *Bundesakademie fur Sicherheitspolitik*. Available from: https://www.baks.bund.de/de/aktuelles/working-paper-russias-hybrid-warfare-a-success-in-propaganda. [Accessed May 12, 2015].

HUNTER, E & PERNIK P 2015, ‘The Challenges of Hybrid Warfare.’ *International Centre for Defence and Security*. Available from: http://www.icds.ee/fileadmin/media/icds.ee/failid/Eve_Hunter__Piret_Pernik_-_Challenges_of_Hybrid_Warfare.pdf. [Accessed May 7, 2015].

International Centre for Defence and Security. 2015. *CyCon Day 2&3: Militarization of Cyberspace?* Available from: http://www.icds.ee/blog/article/cycon-day-2-3-militarization-of-cyberspace/. [Accessed June 1, 2015].

JONES, S 2014, ‘Ukraine: Russia’s new art of war’. *The Financial Times.* August 28. Available from: https://www.ft.com/content/ea5e82fa-2e0c-11e4-b760-00144feabdc0. [Accessed April 1, 2017].

Krivoruchko, Natalya , Lukasz Wenerski. 2015. “How Kremlin propaganda works in Europe.“ *Stopfake*. Available from: http://www.stopfake.org/en/how-kremlin-propaganda-works-in-europe/. [Accessed October 16, 2015].

McCULLOH, T & JOHNSON, R 2013, ‘Hybrid Warfare’. *Joint Special Operation University*. Available from: http://jsou.socom.mil/JSOU%20Publications/JSOU%2013-4_McCulloh,Johnson_Hybrid%20Warfare_final.pdf. [Accessed May 5, 2015].

NICHIPORUK, B 2002, ‘U.S. Military Opportunities: Information-Warfare Concepts of Operation’. in Z. Khalilzad & J. Shapiro (eds), *Strategic Appraisal: United States Air and Space Power in the 21st Century*, pp. 179-215. RAND Corporation. Available from: https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1016/MR1016.chap7.pdf. [Accessed

October 12, 2015].
NORDEFCO n.d., *The basics about NORDEFCO*. Available from: http://www.nordefco.org/The-basics-about-NORDEFCO. [Accessed June 12, 2015].
North Atlantic Treaty Organization 2017. *Defence Expenditure of NATO Countries (2009-2016)*. Available from: http://nato.int/nato_static_fl2014/assets/pdf/pdf_2017_03/20170313_170313-pr2017-045.pdf. [Accessed March 21, 2017].
North Atlantic Treaty Organization 2015, *Six NATO Force Integration Units Activated*. Available from: http://www.aco.nato.int/six-nato-force-integration-units-activated. [Accessed January 14, 2016].
NYE, J. S 2004, 'Soft Power: The Means to Success in World Politics.' *Foreign Affairs.* Available from: https://www.foreignaffairs.com/reviews/capsule-review/2004-05-01/soft-power-means-success-world-politics. [Accessed July 20, 2015].
ONDREJCSÁK, R 2015, 'Ruská hybridná vojna môže spôsobiť zmätok v NATO'. *Denník N*. 27 February. Available from: https://dennikn.sk/59065/ruska-hybridna-vojna-moze-sposobit-zmatok-v-nato/. [Accessed June 13, 2015].
ONDREJCSÁK, R 2015, 'Rusko vie, že prítomnosť NATO na východe Európy je obmedzená'. *Pravda*. Available from: http://spravy.pravda.sk/svet/clanok/356017-rusko-vie-ze-pritomnost-nato-na-vychode-europy-je-obmedzena/. [Accessed May 25, 2015].
PSZCZEL, R 2015, 'EU, NATO Try To Counter Russian Propaganda'. *DefenceNews*. 3 May. Available from: http://www.defensenews.com/story/defense/international/europe/2015/05/03/eu-nato-try-counter-russian-propaganda/26835303/. [Accessed May 26, 2015].
RENZ, B & SMITH, H 2016. 'Russia and Hybrid Warfare – Going Beyond the Label'. *Aleksanteri papers.* Available from: http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf. [Accessed March 29, 2017].
SABET-PARRY, R 2015, 'Ukraine crisis: Inhabitants of the Baltic states fear that they will be next in the firing-line'. *The Independent*. 19 February. Available from: http://www.independent.co.uk/news/world/europe/ukraine-crisis-inhabitants-of-the-baltic-states-fear-that-they-will-be-next-in-the-firingline-10058085.html. [Accessed June 12, 2015].
''Salutin' Putin: inside a Russian troll house' 2015, *The Guardian* , 2 April. Available from: http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house. [Accessed June 12, 2015].
The Military Balance 2015. 'The Military Balance. The annual assessment of

global military capabilities and defence economics'. *International Institute for Strategic Studies*. Available from: https://www.iiss.org/en/publications/military%20balance/issues/the-military-balance-2015-5ea6. [Accessed May 23, 2015].

UK Defence Committee. 2014, *Towards the next Defence and Security Review: Part Two-NATO. Defence Committee – Third Report*. Available from: http://www.publications.parliament.uk/pa/cm201415/cmselect/cmdfence/358/35802.htm. [Accessed May 19, 2015].

'Putin's decree on military losses may be evidence Russian troops in Ukraine – Amnesty International' 2015, *UNIAN,* 5 May. Available from: http://www.unian.info/politics/1083486-putins-decree-on-military-losses-may-be-evidence-russian-troops-in-ukraine-amnesty-international.html. [Accessed June 12, 2015].

URBAN, M 2015, 'How many Russians are fighting in Ukraine?' *BBC News*. 10 March. Available from: http://www.bbc.com/news/world-europe-31794523. [Accessed June 12, 2015].

The Washington Post. 2007. 'Putin's Prepared Remarks at 43rd Munich Conference on Security Policy.' February 12. Available from: http://www.washingtonpost.com/wp-dyn/content/article/2007/02/12/AR2007021200555.html. [Accessed July 20, 2015].

WINNERSTIG, M 2014. 'Introduction.' In *Tools of Destabilization. Russian Soft Power and Non-military Influence in the Baltic States*, edited by Mike Winnerstig, 14-16. Swedish Defence Research Agency (FOI). Available from: http://appc.lv/wp-content/uploads/2014/12/FOI_Non_military.pdf. [Accessed July 20, 2015].