Research Article		Open Access

David Takacs*

Ukraine‘s deterrence failure: Lessons for the Baltic States

DOI 10.1515/jobs-2017-0001
received January 31, 2017; accepted March 7, 2017.

Abstract: The annexation of Crimea in 2014 was a clear sign that Moscow is looking to extend its sphere of influence and it forced the Baltic States to take a very close look at their deterrent capabilities. The article introduces the basic concepts of deterrence and discusses the differences between the deterrent capabilities of Ukraine and the Baltic States. Furthermore, the threats that Russia presents, the factors that were responsible for Ukraine's deterrence failure and the challenges that the Baltic States are facing are analysed. The article concludes that while the Baltic States are significantly better prepared for possible Russian aggression, their deterrent capabilities must continuously evolve to reflect the changes in the nature of modern warfare.

Keywords: deterrence, Russia, Baltic States, Ukraine, Crimea, hybrid warfare

Introduction

Over recent years, the European geopolitical map has been through a period of turbulent development, with the events in Ukraine being the most serious geopolitical conflict in Eastern Europe since the end of the Cold War. The annexation of Crimea and the events surrounding it were not only severe violations of international law and treaties, but have been a clear sign that Russia is looking to revise the structure of international relations in the region. Its implications reach far beyond Eastern Europe and it forces us to re-evaluate the perceptions of international conflict and to develop a new understanding of war and peace as the distinction between them seems to have been blurred. Ukraine demonstrates just how thin the line is and serves as a reminder that the status quo is never guaranteed. The Baltic States have been paying close attention to their Eastern neighbour and have been preparing for possible Russian intervention, whatever shape it may take. To prevent an attack, the Baltic States have put a lot of effort into improving their deterrent capabilities over the past few years.

Deterrence

Deterrence has been brought up countless times over recent years, most recently in relation to Russia and its revisionist behaviour in Ukraine. Essentially, deterrence means trying to prevent a conflict by convincing a potential adversary that the consequences of its actions, including retaliation, economic sanctions, political isolation, legal challenges or even military defeat, will outweigh the potential gains (Ducaru, 2016, p. 9), or that it will incur a higher loss or lower gain that would follow from avoiding an

***Corresponding author: David Takacs,** Associate Fellow at Slovak Security Policy Institute, Na vŕšku 8, 811 01 Bratislava, Slovak Republic, E-mail: david.takacs1@gmail.com

attack. The logic of deterrence, therefore, is to reduce the probability of an enemy attack (Snyder, 1961, p. 12). However, for deterrence to be effective it has got to be backed up by both political resolve and military capabilities (Anderson, Larsen and Holdorf; 2013, p. 7).

While the concept of deterrence is a rather broad one, there are two major ways in which it can be categorised. One of them is to differentiate between deterrence by denial and deterrence by punishment, where the former 'results from the capacity to deny territorial gains to the enemy' (Snyder, 1961, p. 14). The aggressor therefore chooses not to take action because the deterring country 'has taken, or will take, steps to ensure this action will fail to achieve its desired result' (Anderson, Larsen and Holdorf; 2013, p. 3). On the other hand, deterrence by punishment can be achieved through the threat of retaliation (Snyder, 1961, p. 14), which would make the adversary reconsider his attack due to the actions that would follow. However, as noted by Davis (2014, p. 4), concepts of denial and punishment do not stand alone and deterring an adversary should be viewed as a combination of the two. Another way of categorising deterrence is to differentiate between direct and extended deterrence. As described by Huth (1999, p. 27), 'a policy of deterrence can be directed at preventing an armed attack against a country's own territory (direct deterrence) or that of another country (extended deterrence)'. An example of direct deterrence would therefore be the Estonian armed forces trying to deter Russia from attacking Estonia, whereas extended deterrence would be foreign armed forces trying to prevent an attack on Estonia, such as the North Atlantic Treaty Organisation's (NATO) multinational battalions which are to be deployed in each of the Baltic States and Poland in early 2017.

The Russian threat

Russia and its revisionist behaviour present the Baltic States with a multitude of threats, making deterrence a top priority in the Baltic Region. Not only does Moscow wish to extend its sphere of influence to include what it describes as 'near abroad', it must carefully protect its own model of 'sovereign democracy' at home. Prior to Russian involvement, Ukraine was getting close to signing an association agreement with the European Union (EU) and it was feared that 'democratic change in brotherly Ukraine could spread to Russia'. Transforming Ukraine to a western democracy was seen as a threat to the Russian regime and was thus stymied at its source (Snegovaya, 2014). However, the Baltic States have already been fully integrated into NATO and the (EU) and have been stable democracies for over two decades now. So what is the nature of the threat that Russia presents to the Baltic States?

Putin is using hybrid tactics as a means of achieving his objectives of a politically restructured Europe. These include massive pro-Russian propaganda and misinformation campaigns, using economic levers, intimidation, or the employment of cyber warfare elements. In Ukraine in 2014, Russia has once again demonstrated its resolve to use both military and non-military means to create and fuel conflicts in pursuit of its wider geopolitical interests. The Kremlin is busily trying to regain its sphere of influence over nations that were formerly part of the Soviet Union, and the Baltic States' governments are continuously being reminded to stay alert. In addition, NATO frontier allies face much more significant threats due to their proximity to the potential aggressor (Grygiel and Mitchell, 2016, p. 166). Thus, what NATO needs most to deter Russia is 'to demonstrate robust political solidarity' within the alliance (NATO Parliamentary Assembly Report, 2015, pp. 4-6). There has been a significant increase in Russian probing activities to gauge NATO's commitment to the Baltic States over the past two years. Grygiel and Mitchell (2016, p. 43) define Russian probing as a 'low-intensity and low-risk test aimed at gauging the opposing state´s power and will to maintain security and influence over a region'. In case of the Baltic States, probing is aimed at the US and the strongest European countries, their power and their will to back up their most exposed allies. As mentioned by Grygiel and Mitchell (2016, p. 122), 'there is a strong correlation between the existence of alliances in a given region and the effectiveness of deterrence against a threatening power'. Building on the allies' fear of abandonment and US fear of entrapment in local conflicts, Russia is aiming to hinder their relationships which could ultimately provide Moscow with more room for probing and manoeuvring in the Baltic Region.

Hybrid or conventional?

A lot of attention has also been directed towards what approach Russia might take if it decides to launch an attack on the Baltic States and whether they would be able to employ the same hybrid strategy as they did in Ukraine. The term hybrid warfare, also called asymmetrical or non-linear warfare, has been brought up countless times since the Russian invasion of Ukraine in 2014. It has been defined as a ‘mixture of coercive and subversive activities, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare’ (European Commission, 2016b, p. 2). Essentially, this form of offensive can include various tactics aimed at influencing the decision-making processes, such as information campaigns or using proxy actors for certain tasks (NATO Cooperative Cyber Defence Centre of Excellence, 2016). In reality, any threat can be perceived as hybrid as long as it is not limited to a single element of warfare. Puyvelde (2015) explains that the term hybrid should not be overused as it might cause confusion instead of ‘clarifying the reality of modern warfare’. The word hybrid therefore does not truly differentiate one type of warfare from another, as the vast majority of (if not all) conflicts have utilised a multitude of forms and dimensions of warfare. NATO has already experienced this as well, as the Soviet Union used to create ‘grey zones of ambiguity surrounding the degree of its involvement’ in manipulating NATO members´ domestic issues (NATO Parliamentary Assembly Report, 2015, p. 3). Figure 1 shows changes in the character of armed conflict according to Valery Gerasimov, the Chief of Russia’s General Staff (2013).

Traditional Military Methods	New Military Methods
– Military action starts after strategic deployment (Declaration of War). – Frontal clashes between large units consisting mostly of ground units. – Defeat of manpower, firepower, taking control of regions and borders to gain territorial control. – Destruction of economic power and territorial annexation. – Combat operations on land, in the air and at sea. – Management of troops by rigid hierarchy and governance.	– Military action starts by groups of troops during peacetime (war has not been declared at all). – Non-contact clashes between highly manoeuvrable interspecific fighting groups. – Annihilation of the enemy’s military and economic power by short-term precision strikes on strategic military and civilian infrastructure. – Massive use of high-precision weapons and special operations forces, robotics, and weapons that use new physical principles (directed-energy weapons – lasers, shortwave radiation, etc.). – Use of armed civilians (4 civilians to 1 military). - Simultaneous strikes on the enemy’s units and facilities in all territories. – Simultaneous battle on land, in the air, at sea, and in cyberspace. – Use of asymmetric and indirect methods. – Management of troops in a unified informational sphere

Figure 1: Changes in the Character of Armed Conflict according to Gerasimov (2013).

It is clear that deterring hybrid elements of warfare requires a much different approach than that of deterring a conventional attack, including ‘increased resilience of cyber networks, diversification of energy supplies, and strategic communications that can rapidly correct false information spread by an opponent’ (Rühle, 2015). *Deterrence-by-resilience* has been suggested as a response to the Russian hybrid warfare strategy employed in Ukraine. This type of deterrence is meant to dissuade the aggressor by demonstrating the futility of its approach rather than by inflicting punishment upon it (Shea, 2016). In twenty-first century warfare it is inevitable to consider it a core element of a country’s deterrence capabilities of the same level of importance as conventional military deterrence measures.

Deterrence measures of Ukraine

It is clear that Ukraine has failed to deter Russia from aggressive behaviour, and there are several reasons for this. Firstly, let's examine the elements of hybrid warfare which were employed in Ukraine throughout the crisis. Russia has employed both an overt and covert military presence in the conflict, creating a rather confusing environment by using unmarked 'little green men' (Miller et al., 2015) on the 'battlefield'. Cyber-attacks were also employed, albeit as part of a broader strategy of information (or psychological) warfare. Propaganda and disinformation in the forms of pro-Russian and anti-Western attitudes are powerful psychological components which were used to divide Ukrainian society and change the general perception of ongoing events (Rogers and Tyushka, 2016). Digital propaganda, denial-of-service (DoS) campaigns, website defacements or information leaks were all used during the crisis for this purpose (Geers, 2015, p. 8). Finally, economic warfare was used to inflict various trade sanctions upon Ukraine. Consequently, Ukraine's gross domestic product contracted by around 16% between 2014 and 2015 (Aslund, 2015).

Self-evidently, Russia has launched its offensive on many fronts and Ukraine was unable to adequately respond to any of them. At the time of Russian involvement, Ukraine's military deterrence capabilities were solely dependent on its national army due to the lack of collective defence arangements with other countries and few effective resilience capabilities. An agreement which was supposed to keep Ukraine intact was the Budapest Memorandum from 1994 where Ukraine's territorial integrity was guaranteed by the United Kingdom, the US and Russia in exchange for its nuclear arsenal (Rogers and Martinescu, 2015, p. 15). Needless to say, Moscow has completely disregarded this in the pursuit of its geopolitical agenda. It is also important to note that whatever support Ukraine has received from other countries were only ad-hoc measures rather than structured deterrence mechanisms. Besides the clear advantage in size of the Russian military compared to that of Ukraine, there were several other factors present which resulted in Ukraine's inability to deter the Kremlin. According to an official from the Lithuanian Ministry of National Defence (2016), the Ukrainian army was in bad shape and nowhere near ready to go to war, both in terms of equipment and chain of command. Ambiguous rules of engagement, overlapping competences and severe corruption throughout the entire government were all contributing factors. As mentioned by Bulakh (2016), 'the Kremlin effectively exploited a number of vulnerabilities in Ukraine's societal cohesion, the lack of a nation-state narrative, corruption and weak government institutions, and a lack of trust and cooperation between the state and civil-society actors and citizens'. The lack of preparation for a stealthy incursion of the Russian army on its territory was met with certain legal constraints which made the situation even more difficult, such as the fact that the Ukrainian army could only be used against a foreign intruder. It was not a simple task to identify foreign military present at the time, as Russia had created a 'fog of war' with unclear participants. On top of this, the Kremlin's narrative regarding the protection of Russians abroad might have kept Ukraine in check in order not to give Russia a pretext to escalate its aggression (Rogers and Martinescu, 2015, p. 14).

There were several possibilities discussed in order to prevent the aggressive behaviour of Russia. For instance, it was suggested that Ukraine could cause great economic harm to Russia as half of its energy exports travel through Ukrainian pipelines, or that Ukraine could cut Crimea off from electricity, food and water supplies to deter further Russian belligerence. However, it is almost certain that none of these would have worked. Firstly, Russia has alternative routes for exporting its energy and Ukraine is heavily dependent on Russian pipelines anyway; secondly, cutting Crimea off could result in more aggressive actions from Russia as this 'new part of Russia' would now be directly threatened (Person, 2015). Regarding the threats from the EU and US about severe economic sanctions towards Russia, these were simply not perceived as harsh enough by the Kremlin. The potential gains for Moscow, i.e. preventing Ukraine from integrating further into European-, and potentially, the Euro-Atlantic structures, outweighed whatever economic losses Russia was going to incur. Therefore, Ukraine's inability to deter Russia resulted in the loss of Crimea.

Deterrence measures of the Baltic States

To begin with, there are several important differences between the Baltic States and Ukraine. Firstly, in light of Russia’s geopolitical belligerence in Ukraine, the Baltic States are well aware of the possibility of Russian aggression towards themselves; secondly, they have already experienced several elements of hybrid warfare. The point could be made that the Baltic States have even been experiencing elements of hybrid warfare since regaining their independence in 1991 due to constant pro-Russian propaganda in the region. Furthermore, since the collapse of the Soviet Union, Russia has attempted to affect policy changes in the Baltic Region in the form of gas supply cut-offs (Smith, 2004, p. 1), or, more recently, the Russian cyber-attack on Estonia in 2007. These two points clearly differentiate between the preparedness of Ukraine and the Baltic States.

In terms of deterrence measures, the Baltic States have much more to offer than Ukraine, especially since 2014, as they have put a lot of effort into strengthening their capabilities. There have been changes on the national, regional and NATO & EU levels as well. On the national level, Lithuania has reintroduced conscription and amended its legislation to allow the use of armed forces during peacetime to shorten reaction times in case of an attack (Szymański, 2015, pp. 1-5). Similarly, Latvia has amended a national security law which gives the commanders of particular units rights and obligations to act without prior political agreement to allow for quicker reactions (Representative from the Latvian Ministry of Defence, 2016). There have been developments in terms of cyber-security as well, such as Estonia integrating cyber-defence into its compulsory military service and the establishment of a cyber-command which is currently awaiting the government’s approval (Pernik, 2016). Other measures include increased military expenditures to accelerate the modernisation of the armed forces, as well as raising the combat readiness of certain units and the modernisation of training scenarios to include elements of hybrid warfare (Szymański, 2015, pp. 1-5).

In terms of regional cooperation, there have been several military projects created in the Baltic States since they regained their independence in 1991 to improve their defence capabilities. These include the Baltic Peacekeeping Battalion (BALTBAT), the Baltic Naval Squadron (BALTRON), the Baltic Air Surveillance Network (BALTNET), the Baltic Security Assistance Group (BALTSEA) and the Baltic Defence College (BALTDEFCOL) (Ito, 2013, p. 246). Furthermore, Lithuania, Latvia and Estonia hold regular meetings on several levels with plans to strengthen this cooperation over the coming years and there is also an information exchange channel – used daily – for intelligence sharing amongst the Baltic States (Representative from the Latvian Ministry of Defence, 2016). While these are steps in the right direction towards confirming the direct deterrent of the Baltic States, they cannot by themselves be viewed as a credible deterrent against an adversary as powerful as Russia.

The backbone of deterrence of the Baltic States is their NATO membership. Since 2004, the Baltic States have enjoyed the security provided by NATO’s Article 5 in relation to collective defence. However, after the events in Ukraine in 2014 and increased Russian probing activity in the Baltic Region, NATO has significantly improved its deterrent posture on the Eastern Flank. There have been two large NATO Summits since the annexation of Crimea, both of which have introduced significant changes regarding NATO’s deterrent posture in the Baltic Region. The NATO Wales Summit in 2014 resulted in a Readiness Action Plan (RAP), which provides an initial answer to the ‘challenges posed by Russia and their strategic implications’ (NATO, 2014). It comprises both adaptation measures, which are changes to NATO’s long-term military posture and capabilities, and assurance measures, namely an immediate increase in the military presence on the Eastern Flank (NATO, 2015a). As part of the RAP measures, the NATO Response Force (NRF) has been improved by creating the Very High Readiness Joint Task Force (VJTF) within it. The NRF consists of about 40,000 personnel, 5,000 of which will be part of the VJTF and will be capable of deploying within 2-3 days (NATO, 2016b). Furthermore, a NATO Force Integration Unit (NFIU) has been established in each of the Baltic States to ‘support collective defence planning and assist in coordinating training and exercises’ (NATO, 2015b, p. 2).

During the latest NATO Summit in Warsaw, further modifications were made to the alliance’s deterrent posture in the Baltic Region. NATO has pledged to increase its forward presence on the Eastern Flank by positioning one battalion in each of the Baltic States and Poland starting in early 2017 (NATO, 2016a). These battalions will comprise multinational forces with emphasis being placed on the rotation of forces in order not to violate the NATO-Russia Founding Act of 1997, which states: ‘NATO reiterates that in the current and foreseeable security environment, the alliance will carry out its collective defence and other missions by ensuring the necessary interoperability, integration, and capability for reinforcement rather than by additional permanent stationing of substantial combat forces’ (NATO-Russia Council, 1997, p. 14). Even though Russia has unilaterally and forcefully altered the security environment, the rotation of forces ensures that NATO continues to uphold the agreement, as they are not permanently stationed. Having combat-ready battalions present in the region is a major shift from the past. Even though there were foreign soldiers present in the Baltic States, their numbers were significantly fewer and they never formed an entire ‘package’ including enablers – which these battalions will contain. Not only is this a clear sign that the Baltic States have the alliance’s full support, it is also a message to Russia that an attack on the Baltic Region will quite literally be an attack on all. When calculating potential gains and losses of an attack on the Baltic States, getting engaged with thousands of foreign troops suggests a rather weighty item in the ‘potential losses’ column. While retaliation resulting from the deaths of a small number of foreign troops could have been questionable, it is unthinkable that the obliteration of a battalion-sized unit – some backed by nuclear powers – would not be met with a massive response.

In addition, there have also been some significant improvements related to overcoming hybrid elements of warfare. When talking about ‘deterrence-by-resilience’, Shea (2016) outlined seven basic requirements, which cover the entire spectrum of the crisis – from evolving hybrid threats to the worst possible scenarios. The requirements are the following:

1. Assured continuity of government and critical government services;
2. Resilient energy supplies;
3. Ability to deal effectively with the uncontrolled movement of people;
4. Resilient food and water resources;
5. Ability to deal with mass casualties;
6. Resilient communications systems; and finally
7. Resilient transportation systems.

In part due to the initiatives of the Baltic States, these are now being addressed on both the EU and NATO levels. The EU has recently introduced a Joint Framework to improve the resilience of EU Member States while increasing cooperation with NATO on countering hybrid threats. Even though countering these types of threats is primarily the responsibility of Member States, the Joint Framework helps in the process by combining national and European instruments more effectively. The EU Joint Framework proposes operational actions aimed at raising awareness, building resilience, preventing crises, responding to crises and recovering & stepping up the cooperation between the EU and NATO as well as other partner organisations (European Commission, 2016a). The timeframe for the implementation of these measures is largely dependent on EU Member States. It should, however, be one of the top priorities in the most exposed regions such as in the Baltic States.

One of the most significant instruments regarding hybrid threats will be the EU Hybrid Fusion Cell. The aim of this will be to ‘receive, analyse and share classified and open source information specifically relating to indicators and warnings concerning hybrid threats’ from various stakeholders (European Commission, 2016b, p. 4). Furthermore, National Contact Points will be established by Member States to cooperate and communicate with the EU Hybrid Fusion Cell; equally, staff of the EU Hybrid Fusion Cell will be trained to recognise early hybrid threat signs. Another measure seeks to develop a strategic communication strategy: preventing and countering disinformation is crucial as ‘providing swift factual responses and raising public awareness about hybrid threats are major factors for building societal resilience’ (European Commission, 2016b, p. 4). Finally, the EU is looking to establish a Centre of Excellence to focus on researching hybrid threats and ensuring that decision-making is well informed with regard to the complexities and ambiguities associated with hybrid threats (European Commission, 2016b, p. 5). The EU Joint Framework also mentions increasing cooperation with NATO to be better prepared to face and respond to hybrid threats in a complementary manner. This would involve sharing analyses and best practices and liaising with the EU Hybrid Fusion Cell and NATO´s Hybrid Fusion Cell (European Commission, 2016b, p. 17).

To further enhance resilience, the EU emphasises protecting critical infrastructure which is vital in preventing economic or societal disruption. This includes diversifying EU’s energy sources, suppliers and routes, but also increasing the resilience of nuclear infrastructures by promoting safety and security standards (European Commission, 2016b, p. 6). Furthermore, the EU is improving its legislation and processes to enhance the protection of transport and supply chains (airports, road infrastructure, ports, etc.), increase the resilience of space infrastructure, strengthen defence capabilities (e.g. surveillance and reconnaissance capabilities) and protect public health and food security. Cybersecurity is another vital element of building resilience as the vast majority of services across the EU can be subject to a cyber-attack. A cyber-attack can trigger an Article 5 response, however, NATO’s mandate with regard to cybersecurity is strictly defensive and its role is to protect the networks of the alliance and its allies. It is essential to protect NATO’s Information Technology infrastructure to ‘fulfil NATO’s core tasks, maintain its technical edge and ensure its capabilities work as an integrated whole in the 21st century, where information warfare is a 24/7 battle’ (Fertasi and Vivo, 2016). The NATO Cooperative Cyber Defence Centre of Excellence is an international military organisation with the mission to enhance the capability, cooperation and information sharing ability of NATO, its member countries and partners in terms of cyber defence. Meanwhile, the EU Joint Framework on countering hybrid threats further considers improving cybersecurity resilience in terms of energy, financial systems, transport, hybrid threat financing, resilience against radicalisation and violent extremism, and cooperation with third-party countries (European Commission, 2016b, p. 10).

Challenges

While the Baltic States, the EU and NATO seem to have been strengthening every aspect of their deterrence capabilities, there are still many challenges ahead. According to an official from the Lithuanian Ministry of National Defence, most of their attention should be directed towards an enhanced forward presence in the region its implementation, sustainability and role within the overall defence plans. While the NATO battalions provide a significant increase in terms of combat-ready land forces, Praks (2016) suggests that similar steps regarding naval and air forces should follow to further increase the deterrent effect. Furthermore, as NATO is a multinational organisation, its decision-making processes can be rather lengthy. The challenge for the future is to shorten them as much as possible to allow prompt reactions by the alliance as one of the major lessons learned from Ukraine is the need to be decisive and act quickly. To make the most of the armed forces present in the region, the rules of engagement in case of an attack should be perfected, including the logistics and lines of command, a process that is currently underway. However, this is not a national matter and requires strong NATO involvement (Official from the Lithuanian Ministry of National Defence, 2016).

Should Russia adopt the same approach towards the Baltic States as it used in Ukraine, it would in all likelihood not be as successful as a hybrid approach would allow for the country under attack (which is always the first responder) and the Alliance to mobilise itself and disrupt any potential threats (Praks, 2016). However, this idea presumes the ability to identify any emerging threat from its earliest stages, which is currently lacking. The EU Hybrid Fusion Cell is addressing this issue directly by providing a platform to share and analyse intelligence, as well as by having staff trained to recognise early signs of hybrid threats. The establishment of this mechanism is currently ongoing; however, one of the greatest challenges will be the successful implementation of the goals set out in the EU Joint Framework by EU Member States into their legislation (European Commission, 2016b, p. 18). As far as conventional attacks go, snap exercises occurring in close proximity to the borders of the Baltic States should not be underestimated. Since 2014 there has been a notable increase in unannounced Russian snap exercises of significant sizes near the borders of the Baltic States (Hurt, 2016, p. 38). These exercises sometimes consist of as many as 45,000 troops and could be used to create a new state of normality. Then, once the alliance no longer sees snap exercises as something extraordinary, they might be used to launch a surprise attack.

Furthermore, the Russian speaking population is a potential vulnerability which should not be overlooked, even though there is a significant difference between the Russian minority in the Baltic States and in Ukraine. Even though parts of the Russian minority do not enjoy the same rights as Estonian or Latvian citizens, including restricted political rights (Cianetti, 2014, p. 86), their living standards are still significantly higher than those of Russian speakers in Ukraine, or even those in Russia itself. Only a small minority of them are considered to be radical and according to a representative from the Latvian Ministry of Defence, they are not thought of as a threat. However, it is essential that pro-Russian propaganda and disinformation is constantly countered and objective information is available to all. Certain measures to make the minority feel more included have already been taken, e.g. by redistributing much of Riga's budget to be invested in the easternmost part of Latvia where the majority of the Russian-speaking population is situated, or plans to establish a Russian-speaking television network across the Baltic Region (Representative from the Latvian Ministry of Defence, 2016).

Given the broad spectrum of elements that twenty-first century warfare presents us with, it is essentially impossible to succeed in deterring it completely. The Baltic States must work diligently to successfully implement the features of the EU Joint Framework on countering hybrid threats in their legislation and continuously keep improving their own processes and capabilities, both nationally and within the region. What the alliance needs to do is to show unconditional support towards all its members and thus erase any doubts concerning NATO's stability, especially in terms of the current situation regarding the question mark surrounding the direction of US foreign policy during the coming administration of Donald Trump. If these conditions are met, the Baltic States will be a very hard puzzle to solve for Russia, whichever approach it might choose.

Conclusion

Ukraine's lack of collective defence treaties and no resilience capabilities on the one hand and the NATO membership of the Baltic States on the other are the seemingly obvious reasons as to why Ukraine has not been able to deter Moscow while the Baltic States have been successful so far. The alliance provides them with a powerful extended deterrent through the possibility of activating Article 5, and a shift towards accommodating all aspects of non-linear warfare by NATO is currently ongoing to cover the entire spectrum of potential threats. While this has indeed been the most significant difference between Ukraine and the Baltic States, there are more contributing factors including the previous experiences of the Baltic States in dealing with elements of hybrid warfare or their anticipation of belligerent Russia, which has also fueled regional cooperation. While the gap in terms of deterrent capabilities between Ukraine and the Baltic States was already quite significant back in 2014, it has been widening continuously ever since as the Baltic States, the EU and NATO focus on improving their military and non-military deterrence measures and related processes.

References

Anderson, J., Larsen, J. and Holdorf, P. (2013). *Extended Deterrence and Allied Assurance: Key Concepts and Current Challenges for U.S. Policy*. [online] Colorado: USAF Institute for National Security Studies at the USAF Academy, Available at: http://www.usafa.edu/df/inss/OCP/OCP69.pdf [Accessed 3 Nov. 2016].

Aslund, A. (2015). *Russia's War on Ukraine's Economy.* [online] Project Syndicate, Available at: https://www.project-syndicate.org/commentary/russia-war-on-ukraine-economy-by-anders-aslund-2015-07?barrier=true [Accessed 3 Nov. 2016].

Bulakh, A. (2016). *Defining Ukraine’s National Resilience in Light of Non-linear Threats: Where to Start?* [online] International Centre for Defence and Security, Available at: http://www.icds.ee/blog/article/defining-ukraines-national-resilience-in-light-of-non-linear-threats-where-to-start/ [Accessed 25 Dec. 2016].

Cianetti, L. (2014). Granting Local Voting Rights to Non-Citizens in Estonia and Latvia: The Conundrum of Minority Representation in Two Divided Democracies. *Journal on Ethnopolitics and Minority Issues in Europe,* Vol. 13 (Issue 1), [online] Available at: http://www.ecmi.de/fileadmin/downloads/publications/JEMIE/2014/Cianetti.pdf [Accessed 30 Jan. 2017], pp. 86-112.

Davis, P. (2014). *Toward Theory for Dissuasion (or Deterrence) by Denial: Using Simple Cognitive Models of the Adversary to Inform Strategy*. [online] Available at: http://www.rand.org/content/dam/rand/pubs/working_papers/WR1000/WR1027/RAND_WR1027.pdf [Accessed 20 Oct. 2016].

Ducaru, S. (2016). Framing NATO´s Approach to Hybrid Warfare. In: N. Lancu, A. Fortuna, C. Barna and M. Teodor, ed., *Countering Hybrid Threats: Lessons Learned from Ukraine*, 1st ed., Amsterdam: IOS Press BV, pp. 3-11.

European Commission, (2016a). *Security: EU strengthens response to hybrid threats.* [online] Available at: http://europa.eu/rapid/press-release_IP-16-1227_en.htm [Accessed 2 Nov. 2016].

European Commission, (2016b). *Joint Framework on countering hybrid threats: A European Union response.* [online] Available at: http://data.consilium.europa.eu/doc/document/ST-7688-2016-INIT/en/pdf [Accessed 2 Nov. 2016].

Fertasi, N. and Vivo, D. (2016). *Cyber resilience: protecting NATO’s nervous system.* [online] NATO Review magazine. Available at: http://www.nato.int/docu/review/2016/Also-in-2016/nato-cyber-resilience-security/EN/index.htm [Accessed 4 Dec. 2016].

Geers, K. (2015). Foreword. [online] In: K. Geers, ed., *Cyber War in Perspective: Russian Aggression against Ukraine*, Tallinn: NATO CCD COE Publications, pp. 8-9. Available at: https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf [Accessed 3 Dec. 2016].

Gerasimov, V. (2013). Новые вызовы требуют переосмыслить формы и способы ведения боевых действий, *Военно-промышленный курьер*, No. 8 (476). [online] Available at: http://www.vpk-news.ru/articles/14632 [Accessed 2 Dec. 2016].

Grygiel, J. and Mitchell, A. (2016). *The Unquiet Frontier: Rising Rivals, Vulnerable Allies, and the Crisis of American Power.* New Jersey: Princeton University Press.

Hurt, M. (2016). Preempting Further Russian Aggression Against Europe. *The Heritage Foundation*. [online] Available at: https://s3.amazonaws.com/ims-2016/PDF/2016_Index_of_US_Military_Strength_ESSAYS_HURT.pdf [Accessed 2 Nov. 2016].

Huth, P. (1999). Deterrence and International Conflict: Empirical Findings and Theoretical Debates. *Annual Review of Political Science,* 2, pp. 25-48.

Ito, P. (2013). Baltic Military Cooperative Projects: A Record of Success. In: T. Lawrence and T. Jermalavičius, ed., *Apprenticeship, Partnership, Membership: Twenty Years of Defence Development in the Baltic States*, 1st ed. Tallinn: International Centre for Defence Studies, pp. 246 – 281.

McDermott, R. (2014). Putin Orders Largest Snap Inspection Exercise of the Year. *Eurasia Daily Monitor*, Vol. 11 (Issue 162). [online] Available at: https://jamestown.org/program/putin-orders-largest-snap-inspection-exercise-of-the-year/ [Accessed 12 Oct. 2016].

Miller, J., Vaux, P., Fitzpatrick, C. and Weiss, M. (2015). An Invasion by Any Other Name: The Kremlin’s Dirty War in Ukraine. *The Interpreter.* [online] Available at: http://www.interpretermag.com/wp-content/uploads/2015/09/IMR_Invasion_By_Any_Other_Name.pdf [Accessed 3 Nov. 2016].

NATO, (2014). *Wales Summit Declaration*. [online] Available at: http://www.nato.int/cps/en/natohq/official_texts_112964.htm [Accessed 20 Oct. 2016].

NATO, (2015a). *NATO’s Readiness Action Plan*. [online] Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_05/20150508_1505-Factsheet-RAP-en.pdf [Accessed 20 Oct. 2016].

NATO, (2015b). *NATO Force Integration Units.* [online] Available at: http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2015_09/20150901_150901-factsheet-nfiu_en.pdf [Accessed 20 Oct. 2016].

NATO, (2016a). *Warsaw Summit Communiqué*. [online] Available at: http://www.nato.int/cps/en/natohq/official_texts_133169.htm [Accessed 15 Oct. 2016].

NATO, (2016b). *NATO Response Force.* [online] Available at: http://www.nato.int/cps/en/natohq/topics_49755.htm [Accessed 8 Nov. 2016].

NATO Cooperative Cyber Defence Centre of Excellence, (2016). EU Policy on Fighting Hybrid Threats. [online] Available at: https://ccdcoe.org/eu-policy-fighting-hybrid-threats.html [Accessed 9 Nov. 2016].

NATO Parliamentary Assembly Report, (2015). Hybrid Warfare: NATO´s New Strategic Challenge? No. 03/15. [online] Available at: http://www.ndc.nato.int/news/news.php?icode=814 [Accessed 20 Oct. 2016].

NATO–Russia Council, (1997). *Founding Act on Mutual Relations, Cooperation and Security Between NATO and the Russian Federation*. [online] Available at: http://www.nato.int/nrc-website/media/59451/1997_nato_russia_founding_act.pdf [Accessed 20 Oct. 2016].

Official from the Lithuanian Ministry of National Defence, (2016). Interviewed by David Takacs, 26 Oct. 2016.

Pernik, P. (2016). *CyCon 2016 and NITEC2016: NATO's Cyber Defence Post-Warsaw.* [online] International Centre for Defence and Security, Available at: http://www.icds.ee/blog/article/cycon-2016-and-nitec2016-natos-cyber-defence-post-warsaw/ [Accessed 05 Dec. 2016].

Person, R. (2015). Ukraine and The Limits of Deterrence. [online] Vox Ukraine, Available at: http://voxukraine.org/2015/07/23/ukraine-and-the-limits-of-deterrence_eng/ [accessed 12 Oct. 2016].

Praks, H. (2016). Interviewed by David Takacs, 1 Nov. 2016.

Puyvelde, D. (2015). *Hybrid war – does it even exist?* [online] NATO Review magazine, Available at: http://www.nato.int/docu/Review/2015/Also-in-2015/hybrid-modern-future-warfare-russia-ukraine/EN/index.htm [Accessed 20 Oct. 2016].

Representative from the Latvian Ministry of Defence, (2016). Interviewed by David Takacs, 21 Nov. 2016.

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

Rogers, J. and Tyushka, A. (2016). Russia's "Anti-hegemonic" Offensive: A New Strategy in Action. *Diplomaatia*, No. 160, [online] Available at: http://www.diplomaatia.ee/en/article/russias-anti-hegemonic-offensive-a-new-strategy-in-action/ [accessed 23 Dec. 2016].

Rühle, M. (2015). Deterrence: what it can (and cannot) do. [online] NATO Review magazine, Available at: http://www.nato.int/docu/Review/2015/Also-in-2015/deterrence-russia-military/EN/index.htm [accessed 28 Oct. 2016].

Shea, J. (2016). *Resilience: a core element of collective defence.* [online] NATO Review magazine, Available at: http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm [Accessed 20 Oct. 2016].

Smith, K. (2004). *Russian Energy Politics in Poland, Ukraine and the Baltic States.* [online] Available at: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/041019_smith_presentation.pdf [Accessed 20 Oct. 2016].

Snegovaya, M. (2014). Ukraine's Crisis Is Not the West's Fault. *The Moscow Times.* [online] Available at: https://themoscowtimes.com/articles/ukraines-crisis-is-not-the-wests-fault-39411 [Accessed 9 Nov. 2016].

Snyder, G. (1961). *Deterrence and Defense: Toward a Theory of National Security*. New Jersey: Princeton University Press.

Szymański, P. (2015). Between continuation and adaptation: The Baltic States' security policy and armed forces. *Ośrodek Studiów Wschodnich*, Volume 190. [online] Available at: https://www.osw.waw.pl/en/publikacje/osw-commentary/2015-11-24/between-continuation-and-adaptation-baltic-states-security [Accessed 8 Nov. 2016].