ISSN 2335-870X

sciendo LITHUANIAN ANNUAL STRATEGIC REVIEW
2017-2018 Volume 16

***Eitvydas Bajarūnas*[*], *Vytautas Keršanskas*[**]**
General Jonas Žemaitis Military Academy of Lithuania[***]

Hybrid Threats: Analysis of Content, Challenges Posed and Measures to Overcome[****]

The study analyses, in both theoretical and practical aspects, the topic of hybrid warfare and threats that have become particularly relevant after Russia's war in Ukraine. First, the authors examine the theoretical debates, concerning the definition of hybrid threats by singling out its main elements and estimating, on their basis, the definitions used by the European Union and NATO. Second, on the grounds of examples of the Baltic states and specifically of Lithuania, the article presents practical challenges related to hybrid threats and posed by Russia. Finally, the study surveys the decisions taken during recent years at the level of Lithuania, the European Union, and NATO with the exception of essential measures in fighting against hybrid threats.

Introduction

The term "hybrid", that became relevant after Russia's illegal annexation of the Crimea and its continued aggression in Eastern Ukraine, turned essential in conceptualizing modern warfare and threats. A somewhat new paradigm emerged in defining anew the threats that the European security architecture is facing. Yet, in spite of great interest in this topic, many theoretical and practical challenges remain unsolved.

[*] *Eitvydas Bajarūnas* – Ambassador at large, Ministry of Foreign Affairs of the Republic of Lithuania. Address for correspondence: J.Tumo-Vaižganto 2, LT-01511 Vilnius, Lithuania, tel. +370 5 236 2444, e-mail:. eitvydas.bajarunas@urm.lt.
[**] *Vytautas Keršanskas* – Deputy Director and Policy Analyst of the Eastern Europe Studies Centre. Address for correspondence: D. Poškos g. 59, LT-08114 Vilnius, Lithuania, tel. +370 5 270 59 93, e-mail: vytautas.kersanskas@eesc.lt.
[***] This study was commissioned by the General Jonas Žemaitis Military Academy of Lithuania. Contract nr. 8P-3, 13 November 2017.
[****] Assessments and views expressed in the article are exceptionally those of the authors and can never be treated as the official position of the Ministry of Foreign Affairs of the Republic of Lithuania or its subunits.

DOI: 10.2478/lasr-2018-0006

The phenomenon of asymmetrical, non-military, and mixed fighting attracted attention much earlier. It suffices to recall the continued antagonism between Israel and Hezbollah, Russian-Chechen wars, the confrontation going on in Afghanistan, or ISIS/DAESH activities – all these unconventional conflicts correspond to the existing definitions of hybrid warfare. In addition to these, the term "political warfare" that has some similarities with hybrid warfare also plays a part in theoretical debates.[1] In order to explain non-military measures, there exists a four-decades-ago-developed concept of "soft power" that is an important pillar of the foreign and security policy of Western countries.[2] Meanwhile, the USSR worked out its own means of influence, such as ideological fighting, propaganda, agitation, deception, "reflexive control", and "active measures" (rus. *активные меры*), developed specifically by the KGB and taken over, at least partly, by Russia. The elements of all these concepts are also part and parcel of the discussions concerning hybrid warfare.

Warfare or confrontation while employing non-military means, is, as well, deep-rooted; however, Russian intervention in Ukraine distinguished itself by an exceptionally wide employment of these means. Instead of an obvious enemy, "little green men" without insignia conducted operations. Ukraine suffered diplomatic, energy-related and economic pressure, unprecedented informational impact, cyberattacks, and actions by special operations forces. Eventually, these actions turned into conventional military actions. These developments are well described in studies by Evgen Dykyi,[3] Evgenij Magda,[4] and others.

Responding to new circumstances, the academics community of and analysts split into supporters and sceptics of hybrid warfare as a new type of warfare. Roger McDermott called hybrid warfare a myth,[5] while Michael Koffman and Mathew Rojansky stated that hybrid warfare cannot replace the perception of traditional warfare and might only explain the dissemination of Russia's influence.[6] In the opinion of Mary Ellen O'Connell, in the history of

[1] Hoffman F., „On Not-So-New Warfare: Political Warfare vs Hybrid Threats", July 28, 2014, https://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybrid-threats/, 2017 10 02.
[2] Jones S., „Understanding Soft Power in U.S. Foreign Policy", June 15, 2017, https://www.thoughtco.com/soft-power-in-u-s-foreign-policy-3310359, 2017 10 02.
[3] Dykyi E., *The 'hybrid war' of Russia: experience of Ukraine for the Baltic States*. Vilnius: The General Jonas Žemaitis Military Academy of Lithuania, 2016.
[4] Магда Е., *Гибридная агрессия России: Урок для Европы*, Киев: Каламар, 2017.
[5] McDermott R., „Does Russia's 'Hybrid War' Really Exist?", *Eurasia Daily Monitor*, Vol. 12, Issue 103, June 3, 2015, https://jamestown.org/program/does-russias-hybrid-war-really-exist/, 2017 10 02.
[6] Kofman M., Rojansky M., „A Closer Look at Russia's "Hybrid War", *Kennan Cable*, No. 7, April 2015, https://www.wilsoncenter.org/sites/default/files/7-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf, 2017 10 03.

the 20th century, one might find many examples of analogous warfare; therefore, the events in Ukraine are not an example of a new kind of warfare.[7] Eventually, Bettina Renz and Hanna Smith also emphasized that such an analytical tool is defective in order to estimate threats posed by Russia as it narrows the approach and thus might serve the aggressor himself.[8]

Nonetheless, the concept of hybrid warfare and threats attracted many supporters. Jury Raitasallo, though stating that as an analytical tool, this concept is limited since many of its elements are an "elementary, traditional" statecraft, still believed that it is necessary to return to the discourse the traditional perception of power in international relations, the perception that was forgotten in the security concept dominating in the West after the Cold War.[9] Alexander Lanoszka argued that the concept of hybrid warfare enables explaining, in the best way, Russia's ambitions in the post-soviet space in order to project the response of these countries and NATO to the evolving threats.[10] Christopher S. Chivvis underlined that, though hybrid threats are not new, Russia tailored them to the 21st century; therefore, the development of this concept is necessary to formulate a response.[11] Lithuanian authors Kęstutis Kilinskas[12] and Remigijus Žilinskas,[13] as well, put forward arguments and substantiated the relevance of the concept of hybrid warfare and also the Russian hybrid war's exceptionality, which is determined by the scope of Russia's power projection and the application of old methods in new ways, thus causing a threat to the functioning of states and national security.

In general, the concept of hybrid warfare refers to a much earlier developed concept of the fourth-generation war,[14] the essence of which lies in the manipulation of mass media, execution of acts of terrorism, absence of a

---

[7] O'Connell M. E., „Myths of Hybrid Warfare", *Ethics and Armed Forces*, No. 2, 2015, http://www.ethikundmilitaer.de/en/full-issues/20152-hybrid-warfare/oconnell-myths-of-hybrid-warfare/, 2017 10 03.

[8] Renz B., Smith H., „Russia and Hybrid Warfare – Going Beyond the Label", *Aleksanteri Papers*, No. 1, 2016, https://helda.helsinki.fi/bitstream/handle/10138/175291/renz_smith_russia_and_hybrid_warfare.pdf?sequence=1, 2017 10 03.

[9] Raitasallo J., „Getting a Grip on the So-Called "Hybrid Warfare", *ASPJ Africa & Francophonie*, 3rd quarter, 2017, p. 20-22, http://www.airuniversity.af.mil/Portals/10/ASPJ_French/journals_E/Volume-08_Issue-3/raitasalo_e.pdf.

[10] Lanoszka A., „Russian hybrid warfare and extended deterrence in eastern Europe", *International Affairs*, Issue 92, No. 1, 2016, http://www.alexlanoszka.com/LanoszkaIAHybrid.pdf, 2017 10 04.

[11] Chivvis C. S., „Understanding Russian "Hybrid Warfare" and What Can Be Done About It", *Testimony presented before the House Armed Services Committee*, March 22, 2017, https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT468/RAND_CT468.pdf, 2017 10 05.

[12] Kilinskas K., „ Hybrid Warfare: an Orientating or Misleading Concept in Analysing Russia's Military Actions in Ukraine? ", *Lithuanian Annual Strategic Review*, 2015-2016, vol. 14, p. 139-158.

[13] Žilinskas R., „Valstybės atsparumas išorinėms hibridinio pobūdžio grėsmėms: hipotetinis modelis", *Politologija*, Nr. 3 (87), 2017, p. 45-87.

[14] Williamson S., „From fourth generation warfare to hybrid warfare", US Army College, 2009.

clear hierarchy and structure of the enemy, employment of military, economic, financial, energy-related and social pressure measures, use of asymmetric tactics, and the implementation of combined and coordinated, overt and covert military, para-military and civilian measures. Taking advantage of the vulnerability of a country or region, the enemy performs these actions to affect or destabilize the adversary, hinder the process of decision-making and thus achieve the agreed tasks. The Ukrainian experience indicates that political and energy-related pressure, propaganda, and provocations might become a preparatory stage of conventional aggression.

On the other hand, in developing a new definition and its content, authors often encounter another extreme. The term "hybrid" is often used while attempting to define everything that takes place in a non-conventional form or is more difficult to define by using traditional terms, for example, attributing a single hacker attack or employees protesting because of social problems to hybrid actions.

With Russia continuing to pursue an aggressive policy directed against the West, the Baltic States are often defined as yet another potential object of Russia's hybrid actions. Therefore, for them, the term "hybrid" became relevant not only theoretically but also practically; not only as an academic but also as a strategic challenge.

In the absence of a completely precise definition or content of a hybrid threat, countries or their groups face a significant dilemma – how to fight against these types of threats, what measures to counter them with? Therefore, hybrid threats should be conceptualized from both the theoretical aspect and, resting on it, estimated from the point of view of practical-retaliatory actions.

Thus, while intensive debates on hybrid threats are still going on, the objectives of this article are: (1) to survey theoretical discussions on the definition of the concept of hybrid warfare and threats, as well as to single out the relevant definition; (2) to assess external influence measures used by Russia, their role in strategic documents, and the challenges posed by them to Lithuania, the European Union, and NATO; (3) to review and assess measures and actions of states, of the European Union and NATO in countering hybrid threats.

Having surveyed various scientific studies that researched hybrid warfare, the authors will name in the article the essential elements of hybrid warfare and, later, on their basis, will assess the concept of hybrid threats in the strategic documents of the European Union and NATO, as well as their application in Lithuania. Further, resting largely on the case of the Baltic States, the researchers

will present in detail the effect of Russia's hybrid influences. Finally, the authors will pay particular attention to fighting against hybrid threats: starting with the survey of theoretical means and finishing with the actions of Lithuania, the European Union, and NATO seeking to enhance resilience to hybrid threats.

1. The Definition of Hybrid Threats: From Theory to Practice

Traditional security studies divide aggressive actions into conventional and non-conventional warfare, though this division has always raised discussions because warfare, in a broad sense, has been perceived for more than 2,500 years – since the time of the Chinese thinker Sun Tzu. As well as warfare thinkers such as Thucydides or Carl von Clausewitz, who spoke about the employment of non-conventional means for the objectives of the state, and "practitioners" Lenin and Mao Tse-tung, who developed the concept "guerrilla war".[15] Therefore, in terms of purely theoretical conceptualization, present-day debates on hybrid warfare are neither new nor suggesting a qualitatively different attitude to warfare.

Still, the development of this concept is important in several ways. First, though pointing out that in the long term this may make the decision-making process more difficult, Antulio J. Echevarria states that new strategic concepts help direct decision-makers' attention to evolving new security challenges.[16] Second, Kęstutis Kilinskas maintains that the refinement of a hybrid warfare concept will help the community to understand modern threats better and states to prepare corresponding mechanisms for countering them.[17] Finally, this concept helps to seek a much more fundamental challenge – in Europe to "securitize" anew a traditional perspective of great powers in international relations, the perspective that was essentially renounced, particularly in the reasoning of West Europe, however, after the annexation of the Crimea, it again became particularly relevant.[18]

Keeping this in mind, theoretical debates on the definition of hybrid warfare and threats are more widely discussed, not in order to propose our

[15] See. Tse-tung M., „On Guerrilla Warfare", *Selected Works of Mao Tse-tung*, Vol. IX, 1937, https://www.marxists.org/reference/archive/mao/works/1937/guerrilla-warfare/index.htm, 2017 10 05.
[16] Echevaria A. J., *Fourth generaion warfare and other myths*, Carlisle, PA: Strategic Studies Institute, 2015, p. 16.
[17] Kilinskas, (footnote 12) p. 133.
[18] Raitasallo, (footnote 9) p. 20-21.

own, qualitatively new definition but rather refine the most important elements of hybrid warfare and, according to them, to assess the definitions used by Lithuania, the European Union, and NATO.

1.1. Theoretical Discourse on the Concept and Content of Hybrid Warfare

The annexation of Crimea carried out by Russia's military actions in Eastern Ukraine reminded the world that the concept of hybrid warfare has quite a few historical analogies. Historians compare this event with such 20th century processes as the annexation of Klaipėda by Nazi Germany,[19] the attempt by the USSR to launch a Bolshevik coup in Estonia in 1924,[20] or Lucjan Želigovsky's actions that predetermined the occupation of Vilnius area/territory in 1920.[21] What the Baltic States experienced during the Soviet annexation in 1940 – overt and covert diplomatic, economic and military operating of external forces,[22] as well as the activity of the USSR in international space (creating influence "networks" through political contacts, non-governmental organizations, movements, etc.) – essentially corresponds to modern definitions of hybrid warfare and are an important resource in understanding such operations better.

The concept of hybrid warfare seeks to define what is "in between" the concept of the conventional and unconventional warfare division (see Fig. 1). In the 21st century, the term "hybrid threat" was, for the first time, used by the US Department of Defense in the 2006 publication *Quadrennial Defence Review* and later repeated in 2010, as well as developed in US strategic military documents. Frank Hoffman was the first to start considering the modern concept of hybrid warfare and was one of the first authors predicting that, in

[19] Garškaitė R., „Istorikas: Krymo okupacija primena Klaipėdos krašto užėmimo scenarijų", 2014 11 21, http://lzinios.lt/lzinios/istorija/istorikas-kryma-rusai-uzeme-taip-pat-kaip-naciai-klaipedos-krasta/191628, 2017 10 05.

[20] Merle M, „Nothing new in hybrid warfare: The Estonian experience and recommendations for NATO", February 12, 2015, http://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato, 2017 10 06.

[21] Siekanski M., „Nasz polski Krym w dwdziestoleciu międzywojennym", *Gazeeta Baltycka*, 20 03 2014, http://gazetabaltycka.pl/promowane/nasz-polski-krym-w-dwudziestoleciu-miedzywojennym, 2017 10 07.

[22] See: Butkus Z., „SSRS Intrigos Baltijos šalyse 1920 – 1940", *Darbai ir dienos*, t. 8, 1998, p. 141 – 160; Butkus Z., „Vokietijos ir Sovietų diplomatijos poveikis Baltijos valstybių užsienio bei vidaus politikai 1920 –1940 m.", *Habilitacijos procedūrai teikiamų mokslo darbų apžvalga*, Vilnius, 2007; Švilpa J., „Komintermas irkomunistinis pogrindis Lietuvoje XX a. ketvirtajame dešimtmetyje (organizaciniai veiklos aspektai)", daktarodisertacija, Kaunas, 2007.

the future, the distinction between peace and war will be blurred. He defined such warfare as the ability of the adversary to employ, in the battlefield, conventional weapons, asymmetric actions, terrorism, and other means in order to achieve political aims.[23]

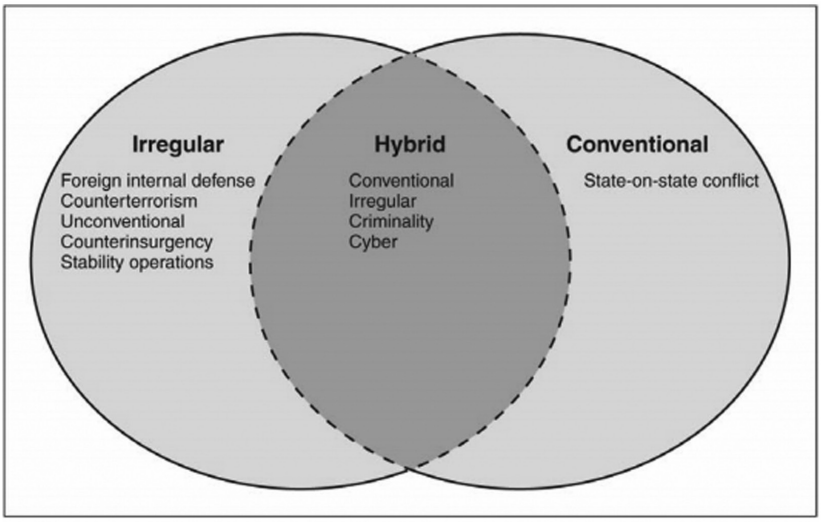

Figure1. **Visual concept of hybrid warfare[24]**

First, hybrid threats encompass elements of asymmetry and unexpectedness. As the previously mentioned Sun Tzu put it, "in war the best thing is to take the enemy's country whole and intact [...] and be able to subdue the enemy without fighting".[25] However, hybrid warfare might last a long time if its protraction is beneficial to the aggressor (example – "frozen conflicts" in the post-soviet space).

Another widely discussed element is the ambiguity of the conflict. According to Aapo Cederber and Pasi Eronen, "hybrid warfare intentionally blurs the distinction between the times of peace and war making it hard for the targeted countries to devise policy responses in a proper and timely manner".[26]

The term "grey zone" also refers to the ambiguity phenomenon caused

[23] Hoffman (footnote 1).

[24] Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Services, House of Representatives, Hybrid Warfare, 10 September 2010, http://www.gao.gov/new.items/d101036r.pdf, 2017 10 06.

[25] Tzu S., *The Art of War*, Chiron Academic Press, 2015.

[26] Cederber A., Eronen P., „How can Societies be Defended against Hybrid Threats?", *Strategic Security Analysis*, No. 9, 2015, p. 2, http://www.gcsp.ch/News-Knowledge/Publications/How-are-Societies-Defended-against-Hybrid-Threats, 2017 10 07.

by hybrid threats. In Martin N. Murphy's and Gary Schaub's opinion, "'grey-zone'" captures the orchestrated multidimensional nature of actions calibrated to gain specified strategic objectives without crossing the threshold of overt conflict and exploit Western concepts of war and peace as two distinct conditions".[27]

It is important to point out that though it is possible to use individual hybrid threats independently, hybrid warfare combines the employment of several or all elements symmetrically. A. Cederber and P. Eronen bring to light how hybrid warfare goes on symmetrically in all the stages (from the emergence of the political motive, granting of the mandate, to the implementation), together with the element of unexpectedness as well as using diversion and deception tactics.[28]

Timothy McCulloh and Richard Johnson, in their comprehensive study about hybrid threats, singled out principles that define the tactics of hybrid warfare. They argue that the use of hybrid force is tailored to a specific context defined by geographic, socio-cultural, current, and historical aspects. The internal hybrid force narrative is associated, through a certain ideology, with a strategic context, within which it is used.[29]

The main objectives of a hybrid operation are to identify vulnerabilities and weaknesses of the targeted country. The latter might be from any vitally important state or community area, i.e., the primary objective of the country employing hybrid means is to identify weaknesses of the target. For example, it was not Russia that "created" the United Kingdom's exit from the European Union, but Russia made use of hot discussions concerning the "Brexit" referendum in 2016 to strengthen the splitting of the community and bring chaos to the European political agenda. A migration card was taken advantage of in Germany – an anthology-worthy case of an allegedly raped Russian girl, Lisa, by Muslim migrants – when Russia attempted to exploit the Russian-speaking community, living in Germany and using Russian mass media, in order to provoke a wave of discontent and thus weaken the position of Chancellor Angela Merkel.[30] In the case of Sweden, attempts were made to "deal a blow" to Defen-

[27] Murphy M. N, Schaub G., „The Baltic: Grey-Zone Threats on NATO's Northern Flank", Center for International Maritime Security, March 29, 2017, http://cimsec.org/baltic-grey-zone-threats-natos-northern-flank/31529, 2017 10 07.

[28] Cederber, Eronen, (footnote 26) p. 3.

[29] McCulloh T., Johnson R., „Hybrid Warfare", Joint Special Operations University Report, No. 13-4, August 2013, http://www.dtic.mil/dtic/tr/fulltext/u2/a591803.pdf, p. 14-17.

[30] Rinke A., Carrel P., „German-Russian ties feel Cold War-style chill over rape case", *Reuters*, February 1, 2016, https://www.reuters.com/article/us-germany-russia/german-russian-ties-feel-cold-war-style-chill-over-rape-case-idUSKCN0VA31O, 2017 10 10.

ce Minister of Social Democrats' government Peter Hultqvist, a well-known critic of Russia, by making use of letters on supplying weapons to Ukraine allegedly written by him. In the case of Finland, "history" was resorted to, stating that social services of this country allegedly kidnap Russian-speaking children in order to "have fresh blood for the ageing community".[31]

During asymmetric, based on fraud and deceptive actions, the boundary between war and peace disappears. According to Aurel Sari, "war in a technical sense refers to a legal condition marked by certain formalities, such as the declaration of war. However, more often than not, states eschewed formal war in favour of engaging in warlike acts under another name".[32] This absence of a distinct boundary is achieved by employing various measures – both violent and non-violent, military and civilian – by planning them thoroughly in such a way as to avoid uselessly crossing "the red line", including the legal one. This also poses serious challenges in assessing conflicts through national or international law.

Comprehensive studies on the nature of hybrid threats continue. For example, recently a group of prominent international authors also proposed their list of hybrid tools[33] ranging from propaganda and fake news to strategic leaks (e.g. candidate Macron's emails leaked 48 hours before elections), funding organisations, political parties, organised protest movements, proxies, and unacknowledged war, etc.

1.2. The Concept of Hybrid Threats in the Strategic Documents of the European Union and NATO and Application in Lithuania

The definition of hybrid threats does not limit itself to the theoretical field. Both the European Union and NATO have consolidated, in their strategic documents, what they consider hybrid challenges. It is worth mentioning that this has been achieved due to the attempts of Lithuania and other Eastern European states, since these challenges are primarily associated with them.

[31] Rosendahl J., Forsell T., „Finland sees propaganda attack from former master Russia", *Reuters*, October 19, 2016, https://www.reuters.com/article/us-finland-russia-informationattacks/finland-sees-propaganda-attack-from-former-master-russia-idUSKCN12J197, 2017 10 15.

[32] Sari A., „Blurred Lines: Hybrid Threats and the Politics of International Law", *Strategic Analysis*, January 2018, p. 2, https://www.hybridcoe.fi/publications/strategic-analysis-january-2018-blurred-lines-hybrid-threats-politics-international-law/, 2017 10 20.

[33] Treverton G.F., Thvedt A., Chen A.R., Lee K., McCue M., "Addressing Hybrid Threats", Swedish Defence University, May 9, 2018, https://www.hybridcoe.fi/publication-tags/reports/.

In the Joint Communication of the European Union, adopted in 2016, the concept of hybrid threat is defined as

> the mixture of coercive and subversive activity, 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. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalize, recruit and direct proxy actors can be vehicles for hybrid threats.[34]

By the way, in official documents of the European Union, translated into the Lithuanian language, the term "mixed" instead of "hybrid" is used.[35]

The NATO definition of hybrid threats in Warsaw Summit Communique is almost identical, adopted in July 2016, it states that hybrid threats are "a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary, and civilian measures, employed in a highly integrated design by state and non-state actors to achieve their objectives".[36] Both these definitions correspond to the most important elements, singled out in the previous section; therefore, they will be used in further analysing both the impact of specific hybrid threats and discussing methods of fighting against them.

It is worth mentioning that the definition of "hybrid threats" has not been established in Lithuania at the national level; however, separate elements are identified in main documents related to national security.

In the Annual Assessment of Threats to the National Security, the two Lithuanian intelligence services, i.e. the State Security Department of Lithuania and the Second Operative Services Department under the Ministry of National Defense, claim that the primary threat to Lithuania's national security is caused by Russia's aggressive intentions and actions as well as Russia's objectives to change the global power balance and dominate in the self-attributed interest zone that includes the Baltic region. Russian intelligence services are particularly interested in the Lithuanian presidential elections in 2019. The major part of hostile activity in cyber space, ascertained in 2017, per-

---

[34] European Commission, Joint Communication to the European Parliament and the Council, Joint Framework on countering hybrid threats: a European Union Response, JOIN (2016) 18 final, 2016 04 06, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018&from=LT, 2017 10 20.

[35] Though in terms of the content it is not relevant, yet, in the sense of everyday use or perception, it would be worth considering whether such a term is more accurate or more convenient for general use.

[36] NATO, „Warsaw Summit Communiqué", Warsaw, July 9, 2016, https://www.nato.int/cps/en/natohq/official_texts_133169.htm, 2017 10 25.

tains to Russia. Russia operates against Lithuania using other means as well; for example, by pursuing aggressive informational and ideological policy and developing history policy projects. In 2017, Russia's propaganda mass media attention towards Lithuania kept growing. While preparing reports about Lithuania, Russian propagandists disguised genuine motives of the activity and would come to Lithuania using business or tourist visas, issued in some West European state. Through the informational space of social networks, Russia sought to spread anti-Western sentiments and form public opinion favourable to Russia. In 2017, Russia continued to strive for dominance in the energy market of the region and hinder its integration into the West European energy system. Belarus, in concert with the Russian corporation "Rosatom", accelerated the construction of the Ostrovets atomic power plant (further – AS). The dependence of Belarus on Russia is growing and remains a risk factor for Lithuania's national security. Further, the foreign and military policies of Belarus are closely coordinated with Russia.[37]

Consequently, the National Security Strategy of Lithuania, renewed in 2017,[38] points out these threats, dangers, and risk factors corresponding to the hybrid warfare elements singled out in the theoretical part: deceptive military and intelligence measures, threats to the unity of the Euro-Atlantic community, terrorism, extremism, radicalization, informational threats, cyber threats, economic and energy-related dependence, development of insecure nuclear energy along the borders of the Republic of Lithuania, corruption, and organized crime.

Although formal Lithuanian documents do not use the term "hybrid", in Lithuania it is used in the press, expert discussions, and the top command of the country. For example, speaking at the World Economic Forum in Davos at the beginning of 2018, President Dalia Grybauskaitė emphasized that the exercise "Zapad" clearly demonstrated that the country faces not only military but also hybrid threats. By the way, surveying hybrid threats, the president emphasized that "the nuclear power plant in Ostrovets might also be rereferred to as a non-conventional weapon".[39]

There are quite a few countries singling out new generation threats

[37] Valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie KAM, „Grėsmių nacionaliniam saugumui vertinimas", 2018, https://www.vsd.lt/wp-content/uploads/2018/03/LTU.pdf , 2017 03 26.

[38] Lietuvos Respublikos Seimas, „Nutarimas dėl Nacionalinio saugumo strategijos patvirtinimo", XIII-202, 2017 01 17, https://www.e-tar.lt/portal/lt/legalAct/TAR.2627131DA3D2/LLwfQepmnD, 2017 10 30.

[39] Stašaitytė V., „Grybauskaitė Davose dalyvavo diskusijoje apie Vidurio ir Rytų Europą", *Verslo žinios*, 2018 01 26, https://www.vz.lt/verslo-aplinka/2018/01/26/grybauskaitedavose-dalyvavo-diskusijoje-apie-vidurio-ir-rytu-europa#ixzz55Vzuw3rS, 2018 01 30.

which do not similarly use the term "hybrid". For example, the National Security Strategy of the United States of America[40], approved at the end of 2017, also addresses international criminal organizations and their secondary networks, cyber-attacks, purposeful assaults, accidents, natural disasters, upheavals, and threats to economy and democratic system. Although US scientists and military personnel take an active part in theoretical debates about hybrid warfare, this definition figures in official documents depending from the context. In Finland, the term "comprehensive security"[41] is used, though the threats under discussion correspond to the elements of hybrid threats. Meanwhile, the government of the Czech Republic adopted a new version of the Security Strategy of the country that includes a chapter on hybrid threats and priorities granted to them in the Strategy. In addition to that, the National Security Audit of the Czech Republic incorporates a chapter on hybrid threats[42]. Thus, the (non-)employment of the term "hybrid" at the national level pertains to different traditions and specific objectives of the security agenda rather than the essential mismatch of the content.

Summing up, the previously mentioned hybrid warfare elements, singled out in the theoretical field, are implemented through hybrid threats (influences), their manifestation forms:

- Absence of a clear hierarchy and structure of the enemy
- Propaganda and disinformation, manipulation of mass media
- Cyber attacks
- Espionage
- Psychological attacks
- Subversive activities
- Employment of culture, languages and religion by emphasizing differences
- Energy policy
- Influencing elections and political process
- Employment of criminal groups and organized crime
- Military pressure
- Coordinated activity of special forces, proxy groups, mercenaries, guerillas; combined and coordinated employment of overt and covert military, paramilitary and civilian means

[40] „National Security Strategy of the United States of America", December, 2017, p. 12-14, http://nssarchive.us/wp-content/uploads/2017/12/2017.pdf, 2017 11 05.
[41] The Security Committee, „Comperehensive Security", https://www.turvallisuuskomitea.fi/index.php/en/comprehensive-security, 2017 11 05.
[42] Zlatohlavek P., „Hybrid Warfare: A New Phenomenon in Europe's Security Environment", 2nd edition, Praha – Ostrava: Jaggelo 2000, 2016, p. 26, http://data.idnes.cz/soubory/na_knihovna/A161212_M02_029_HH16_PP-EN-V1.PDF, 2017 11 10.

- Employment of means of economic, financial, social pressure and asymmetric tactics
- Actions to exploit the vulnerability of a country or region in order to influence or destabilize the enemy, hinder decision making and thus achieve the set tasks
- All forms of fighting are integrated into one battlefield and take place simultaneously
- Creation of equivocation, ambiguity
- Avoidance of an open conflict when the aggressor is clearly identifiable
- Achievement of objectives by avoiding the declaration of war, attracting the least attention of the international community, reducing conflict costs to the maximum
- Nuclear blackmail that might be used having started a hybrid assault and achieved certain results in deterring the enemy from attempted active actions[43]

Later on, the consolidated information provided in this table will be helpful in analysing specific functioning of hybrid influences.

2. Operation of Hybrid Threats in the Case of Russia

Having discussed the issue of the definition of hybrid warfare and threats as well as its composing elements, the authors think it is important to link them to examples of specific hybrid influences carried out by Russia. Therefore, in this part, they will first review the main strategic documents of Russia and subsequently provide examples of Russia's hybrid influences encountered in Lithuania and other Baltic States.

2.1. Documents and Principles Defining Hybrid Operation of Russia

The concept of Russia's unconventional, asymmetric or "hybrid" warfare is presented by Chief of General Staff of the Russian Federation Armed Forces General Valery Gerasimov in an article published in 2013. Although there is no agreement as to whether the warfare concept called the "Gerasimov Doctri-

[43] Compiled by the authors on the grounds of the sources used in the study.

ne" by Western analysts exists in general[44], this article, nonetheless, reflects what the "ABCs" of hybrid operation cherished by Russia[45] are:

> The "rules of war" themselves have greatly changed. The role of non-military methods in seeking political and strategic objectives has increased and in certain cases have even well surpassed, due to their efficiency, an armed force. The essence of the employed confrontation methods is broad application of political, economic, informational, humanitarian and other non-military measures implemented by employing the potential of population protest. These measures supplement military means of covert nature including the implementation of the informational confrontation activity and actions of special operations forces. Taking into consideration an open use of force, by frequently employing peacekeeping and crisis management measures, only at a certain stage, mostly seeking ultimate success in a conflict.[46]

While assessing this concept, Jānis Bērziņš presents, in a scheme-like way, how Russia's military objectives have changed:

i. from direct destruction to direct influence;
ii. from direct annihilation of the opponent to its inner decay;
iii. from a war with weapons and technology to a culture war;
iv. from a war with conventional forces to specially prepared forces and commercial irregular groupings;
v. from the traditional (3D) battleground to information/psychological warfare and war of perceptions;
vi. from direct clash to contactless war;
vii. from a superficial and compartmented war to a total war, including the enemy's internal side and base;
viii. from war in the physical environment to a war in the human consciousness and in cyber-space;
ix. from symmetric to asymmetric warfare by a combination of political, economic, information, technological, and ecological campaigns;
x. From war in a defined period of time to a state of permanent war as the natural condition in national life[47].

---

[44] Eventually, the author of the term the "Gerasimov Doctrine" Mark Galeotti admitted that it is only one of Russia's principles of strategic operating and cannot be considered as the only form of the future warfare cherished by Russia. It is more an instrument of Western scientists for conceptualizing the theoretical and practical strategic thought of Russia. For more: Galeotti, M., „I'm Sorry for Creating the 'Gerasimov Doctrine", *Foreign Policy*, 5 March, 2018, http://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/.

[45]By the way, it should be noted that Russian official documents do not use the term hybrid threats or warfare. On the contrary, the term is applied by Russian officials and in their documents to characterize the operating of the West against Russia. See: Vanyna E., „Western-style hybrid war against Russia", *Business Report*, 4 December 2017, https://www.iol.co.za/business-report/opinion-western-style-hybrid-war-against-russia-12244594; BNS, „Rusija: JAV ir jų sąjungininkės vykdo hibridinį karą prieš NVS", 2017 12 19, http://kauno.diena.lt/naujienos/pasaulis/ekonomika-ir-politika/rusija-jav-ir-ju-sajungininkes-vykdo-hibridini-kara-pries-nvs-842686, 2017 12 25.

[46] Герасимов В., „Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий", *Военно-промышленный курьер*, 26 февраля 2013, https://www.vpk-news.ru/articles/14632, 2017 11 15.

[47] Bērziņš, J., „Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy", *Policy Paper, National Defence Academy of Latvia,* No. 2, April 2014, p. 5, http://www.naa.mil.lv/~/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx, 2017-11-20.

We see a clear shifting of Russia's strategic thought towards a major use of non-military methods. This approach is also interrelated with Russia's foreign policy concept[48] stipulating that the foreign policy of Russia be grounded on such modern methods and forms as economic diplomacy, global informational space, and the influence of the so-called "soft power". The renewed concept accentuates the necessity to protect the rights of the citizens of the Russian Federation and its compatriots abroad. The arsenal of unconventional methods is supplemented by the new Russia's information security concept[49] as well where information is defined as a type of warfare.

If hybrid influence measures employed by Russia are claimed to be nothing new, why this term became relevant only now? At least two characteristics of what we conceptualize as Russia's hybrid warfare make it possible to speak about the "novelty" of this type of warfare.

First, while carrying out hybrid activities, Russia successfully exploits, for its own purposes, the rights to openness and freedom of speech, granted by the democratic systems of Western states (representatives of Russia can freely operate and invest in Western countries), as well as globalization, and modern information technologies (the impact through social networks is rather cheap yet global). It is only now that the world begins to realize what changes have been introduced by practically total accessibility to big data and the possibility to use it by both governmental and non-governmental actors[50].

Besides, Russia's hybrid warfare is taking place not in a certain concentrated territory but throughout the entire Euro-Atlantic region (if previously the "targets" of Russia were states of the former USSR and the socialist bloc, nowadays hybrid operations go on in the United States, Germany, the United Kingdom, and elsewhere). Russia also manages to exploit certain weaknesses of Western societies, for example, the spreading of propaganda became possible due to the decrease in the confidence in democratic institutions and mass media.

---

[48] The Ministry of Foreign Affairs of the Russian Federation, „Foreign Policy Concept of the Russian Federation", 1 December 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2542248, 2017 11 15.

[49] The Ministry of Foreign Affairs of the Russian Federation, „Doctrine of Information Security of the Russian Federation", December 5, 2016, http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, 2017 11 15.

[50] During the time of the writing of this article, the case of notoriously known Cambridge Analytica came about , eg, "Cambridge Analytica, the shady data firm that might be a key Trump-Russia link, explained", https://www.vox.com/policy-and-politics/2017/10/16/15657512/cambridge-analytica-facebook-alexander-nix-christopher-wylie

Another important aspect is the fact that the National Defence Management Centre controls and coordinates the entire military activity concerning the use of force in Russia's region and abroad. It is a new coordination centre, established in 2014, that comprises the defence ministry of Russia and over 50 other "force" institutions, over a thousand officials and military personnel operating on the principle "24/7" in times of peace and war.[51] This is particularly important in analysing hybrid warfare and the employment of all aspects – military, intelligence, economic energy-related, etc.

In fact, in the case of the war in Ukraine, we witnessed an operation that was coordinated directly from Moscow. The President's Administration (most experts attribute the authorship of the Ukrainian operation ideology to V. Putin's close comrade-in-arms, Vladimir Surkov[52]) and the Kremlin have at their disposal the entire society of Russia (i.e. the Kremlin could easily manipulate and direct the emergence of the so-called various "volunteers", massive "support" events, and, certainly favourable to itself, mass media). The resources of all Russian institutions were coordinated from there and the preparation of the world opinion in advance was going on.

Russia's informational policy, that is a particularly important part of hybrid influences, is pursued in two directions: within the country, attempts are made to restrict to the maximum any alternative means of mass media so that the citizens could hear only the messages sent by the state-controlled or closely to the state related medias; according to the Kremlin "the only correct information". Meanwhile, abroad – both in the neighbourhood and in Western states – the Kremlin makes use of the fundamental principles of liberal democracy and presents lies and propaganda as an alternative position. As F. S. Hansen puts it, the main principle of Russia's disinformation strategy is to suggest the thought that all news are constructed and therefore debatable, that, in the post-modernist tradition, "objective information"[53] does not exist – only different competitive interpretations with the attempt to show them in different aspects that could be called reality. While using lobbyism and public rela-

[51] Gavrilov Y., „National Defence Management Centre established in Moscow", *Rossiyskaya Gazeta*, 04 11 2014, https://www.rbth.com/economics/2014/10/31/national_defence_management_centre_established_in_moscow_39483, 2017 11 20.

[52] Walker Sh., „Kremlin puppet master's leaked emails are price of return to political frontline", 26 10 2016, https://www.theguardian.com/world/2016/oct/26/kremlin-puppet-masters-leaked-emails-vladislav-surkov-east-ukraine, 2017 11 15.

[53] Hansen F. S., „Russian Hybrid Warfare", *DIIS REPORT*, No. 6, 2017, p. 10, http://pure.diis.dk/ws/files/950041/DIIS_RP_2017_6_web.pdf, 2017 12 04. p. 22.

tions agencies, Russia seeks to discredit the states in the international arena.[54]

Russia also supports European extremist groups, attempts to exploit the existing watersheds, and crisis-like situations both in states and at the level of the European Union and NATO. In the European context, Russia frequently supports various radical forces financially and in other ways in spite of their ideological direction, i.e. the forces might be both radical right- and radical left-wing movements and often establish deceptive non-governmental organizations.[55] Thus, the objective is to destabilize state societies from the inside.

Russia also widely employs other measures of hybrid influence: cyber activity, the displacement of the population in order to change the ethnic composition of the population in the frozen conflict region, employment of "proxy groups" (pseudo-NGO, youth organizations, think-tanks, expert groups, motorcycle clubs), cultural diplomacy, fostering of Russian culture abroad (it was for this purpose that the organization „Rossotrudnichestvo" (rus. *Россотрудничество*) was established), the policy of compatriots (justifying aggression against neighbouring countries, allegedly seeking to protect the rights of Russian-speaking population), etc.

The Danish researcher Fleming Splidsboel Hansen called the employment of several or all of these measures a "controlled chaos",[56] i.e. as if there existed some kind of "chaos button" that could be used in order to control the chaos level of some, most often geographically defined, entity. The objective is to cause and aggregate instability, weaken the social structure of society and encumber as well as undermine decision-making. This is the essence of hybrid tactics.

2.2. Russia's Actions towards the Baltic States

How does Russia specifically employs hybrid, asymmetric or non-military methods? Let us analyse this using the example of the Baltic States.

---

[54] Vaišnys A. *et al,* „Rusijos propaganda: analizė, įvertinimas, rekomendacijos", *Rytų Europos studijų centras*, 2017, http://www.eesc.lt/uploads/news/id987/RESC%20monografija_propaganda.pdf, 2017 12 06.
[55] Žr. Gressel G., „Fellow travellers: Russia, anti-Westernism, and Europe's political parties", *ECFR Policy Brief*, 14 07 2017, http://www.ecfr.eu/publications/summary/fellow_travellers_russia_anti_westernism_and_europes_political_parties_7213, 2017 12 03; Polyakova A. *et al*, „The Kremlin's Trojan Horses", *Atlantic Council's Dinu Patriciu's Eurasia Center*, November 15, 2016, http://www.atlanticcouncil.org/publications/reports/kremlin-trojan-horses, 2017 11 30.
[56] Hansen F. S., (footnote 53), p .22

2.2.1. Conventional Threats

Let us start with the conventional military dimension that, in the Baltic Sea region, creates the "background" for hybrid threats. In the Baltic countries, this is a dominating factor. As defined by Martin N. Murphy and Gary Schaub,[57] the security of the Baltic Sea region is determined by Russia's determination to recreate its zone of influence in the region and its desire to probe the weakness of the West, i.e. Russia is less interested in the territory than in the effect itself.

Globally, Russia continues to pursue an aggressive position against NATO and the European Union, a confrontation with the Euro-Atlantic community seeking to weaken Europe, and a discrediting of NATO to thwart the trans-Atlantic ties. At the same time, in the military area, Russia carries out the most intensive modernization in the Western military district, which consequently creates "hard" security challenges for the Baltic countries.[58]

For example, while assessing the exercise "Zapad 2017", conducted in September 2017, it is possible to draw several generalizations. First, actions performed during the exercise enabled the assessment of the aggressive activity of Russia along its entire perimeter, bordering on NATO or its partners: in the Baltic and Black Seas, the Mediterranean Sea, and the Far North. Besides, the actions conducted were of an offensive nature. Second, "Zapad 2017" demonstrated the absence of transparency from the Russian side: some of the manoeuvers took place in other training areas than announced at the same time, well exceeding the declared number of exercise participants. Third, it was established that during the manoeuvers, military personnel were trained in actions learned from the lessons not only from Russian military conflicts in Georgia and Ukraine, but also in Syria. In general, exercise "Zapad 2017" should be treated as an inseparable part of Russia's general military position. This distinctly demonstrated the continual Russian process that has been ongoing for more than 10 years alongside the modernization of the armed forces and high combat readiness of Russian forces: the capability to quickly deploy armed forces and simultaneous implementation of selective international commitments.[59]

---

[57] Murphy, Schaub (footnote 27).

[58] For more see: Wilk A., „The Zapad-2017 exercises: the information war (for now), *OSW Commentary*, 2017 09 04, https://www.osw.waw.pl/en/publikacje/osw-commentary/2017-09-04/zapad-2017-exercises-information-war-now, 2017 11 15.

[59] Ivanauskas V., Keršanskas V., „Po „Zapad 2017" – penkios žinutės Vakarams ir Lietuvai", 2017 10 04, https://www.delfi.lt/multimedija/putino_rusija/v-putino-rusija-po-zapad-2017-penkios-zinutes-vakarams-ir-lietuvai.d?id=75946229; „Zapad-17. Lessons learned", *Warsaw Institute*, 10 16 2017, https://warsawinstitute.org/wp-content/uploads/2017/10/ZAPAD-2017-russia-belarus-military-manuovers-drills-summary-eng.pdf, 2017 11 10.

2.2.2. "The Grey Zone"

Nevertheless, objectively assessing the probability of Russia's direct conventional confrontation with NATO remains limited because of the unbalanced aggregate resource. Therefore, the probability of employing hybrid threats only increases because this makes it possible to circumvent the traditional division line between war and peace and, in fact, entangle the adversary into the "grey zone" situation. As John R. Davis Jr. states, "history is abound with examples in which the weak employed different, hybrid ways and means to achieve their desired end state and defeat the strong".[60] He reminds us that as early as 1999, two officers of the People's Liberation Army of China, Qiao Liang and Wang Xiang, devised the concept of "unrestricted warfare" as a means by which weaker countries could overcome their military inferiorities in relation to a stronger nation. The concept of unrestricted warfare is, in essence, a war without limits or beyond the traditionally accepted physical limits of a war.[61] It is the symbiosis of conventional and hybrid threats that make the basis of the concept of the Baltic States' security challenging.

Why do Russia's actions cause concern for the Baltic countries? Firstly, Russia has never stopped treating the Baltic States as being within its exceptional influence area and has long been using political, economic, energy resources, propaganda, cyber, informational, and other coercive, overt, and covert means in order to make countries vulnerable and weak. Those measures, even comparing them to the increase of Russia's military potential, kept only growing during the recent years.

2.2.3. Dissemination of Disinformation and Propaganda

It is true that hybrid-impact measures in Lithuania and other Baltic countries are most distinctly observed through disinformation with the objective to affect societies, cause doubts as to historical memory and current social economic situations, involve separate groups into favourable for Russia narratives, escalate the feeling of soviet nostalgia, create a sense of insecurity, etc. Propaganda is always constructed purposefully, i.e. a specific message targets a certain community group that can be affected the most. Attempts are

[60] Davis Jr. J. R., „Continued Evolution of Hybrid Threats. The Russian Hybrid Threat Construct and the Need for Innovation", 28/2015, *The Three Swords Magazine*, p. 19, http://www.jwc.nato.int/images/stories/threeswords/CONTINUED_EVOLUTION_OF_HYBRID_THREATS.pdf, 2017 11 05.
[61] *Ibidem*, p. 21.

made to instigate and set one part of society against the remaining part (by making use of purposefully false, fabricated sensitive information) while turning another group into a passive "grey mass" taking no interest in social-political matters ("why should we resist at all if Russia is so powerful"). After the collapse of the USSR and the end of the Cold War, the West, having believed the vision of the world order that has transcended ideological fighting, closed and drastically reduced its information dissemination channels, intended for Eastern Europe or post-soviet space whereas Russia has never stopped investing in mass media means – primarily in the neighbouring states with large Russian-speaking communities of the population and, later on, creating global projects in different world languages ("Russia Today", "Sputnik", etc.). Therefore today, with Russia having entered a particularly active phase of propaganda, the West is lagging several steps behind the Kremlin, while in addition, the adequate reaction is encumbered by the ambiguous treatment of V. Putin's Russia in multi-layered Western societies.

The main targets of adverse informational operations in Lithuania are the history of Lithuania and the Lithuanian Armed Forces, encouragement of nihilistic dispositions, instigation of ethnic discord, and the discrediting of NATO and the European Union. Relations between Lithuania and Poland, including sensitive topics referring to the participation of Lithuanians in the Holocaust, are also attributable to Russia's disinformation targets.

Among the most easily affected and thus attracting the greatest attention from Russia society groups are national communities, people still living in soviet nostalgia, persons of the lowest social stratum as well as conservative layers of society. Orientated particularly towards these groups, the Kremlin designs its propaganda in a way to meet their expectations in mass media: entertaining content frequently smacking of soviet times intertwined with informational messages directed towards a specific audience.

For example, attempts are made to show national communities that they are discriminated against and, though actually belonging to the "Russian world", are unnaturally "torn off" by having become a part of Western structures (the European Union or NATO); people of the lowest society stratum are persuaded that the welfare promised by orientating towards the West has not been achieved, whereas life, closely cooperating with Moscow, would be much better. The myth of reviving fascism is cultivated among the people affected by soviet nostalgia, while the image of the "rotten West" is projected to the conservative sections of society.

Special attention should be devoted to the research of the factors that

form the susceptibility of society or its separate groups to propaganda information. The study carried out by the Eastern Europe Studies Centre (EESC)[62] showed that the main factors are two – soviet nostalgia and the assessment of functioning of democracy in Lithuania. In this sense, it is possible to discern both positive and negative tendencies. The part of society that assessed soviet times positively considerably decreased after 2014 and is particularly obvious among young people (only 8.5 percent of the 18-29 age group estimated soviet times positively; for comparison, in the age group of 60 and over – 40.2 percent). Thus, one can state that this factor will eventually stop being as important. However, the assessment of the second factor, i.e. democracy operation, is striking because as many as 42 percent of respondents (who participated in the research commissioned by the EESC) estimated the functioning of democracy negatively or very negatively, while 28 percent were neither satisfied nor dissatisfied.

The Kremlin's propaganda is also orientated towards the membership of NATO and the Baltic States in the Alliance. This is the next logical action because it is the enlargement of NATO towards Eastern Europe that is defined, even in Russia's strategic documents, as one of the main threats. NATO's coming nearer to Russia's borders is perceived in Russia's foreign security concept as violating common security space in the Euro-Atlantic region.[63] Therefore, the Kremlin employs all means seeking to stop even theoretical membership perspectives of Georgia or Ukraine, as well as turn the already admitted East European states into a buffer space of the overlapping security.

2.2.4. Influencing elections

Andrius Kubilius, in particular, developed the topic of Russian hybrid influence on elections and the general political system.[64] According to Kubilius, speaking about Lithuania's experience and the current legal and political situation, one can distinguish the following types of hybrid threats: impact on public opinion, using agents influencing opinion leaders, public organizations; "co-branding" when the images of election commissions, political movements or emerging political parties are created by uncontrolled business funds; officially unpaid, shadow funding for political campaigns; pooling of shadow money and influence groups, using the Kremlin pressure on businesses related to Rus-

[62] Vaišnys A. *et al* (footnote 54).
[63] „Foreign Policy Concept of the Russian Federation" (footnote 48).
[64] Kubilius A, "Demokratijos apsaugos nuo hibridinių grėsmių strategija", https://www.delfi.lt/news/ringas/politics/andrius-kubilius-demokratijos-apsaugos-nuo-hibridiniu-gresmiu-strategija.d?id=77961877

sia and their owners involved in Lithuanian politics, creating parties or otherwise trying to influence the political system; the weakening of the political system, in support of anti-system, populist, pro-Kremlin political forces; the weakening of the institutions, interference with the operation of the infrastructure through the use of cyber-attacks, the introduction of intelligence gadgets; pressure on politicians and influence on public opinion by manipulating disruptions of energy supplies, prices, etc. It is concluded that in 2019, during the presidential elections, Lithuania will face a giant and effective Kremlin hybrid attack campaign.

2.2.5. Other Examples of Russia's Hybrid Influence

According to Jānis Bērziņš, influence-wielding actions of Russia in Latvia (this tactic could be easily applied to the Lithuanian situation) are comprised of Russia's issuing passports to non-citizens, supporting of pseudo-human rights movements, rallying supporters for the referendum concerning the introduction of the Russian language as the second official language in Latvia, asking inhabitants living along the eastern border to fill in questionnaires in order to get information on people's wishes to support scenarios similar to those in Ukraine, influencing home policy through some political parties, etc.[65]

Martin N. Murphy and Gary Schaub, for their part, distinguish between two major Russian measures against the Baltic States: (1) a low-key, possibly opportunistic, campaign that exploits real or manufactured discontent among Russian compatriots to destabilize one or more of the Baltic States, creating a "frozen conflict" that undermines NATO's credibility; or (2) a more structured, high-tempo campaign to achieve the same objectives against NATO power in the Baltic Sea Region.[66]

Experts from the NATO Strategic Communication Center of Excellence have identified these key Russian instruments in the Nordic and Baltic regions: Russia's domestic and international media system; the Internet and social media; government-organized non-governmental organizations (GONGOs); Russia's compatriot policy; pipeline diplomacy; economic interdependency; the encouragement of political radicalization and polarization of Western societies; intelligence operations; and demonstrations of military force.[67]

---

[65] Bērziņš, (footnote 47) p. 7.

[66] Murphy, Schaub (footnote 27).

[67] „Russia's footprint in the Nordic-Baltic information environment", NATO Strategic Communications Centre of Excellence, Report 2016/2017, p. 8, https://www.stratcomcoe.org/russias-footprint-nordic-baltic-information-environment-0, 2017 11 30, p .7

In a study on Russia's hybrid threats, Andrew Radin highlighted three main types of activities that Russia can use for the Baltic States:[68] (1) non-violent subversion; (2) covert violent action; and (3) conventional aggression supported by political subversion. According to A. Radin, in the case of non-violent subversion, Russia's chances of destabilizing the situation in the Baltic States are not high. The analysis of recent years confirms that using this type of activity measures Russia's ability to destabilize the domestic situation in Lithuania remains, however adequate government measures and the reaction of civil society help to minimize it. However, these hybrid Russian measures must be analysed and evaluated. Again, in the case of covert violent actions, the chances are also small, especially given the fact that the countries of the region have learned from the scenario used by Russia and have measures against the "little green men". But these hybrid Russian measures must be analysed and evaluated as well. Finally, according to A. Radin, traditional military measures, especially those supported by subversion practices, pose the greatest risk to the Baltic States, as Russia has strong conventional domination and will quickly overcome resistance. Therefore, a conventional war in combination with hybrid measures remains the top priority for Lithuania as well.

EESC research on hybrid signals, the aim of which was to compile a register of various actions carried out by Russia and attributable to hybrid threats, indicated that already identified threat sources are supplemented by more aspects.[69] First, cyber-attacks against Estonia in 2007 or against Lithuania in 2014–2015. These hackings were aimed at demonstrating the vulnerability of the institutions and influence groups of the country and simultaneously implementing narratives favourable to Russia (e.g. the myth of the Bronze soldier as the liberator), splitting the country's groups, discrediting people, and compromising positions. Another example: in June 2015, members of the Russian parliament, Yevgeny Fyodorov and Anton Ramonov, who are representatives of the "United Russia" party, appealed to the Procurator General and submitted a complaint that the State Council of the USSR illegitimately recognized Lithuania, Latvia, Poland, and Estonia in 1991. By submitting such complaints, the members of Russia's political elite questioned the legitimacy of the Baltic countries and "provoked", in a peculiar way, the authorities and society of the countries, indicating that the Baltic countries have and will have dependence

[68] Radin A., „Hybrid Warfare in the Baltics. Threats and Potential Responses", *RAND Corporation*, 2017, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf, 2017 12 06.

[69] Buinauskas D. *et al,* „Information signals of hybrid warfare: the case of Russia", *EESC Report*, October 2016.

on Russia. Third, in December 2016, inhabitants of some Vilnius quarters received informational brochures in Russian. These brochures invited people of Russian-nationality to participate in the program that supports the transfer of Russians (and not only them) from Lithuania to Russia. Thus, ungrounded attempts were made to cause discontent with the socio-economic situation in Lithuania, erroneously illustrating that the standard of living in Russia is higher.

2.2.6. "Hybrid" Security Environment of the Baltic States

Thus, we can actually see a rather clear consensus, if not concerning an exact definition of hybrid threats, then at least about what the Baltic States, being in the "front" line, should concentrate on in the context of threats:

- Informational threats (particularly operating through Russian-speaking citizens);
- Threats to the cyber space;
- Influencing elections and political system;
- Threats through the potentially poorly guarded state borders (in case of Ukraine, the "green little men" did not emerge from nowhere – they had to cross the state border physically);
- Negative impact on critical infrastructure (this would comprise energy – assurance of supply and diversification; transport – the significance of Klaipėda seaport for the Lithuanian supply and in general the importance of the Baltic Sea for the Lithuanian economy; communications – the only Lithuanian fibre line to the West, lying on the bottom of the Baltic Sea, leads to Sweden; therefore, there are great possibilities to disrupt it);
- Traditional military measures supported by the subversive activity, escalation of fear by coordinating known measures with new ones;
- Covert violent actions;
- Actions aimed at vulnerable society areas, non-violent subversive activity by employing wider military, political, economic, civilian and informational methods;
- The Ostrovets atomic power station now under construction in Belarus next to Vilnius and the possibility to use it for hybrid actions could also be treated as a threat in the hybrid context.

All of the above constitutes the hybrid security environment of Lithuania and other Baltic States. It is obvious that these threats and their manifestation forms, in a broad sense, essentially correspond to the elements of hybrid warfare (p. 134–135).

3. Countering Hybrid Threats: Survey of Theoretical Assumptions and Practical Measures

Having analysed what makes up hybrid threats and discussed threat bases and structure, and given examples of Russia's employment of hybrid influences, we believe it is possible to pass consistently to the survey of means to overcome hybrid threats.

The "vague" nature of hybrid threats is a rather large limiting factor to start in general to talk about defence in just this context. During the Cold War, with the conventional (and nuclear) confrontation present to mobilize the political will of Western societies, choosing a strategy was quite simple. The illusion that emerged after the end of the Cold War and gave the idea that people can finally live in the age of peace and no one will threaten them was temporary; however, the awareness of threats to security is still vague in societies (and in part of the political elite).

A hybrid response requires that, with a clearly identified enemy absent, governments of Western states allocate public resources; thus, it is necessary to mobilize them. For the other side, specifically for Russia, it is much easier to do that due to the authoritarian nature alone. The classical strengths of Western governments – openness, an institutionalized decision-making process, respect to legal restrictions, accountability through legitimately elected legislative bodies, etc. – are not always strengths in order to react effectively to hybrid threats. We will see later that the reaction of the West, though purposeful, is slower than required by the security situation due to just these reasons.

3.1. Aspects of Countering Hybrid Threats

Before discussing the practical actions that Lithuania, the European Union, and NATO undertook after hybrid threats became relevant, it is reasonable to be acquainted with what various authors recommend in the academic-analytical field.

In general, these questions are addressed trying to decide what the system of the country's preparation to fight against hybrid threats should look like: Is there a common interdepartmental understanding of what a hybrid threat is? Are hybrid threats defined or explained in policy planning or national legal acts of the country? Are hybrid threats and scenarios described in the national assessment of threats to the country? Do hybrid threats belong to the

main threats? Is there a fixed standard operation order of all the identified risks? Is there a mechanism enabling identification of emerging dangers and threats (a certain risk-monitoring system) including those that affect new technologies and programs? Is there a structure responsible for the detection of hybrid activity, informing about hybrid activity, reacting to hybrid activity? Are crisis management instructions introduced? Is there a special structure ensuring interdepartmental coordination and crisis management at the strategic/political level? Are there centres of different crises/situations at the Ministers' level? Is there a central agency responsible for the collection of potential threats and analysis? Does the country possess informational systems enabling safe dissemination of information?

The starting point of the overview of countering hybrid threats strategy is a recent study of a group of prominent international authors who also proposed their list of range of hybrid tools.[70] They suggest for practitioners and researchers to emphasize a number of points in thinking about how to respond: respond with the „whole of government" – and beyond principle; be sceptical of metrics (Russia operations in Europe seem to have had most effect on those who were already sympathetic to Moscow); note that the first target of Russian operations is the Russian people; play on strengths (a great strength of the Western democracies is their free media); recognize that the distinction between peace and war is blurred; "the Russians are coming" (the U.S. case makes plain that the Russians have both the will and capacity to intervene in other nations' elections); pay attention to early warnings; tighten links across the public-private divide; pay close attention to the infrastructure of elections, etc.

3.1.1. Comprehensive Defence Concept

Aapo Cederber and Pasi Eronen rather accurately summarize what countering hybrid threats should start with. Those defending from hybrid threats should follow the concept of comprehensive defence. Another important aspect is the involvement of society: the defending country should create a more resilient society. The only secure way to develop public resilience is to retain at least a part of the "home ground" superiority because the aggressor will try to concentrate and use the effect of unexpectedness. However, in order

[70] Treverton G.F., Thvedt A., Chen A.R., Lee K., McCue M. (footnote 33).

to both implement the comprehensive defence concept and involve society, a long-term plan and devotion to implementation are necessary. Those fighting against must have a firm political mandate and a long-term security concept. To achieve that, planning, conscious development, and education are necessary. The main interested sides of society must share a common perception of the situation, common assessment of threats and risk, as well as planning and training processes.[71]

3.1.2. Resilience

Remigijus Žilinskas, whose analysis deals with resilience, distinguishes not only societal/civil resilience (the will of society to resist and oppose kinetic and non-kinetic influence and reduce the consequences as much as possible) but also the necessary-to-retain-state-capabilities of functional resilience that refers to the statecraft, i.e. the institutional system having political, military, economic, social, and administrative authorization to govern the country and take corresponding decisions. Its functioning in crisis is critical.[72]

The term "resilience" as a countermeasure to hybrid influence is referred to in all current studies on fighting against hybrid threats. As Uwe Hartmann underlines, hybrid warfare is an attack against NATO's strategic decisions, i.e. the aim is to damage national governance and (or) political will in security organizations.[73] Until now, the Alliance devoted most of its attention to technical resilience aspects; therefore, resilience should become the primary principle of NATO's future strategic concept.

In turn, Guillaume Lasconjarias proposes to relate resilience and deterrence concepts, stating that deterrence comprises a broad military dimension (both traditional and nuclear) as well as means and capabilities to react to external threat, whereas resilience is largely related to civilian preparedness, i.e. through deterrence – by reducing the vulnerability of society to reduce the probability of an assault.[74] By the way, in the case of the Baltic States, while conventional threats remaining particularly relevant, the association of resilience and deterrence is exceptionally relevant.

---

[71] Cederber, Eronen, (footnote 26) p. 8.
[72] Žilinskas, (footnote 13) p. 79.
[73] Hartmann U., „The Evolution of the Hybrid Threat, and Resilience as a Countermeasure", *Research Paper*, No. 139, September 2017, p. 2, http://www.ndc.nato.int/news/news.php?icode=1083.
[74] Lasconjarias G., „Deterrence through Resilience NATO, the Nations and the Challenges of Being Prepared", *Research Paper*, No. 7, May 2017, p. 1, http://www.ndc.nato.int/news/news.php?icode=1060.

3.1.3. Military and Civilian Cooperation

Military readiness to repel such threats is particularly important but this does not suffice. Response to hybrid threats must also be hybrid. In this situation, the coordination of military and civilians, as well as the involvement of society, are most important. Another aspect is the increase in state resilience. The increase in state resilience in the areas of energy supply, capability to effectively manage flows of uncontrolled movement of the population, food and water supply, systems of communication and transport, etc. A great competence in this area is concentrated in the military sector.

3.1.4. Coordination and Constant Attention of State Officials

The experience of other countries – Finland[75], the United Kingdom, Estonia, etc. – also demonstrates that the coordination at the government level is primarily necessary. State must be ready for such crises. The mechanism of the coordination of various institutions and crisis management must be in good operation, actions and procedures of different institutions prepared and well worked out.

Proposals of Latvian experts are also orientated towards enhancing state capabilities against hybrid threats. At the Government level, Latvia should urgently ensure that national security become a part of the decision-making process; consider the essence and consequences of the decisions, not just the formal application of bureaucratic procedures; Latvia's integration policy should be strategically defined anew, without harming its objectives; support to regional development should be urgently increased; security structures of the Ministry of Internal Affairs should be ready to solve the first five stages of a war; operative capabilities of the National Armed Forces to fight against a new-generation war should be improved; a new model of conscription-based army should be created; Latvian laws should be changed in order to enhance the independence of commanders to decide when to react to the attack.[76]

Experts, united in the Czech analytical "European Values Think-Tank", attribute the safeguarding of the electoral process to the most important prio-

[75] „Security Strategy for Society updated - Building a safe Finland together", *Press release, Government Communications Department Ministry of Defence*, November 2, 2017, http://valtioneuvosto.fi/en/article/-/asset_publisher/10616/yhteiskunnan-turvallisuusstrategia-paivitettiin-turvallinen-suomi-rakennetaan-yhdessa, 2017 11 30.

[76] Bērziņš, (footnote 47) p. 9-10.

rities of countering hybrid threats. As one of the reports emphasizes, Russia's influence on the elections in the US and France and on referendums in the United Kingdom ("Brexit") or the Netherlands (on the agreement of Ukrainian association with the European Union) was clearly felt and this contradicts the democratic mandate and national interests of countries. If a country wants to call itself a sovereign state, a hostile foreign country should not influence a democratic election process. In the authors' opinion, "that is why it is important for democracies to set up tailored national defence systems against hostile foreign interference to keep their domestic choices free and fair, without a foreign power being able to influence the choice of the citizens".[77]

3.1.5. Risk Estimation, Vulnerability

Risk assessment takes a particular place. A developed risk estimation and awareness of the situation enables the better understanding of operations of the adversary before their taking place and help formulate an adequate response to the evolving situation. Reliable situational awareness requires an active intelligence data collection from both open and closed sources. In addition to that, in organizing defence, reliable intelligence information and high-quality analysis are necessary. According to F. S. Hansen, "it is advisable for planners to focus on vulnerabilities and seek to reduce those rather than to address the threats, which presently seem very difficult for external actors to change".[78]

As stated above, during a hybrid attack, the enemy will try to hit the most vulnerable and weakest parts of the state. Therefore, the national assessment of risks in determining which places are the weakest, where a potential asymmetric attack can hit at a specific moment, etc. are a task of state significance.

Thus, summarizing the insights of various authors and the experience of states, the main elements in repelling hybrid threats at the national level are these:

- to have a firm political mandate and comprehensive security concept;
- to have a well-functioning coordination of various institutions at the Government level;

[77] The European Values Think-Tank, „A framework guide to tools for countering hostile foreign electoral interference", *Kremlin Watch Report*, 11 05 2017, p. 1, http://www.europeanvalues.net/wp-content/uploads/2017/05/35-measures-in-15-steps-for-enhancing-the-resilience-of-the-democratic-electoral-process-1-1.pdf

[78] Hansen, (footnote 53) p. 34.

- to have a crisis-management mechanism, prepare and work out actions and procedures of various institutions
- to create a clearly regulating legal base;
- the main interested sides of society should have a common understanding of the situation, common assessment of threats and risks as well as planning and training processes;
- military readiness to counter such threats is particularly important but it alone does not suffice; No one doubts that in case of a conventional Russian attack, the military will know what to do but is it known what to do in case of a more complicated scenario;
- the importance of intelligence. Creation of the system concerning the perception of hybrid threats and influence operations;
- enhancement of the cooperation between military and civilian sectors;
- repelling of informational threats. Involvement and support of society, development of consciousness and education;
- integration of national minorities and development of regional policy;
- rapid reaction;
- enhancement of resilience. i.e. it is important not only to identify the means of enemy influence but also to know weaknesses of Lithuanian society and enhance resilience;
- constant preparation, training, exercises.

Concentration of competences at the national level enables a clear refinement, of which aspects of resilience to hybrid threats could be overcome collectively while operating at the level of the European Union and NATO. The marking of limits remains a future challenge, even though, as presented in section 3.3., a certain understanding exists now.

3.2. National Actions in Deterring Hybrid Threats – Lithuania's Case

After Russia's actions in Ukraine, Lithuania made huge steps in reacting to hybrid threats; therefore, it is worth surveying what has actually been done. This will be assessed following the main elements on the repelling of hybrid threats formed in section 3.1.:

- to have a firm political mandate and comprehensive security concept

Aafter 2014, the consensus on the awareness of external threats and the need

to respond to them on a broad scope became established in both political and institutional fields. This is demonstrated by the considerations of the National Security Strategy 2016–2020: The Strategy names a broad spectrum of threats (covering both conventional and hybrid threats) while discussions did not experience greater disagreements. Lithuanian institutions – the Ministry of Internal Affairs, the Ministry of National Defense, intelligence, police, border protection and other services, undertook specific actions seeking to enhance resilience to hybrid threats. Having reached the limit of 2 percent from the GDP allocated to defence, discussions started in the political area concerning the necessity to further increase financing of national defence. The limit line is considered a minimal basis which must not be violated. Ever growing attention of institutions is devoted to the evolvement of the comprehensive security concept; however, it is too early to estimate the ensuing results.

- military readiness to counter such threats is particularly important but it alone does not suffice

In the area of military defence, the most important decision was to increase the defence budget so that it would reach and even exceed the 2 percent of the GDP required by NATO. A large part of the increased defence budget was allocated for the acquisition of military equipment, with the greatest attention paid to anti-tank defence, air defence, and the enhancement of manoeuvrability using the possibilities of communications and intelligence. This is also important in case of hybrid warfare. Besides, a decision was made to reinstitute the army of conscripts. This step is important not only in augmenting conventional capabilities of the country but also in increasing the reserve and involving Lithuanian citizens in defence.

- rapid reaction

In November 2014, rapid reaction forces were established.[79] Since, in reacting to hybrid threats, it is necessary to act as fast as possible in order to prevent the deepening of the crisis, readiness of these forces is particularly high – the ability to react within 2-24 hours. The structure is also clear – two battalion-size groups, supported by special forces, logistics, and the other capabilities of the armed forces.

[79] BNS, „Lietuvoje pradeda veikti greitojo reagavimo pajėgos", 2014 11 01, https://www.delfi.lt/news/daily/lithuania/lietuvoje-pradeda-veikti-greitojo-reagavimo-pajegos.d?id=66279492, 2017 11 30.

- to have a crisis-management mechanism, prepare and work out actions and procedures of various institutions, enhance the cooperation between military and civilian sectors. constant preparation, training, exercises

In Lithuania in 2014, as part of the preparation to react to hybrid scenarios, exercises employing structures of the national defence and internal affairs, as well as institutions of local authorities, began.[80] In December 2014, Seimas approved legal acts that grant a legal basis to react to hybrid threats by using armed forces in peacetime. For example, if local armed incidents are carried out or border violations (an analogy with the scenario of "little green men" of Ukraine) that do not reach the level of aggression (i.e. peacetime laws are still valid), the President of the Republic may make the decision to directly employ armed forces (the decision must also be approved by the Parliament). This decision should have a clear mandate, and fixed time and territory in which certain civilian functions will be further conducted.

Strengthening of borders is attributed to the reaction to hybrid threats as well. The security of borders starts with the awareness of the situation and the ability to observe. Lithuania, with the support of the US armed forces, for a number of years has been conducting a specific project aimed at considerably increasing national capabilities to strengthen the security of Lithuanian borders. Besides, the protection of borders is improved by employing national means.

After 2016, the planning of civil security and mobilization, exercises, and coordination at a self-governance level became more intensive.

- enhancement of resilience

In December 2014, in responding to cyber-attacks, Seimas confirmed a new law on cyber security, while in 2015, the National Cyber Security Center was established. The greatest attention in it is paid to the protection of the critical information infrastructure, the public sector, with enhanced resilience and reaction capabilities. In 2017, a decision was passed that from then on cyber security matters will be in the hands of only one institution in the country – the Ministry of National Defence.[81]

Lithuania made a breakthrough in assuring energy independence. In

[80] „Nuo rytojaus Lietuvos kariai treniruosis atremti hibridines grėsmes pratybose „Žaibo kirtis 2017", *Vilkaviškio rajono savivaldybė*, 2017 04 27, http://www.vilkaviskis.lt/go.php/lit/Nuo-rytojaus-lietuvos-kariai-treniruosis-atremti-hibridines-gresmes-pratybose-zaibo-kirtis-2017/3592, 2017 12 10.

[81] Ramelienė R., „Kibernetinis saugumas – po vienu skėčiu", 2017 08 08, https://www.lzinios.lt/lzinios/lietuva/kibernetinis-saugumas-po-vienu-skeciu/248415, 2017 12 10.

order to guarantee energy supply independence and decrease Russia's manipulation possibilities, a liquefied gas terminal was built in Klaipėda. Besides, electricity links with Sweden and Poland granted Lithuania a possibility to not buy electricity from Russia or Belarus. Lithuania's possibilities to influence the construction by Russia and Belarus of the nuclear power plant in Ostrovets (in Belarus, a proximity of 40km from Vilnius) should be considered separately. One thing is obvious, the issue of the construction of the Ostrovets nuclear power plant is broader than just ecology, radiation standards, or keeping to the international norms during its construction. It is necessary to look at this project through the prisms of Russia's geopolitical influence and hybrid threats.[82]

- to have a well-functioning coordination of various institutions at the government level. To have a crisis-management mechanism, prepare and work out actions and procedures of various institutions. The importance of intelligence. Creation of the system concerning the awareness of hybrid threats and influence operations.

Responding to hybrid threats and seeking to guarantee an effective prevention of crises, the idea to create a crisis-management mechanism in Lithuania was reverted to several times.[83] Initially, the Center of Crisis Management was established under the Ministry of National Defense. Later the Center was transferred to the Chancellery of the Lithuanian Government, where it shrank to a functional division of the Chancellery. Russia's actions in Ukraine, particularly the used hybrid scenarios, made planners return to the idea of the united crisis management unit. The realization that Lithuania has no integrated institution at the level of the State or Government, the institution that could function in case of crisis and would combine efforts of various institutions as well as coordinate their activity in the evolvement of crises, extreme situations or hybrid scenarios dawned at the beginning of the Ukrainian crisis. At the same time, the need for coordinated activity exists not just at the beginning of an emerging crisis or extreme situation, but for the conducting of crisis prevention, i.e. by integrating and coordinating the activity of different institutions to carry

[82] One of the first attempts to look into the problems of Ostrovets atomic power station more extensively: Česnakas G., Juozaitis J., „Nuclear Geopolitics in the Baltic Sea Region. Exposing Russian Interests Behind Ostravets NPP", *Atlantic Council. Global Energy Center*, July 2017, http://www.atlanticcouncil.org/publications/issue-briefs/nuclear-geopolitics-in-the-baltic-sea-region, 2017 12 10.

[83] Gudavičius S., „ Prezidentė nori, kad Lietuvoje atsirastų Krizių valdymo centras", 2015 11 25, https://www.vz.lt/verslo-aplinka/politika/2015/11/25/prezidente-nori-kad-lietuvoje-atsirastu-kriziu-valdymo-centras#ixzz52UjKgprZ, 2017 12 15.

out the observation and analysis in the real time of the phenomena related to national security.

The Ukrainian situation forced a return to the creation of a coordinated mechanism that would enable a timely identification of potential threats to national security and would assure a coordinated and timely response to these threats. In fact, an institution of this type could conduct the education of society and citizens on modern threats, enhance civil resilience to disinformation, propaganda, and other hostile informational activities, strengthen the perception of citizens in recognizing hybrid threats, and encourage them to get involved in the solution of issues pertaining to national security as well as conduct national exercises on crisis management. Though several governments announced their intentions to develop an integrated system of crisis management and deterrence of hybrid threats, there were no real plans and mechanisms for the implementation. Certainly, a rather well functioning system for overcoming civil emergency crises had already been developed. However, hybrid security raised the coordination issue to a higher level.

The implementation plan concerning the program of the 16th Government provided for a specific activity in the crisis prevention area, i.e. "Creation of an integrated crisis management and hybrid threats deterrence system" with concrete tasks: "establishment of a unit coordinating crises prevention and preparedness to manage them at the Government Chancellery; creation and legalization of the model of crisis management and hybrid threats deterrence system; redistribution of functions of the institutions participating in crisis prevention and management activity in compliance with the approved model; creation of the monitoring system of threat and crisis factors; participation in enhancing the means of the European Union, NATO, and international fighting against hybrid threats".[84]

- to create a clearly regulating legal base

In 2017, the first specific steps were made at the strategic level. On 21 June 2017, the resolution of the Government of the Republic of Lithuania's "On the Formation of the National Security Commission of the Government of the

[84] Lietuvos Respublikos Vyriausybės nutarimas „Dėl Lietuvos Respublikos Vyriausybės programos įgyvendinimo plano patvirtinimo", 2017 m. kovo 13 d. Nr. 167, https://www.e-tar.lt/portal/lt/legalAct/2389544007bf11e79ba1ee3112ade9bc, 2017 12 15.

Republic of Lithuania" was adopted.[85] Several sittings of this Commission have already taken place. In summer, a reformed Government Chancellery, where a crisis prevention and rhreats management bureau was established, started functioning.

Thus, in Lithuania, the framework of a comprehensive mechanism, comprising monitoring/observation, identification, legislature, enhancement of defence capabilities, etc. started emerging.

- repelling of informational threats. Involvement and support of society, development of consciousness and education. Integration of national minorities and development of regional policy

It is necessary to underline separately the achievements in strategic communication. Lithuania's efforts in countering disinformation were implemented in three main ways: (1) enhancement of strategic communication capabilities (establishment of specialized subunits at the Ministry of Foreign Affairs, the Ministry of National Defense, the Armed Forces, intelligence institutions as well as other Departments – e.g. the Ministry of Culture); (2) enhancement of society's awareness of informational warfare and propaganda; (3) preventing the dissemination of war and hatred propaganda.

An important thing in fighting against informational threats became not only the education of officials, politicians, mass media, and society, but also an active communication in identifying lies, deconstructing them, and spreading the information and narratives of Lithuania itself.

Lithuania's example demonstrated that in responding to the influence of Russia, not only with strategic communication and informational knowledge of society about propaganda but also with legal means to deter whatever violates the laws. The Lithuanian Radio and Television Commission was granted the right to temporarily ban the broadcasting of television programs or to initiate legal actions in revoking licenses of those who spread disinformation and hatred.

The fact that fighting conducted by Lithuania against informational threats yielded results is indicated by a concrete example – reaction to the informational attack against German military personnel serving in Lithuania from February 2017 as part of the NATO Enhanced Forward Presence forces.

[85] Lietuvos Respublikos Vyriausybės nutarimas „Dėl Lietuvos Respublikos Vyriausybės nacionalinio saugumo komisijos sudarymo", 2017 m. birželio 21 d. Nr. 477, https://www.e-tar.lt/portal/lt/legalAct/03b7dc2057f311e7846ef01bfffb9b64, 2017 12 15.

Reaction to an alleged rape of a teenage girl by German soldiers was smooth, coordinating actions between the armed forces and police officials, and had no negative influence on the perception of the local population of NATO allies and the battalion of the Alliance in Lithuania.[86]

It is worth pointing out the activity of paramilitary volunteer organizations as part of society resilience, for example, the activity of the Lithuanian Riflemen Union, which encourages patriotic education and civil resistance. It should be emphasized that from 2013, the number of riflemen grew by 38 percent.[87] There also exists civil actions of various forms intended for fighting against informational threats, for example, Lithuanian or Baltic "elves".[88]

The work fighting against informational threats continually intensifies: attempts are made to better understand the model of the activity fostering Russia's influence, attract more of Western pop culture to Lithuania (in order to neutralize Russia's so-called "active measures").

The international activity in promoting resilience to Russian propaganda is also important. Lithuania is part of information sharing and platforms coordination between the Baltic States, the Nordic countries, and Poland, which contributes to the strategic capabilities of the European Union and NATO. Specific projects in this area also exist, for example, in September 2017, the Broadcasting Board of Governors (BBG) of the US installed an AM radio transmitter for the retransmission of programs of the radio station RFE/RL to Russia and Belarus.[89] AM radio can be important in case the institutions of Russian or Belarus authorities decided to block the RFE/RL signal. At present, RFE/RL broadcast throughout Lithuania nearly 10 hours per day and night in the Russian and Belarus languages.

In 2015, the Department of National Minorities under the Government was re-established, with the aim to guarantee better coordination and implementation of the state policy concerning national minorities. At the end of 2017, the Ministry of Internal Affairs presented the White Book on regional policy aiming at reducing non-uniformity between regions and assuring their harmonious and sustainable development.[90]

---

[86] Gurevičius A., Samoškaitė E., „Lietuva vos netapo provokacijos auka", 2017 02 15, https://www.delfi.lt/news/daily/lithuania/lietuva-vos-netapo-provokacijos-auka.d?id=73769620, 2017 12 15.

[87] Jakučionis S., „Naujasis Šaulių sąjungos vadas nori suburti emigrantus", 2017 06 03, http://www.diena.lt/naujienos/lietuva/salies-pulsas/sauliu-sajunga-turi-nauja-vada-814559, 2017 12 15.

[88] Euronews, „Lithuania has a volunteer army fighting a war on the internet", 28 09 2017, http://www.euronews.com/2017/09/28/lithuania-has-a-volunteer-army-fighting-a-war-on-the-internet, 2017 12 15.

[89] „L. Linkevičius: septynios tonos žodžio laisvės - įjungtas naujas radijo programų siųstuvas", *Užsienio reikalų ministerija*, 2017 08 29, https://www.urm.lt/default/lt/naujienos/llinkeviciusseptynios-tonos-zodzio-laisvesijungtas-naujas-radijo-programu-siustuvas, 2017 12 15.

[90] Vidaus reikalų ministerija, *Lietuvos regioninės politikos baltoji knyga"*, 2017, https://vrm.lrv.lt/uploads/vrm/documents/files/LT_versija/Naujienos/Regionines_politikos_baltoji_knyga_20171215.pdf, 2017 12 20.

Lithuanian experts are actively monitoring international or national initiatives aimed at combating propaganda. For example, in the heat of Ukraine's events, the enthusiastic team gathered by the Stopfake.org team of Ukrainians began to analyse all the false messages sent by Russia about Ukraine and sought to deconstruct them, to show a clear lie. In this way, it was not intended to impose its own assessment, but at least it denies manifestly misleading information. It is also a great initiative of the Czech non-government to launch the above-mentioned European Values Think-Tank, launching annual forums for experts involved in information threats, initiating regular analytical studies. Several US NGO initiatives are also worth mentioning - the initiative of the American Atlantic Council, the Digital Forensics Research Lab and the US German Marshall Fund for the Alliance of Democrats, the German Marshall Fund of the United States (also known as the Hamilton68 initiative). These are just a few examples.

3.3. Institutional Reaction of NATO and the European Union

Fighting against hybrid threats relies not only on national but also on collective – NATO and the European Union – efforts. Taking into consideration the nature of hybrid threats, national defence efforts should inevitably be strengthened by an international component. International cooperation, particularly through the European Union and NATO, can offer much on the political, economic and military fields; besides, this helps "cover" some missing national capabilities or render support in developing these capabilities in the areas in which they are not sufficiently developed. International cooperation enables countries to unite separate, scattered national resources in solving issues of a broader, international agenda.

Speaking about the European Union and NATO fighting against hybrid threats, a particular importance is attributed not only to the influence of the organizations themselves but also to the position of Western political leaders. How the President of France, Emanuel Macron, made his points in a joint press conference with the Russian President V. Putin can well serve as standard for other West European leaders: "during the campaign (electoral – authors) *Russia Today* and *Sputnik* were agents of influence which, on several occasions, spread fake news about me personally and my campaign…They behaved like

organs of influence, of propaganda, and of lying propaganda".[91] With Russia actively interfering in elections, referendums, public processes, etc., understanding between the Western elite and experts is growing. This forms a basis for the accelerating systemic activity of the European Union and NATO while fighting hybrid threats.

The documents of both the EU and NATO clearly state that each member country is responsible for a response to hybrid threats. At the same time, due to the efforts of Lithuania and other Central and East European countries, both the European Union and NATO started seriously considering a collective response to hybrid threats. Processes in both organizations are gaining traction.

3.3.1. NATO's Decisions and Actions

The first NATO response to Russia's aggressive actions in Ukraine was more a military-political one. In September 2014, at the summit in Wales, NATO reached an agreement on the Readiness Action Plan (RAP) in order to "address both the continuing need for assurance of Allies and the adaptation of the Alliance's military strategic posture by continuous air, land, and maritime presence and meaningful military activity in the eastern part of the Alliance, both on a rotational basis".[92] The main element of the RAP is a Very High Readiness Joint Task Force (VJTF) – a brigade-size capability in combination with air, special operations forces, and maritime support. This makes it possible to deploy within a few days at any time (on the territory of the Alliance or elsewhere) in order to carry out broad-spectrum missions and stabilize the evolving crisis.

In July 2016, the Alliance took a still larger step – at the summit in Warsaw, the resolution on NATO's Enhanced Forward Presence in those countries that geographically are nearest to Russia was adopted. In the middle of 2017, military groups led by four NATO states – the US, Germany, Canada, and the United Kingdom – were correspondingly deployed in Poland, Lithuania, Latvia, and Estonia.

Speaking more specifically about hybrid threats, in December 2015,

[91] Rose M., Dyomkin D., „After talks, France's Macron hits out at Russian media, Putin denies hacking", May 29, 2017, https://www.reuters.com/article/us-france-russia/after-talks-frances-macron-hits-out-at-russian-media-putin-denies-hacking-idUSKBN18P030, 2017 12 15.

[92] NATO, „Wales Summit Declaration", September 5, 2014, https://www.nato.int/cps/en/natohq/official_texts_112964.htm, 2017 12 15.

NATO Foreign Ministers agreed on NATO's role in countering hybrid threats.[93] The main elements are these: to identify hybrid threats; be resilient; be ready to resist threats, asses them and react effectively. NATO treats strategic hybrid actions as: (1) economic coercion; (2) disinformation; (3) cyber-attacks; (4) attacks or sabotage against objects of a particularly important infrastructure; (5) overt activity based on military force.

While implementing this strategy, NATO made progress responding to Russia's informational attacks: (1) strategic communication capabilities at NATO headquarters were enhanced; (2) in Riga, the NATO Strategic Communications Centre of Excellence was established. In turn, the NATO Cooperative Cyber Defence Centre of Excellence was founded in Tallinn and in Vilnius the NATO Energy Security Centre of Excellence.

Another important NATO resolution on implementing the decision to enhance resilience was made at the NATO summit in Warsaw in July 2016, where NATO's seven baseline resilience requirements were agreed on: (1) guaranteed continuity of government and critical state services; (2) sustainable energy sources; (3) ability to effectively fight uncontrolled population movements; (4) sustainable food and water resources; (5) ability to fight mass casualties; (6) sustainable civil communications systems; and (7) sustainable civil transport systems.[94] These baseline resilience requirements, starting from 2018, were completely incorporated into NATO defence planning (previously, NATO military planning and civil security systems functioned separately). They reflect the level of resilience that should be achieved by each ally in order to always retain the main requirements pertaining to the continuity of the government, the continuity of fundamental services to the population and civil support to the armed forces, even in case of the most demanding scenarios.

At the NATO Warsaw summit in 2016, the role of the Alliance in countering hybrid threats was still more clearly defined: countries themselves should undertake specific countering measures, but NATO would assist in sharing expertise in various areas; besides, the Alliance would be able to decide when the situation was worth the applicability of Article 5.[95] Thus, hybrid threats came to be treated as an element of the collective defence (certainly, some experts believe that this does not suffice and suggest that

[93] NATO, „NATO Foreign Ministers address challenges to the south, agree new hybrid strategy and assurance measures for Turkey", December 1, 2015, https://www.nato.int/cps/ua/natohq/news_125368.htm, 2017 12 17.
[94] NATO, „Warsaw Summit Communiqué" (footnote 36).
[95] *Ibidem.*

the Baltic States should get involved in diplomatic efforts to change the Washington Treaty, particularly Article 5, in order to reflect challenges related to the 4th, 5th, 6th and 7th generation war, thus eliminating the space of a political manoeuvre[96]).

At the summit, the decision on a cyber-defence pledge was taken as well.[97] NATO promised to support members of the Alliance in enhancing cyber resilience.

Apart from these strategic NATO decisions in countering hybrid threats, regular exercises with hybrid scenarios continue to take place. For example, NATO Crisis Management Exercises (CMX) began to include hybrid scenarios, comprising disinformation, threats to critical infrastructure, and "grey zone" situations. NATO undertook, in earnest, the monitoring of adverse propaganda in countries where Forward Presence Forces of the Alliance are deployed. Reporting about hybrid incidents from members of the Alliance and NATO forces was also strengthened. NATO also participates in the European Centre of Excellence for Countering hybrid threats. NATO reviews its management structure, taking into consideration hybrid elements.

The Alliance is also determined to put pressure on Russia, in terms of hybrid threats, by employing periodic and purposeful discussions in the NATO–Russia Council (NRC); however, Russia has so far refused to participate in such discussions.

In the middle of 2017, a NATO–Ukraine Hybrid Platform was established, the first function of which took place in Warsaw.[98] Later, Lithuania sponsored a second seminar in the framework of the NATO–Ukraine Hybrid Platform "Strategic Communications Cooperation in Response to Hybrid Threats".[99]

Finally, at recent NATO Summit meeting in Brussels on July 11, 2018, Allied leaders reiterated that NATO is expanding the tools at its disposal to address hostile hybrid activities and announced the establishment of Counter Hybrid Support Teams, which will provide tailored, targeted assistance to Al-

[96] This is how the author defines the generations of war: 4 – non-state actors, 5 – without contact (employment of drones), 6 – cyber warfare, 7 – informational warfare. See: Jānis Bērziņš, (footnote 46) p. 9.
[97] NATO, „Warsaw Summit Communiqué" (footnote 36).
[98] National Security Bureau of the Republic of Poland, „Poland to start NATO-Ukraine coop re hybrid threats - security bureau", 25 10 2017, http://en.bbn.gov.pl/en/news/621,Poland-to-start-NATO-Ukraine-coop-re-hybrid-threats-security-bureau.html, 2017 12 20.
[99] "Lithuania promotes intensified cooperation between NATO and Ukraine in combating hybrid threats", http://www.urm.lt/default/en/news/lithuania-promotes-intensified-cooperation-between-nato-and-ukraine-in-combating-hybrid-threats, 2017 04 20

lies, upon their request, in preparing for and responding to hybrid activities.[100]

Thus, responding to hybrid threats, the Alliance has essentially taken, and continuing to take, slow but consistent steps in increasing the resilience of both the organization itself and its individual members.

3.3.2. Decisions and Actions of the European Union

Speaking about the efforts of the European Union in countering hybrid threats, the progress was not fast. The first step, to which Lithuanian politicians and diplomats also contributed, was to seek that hybrid threats be acknowledged by the EU at the strategic level. In April 2016, the European Commission (EC) and the High Representative of the EU for Foreign Affairs and Security Policy (HR) Federica Mogherini approved the communication *Joint System for Countering Hybrid Threats: a European Union Response,*[101] which became a fundamental document in terms of the EU efforts in this area.

In addition, in April 2016, the EU communication on the establishment of the *Security Union* recognized that it is necessary to fight against hybrid threats and that it is important to assure a greater consistency of internal and external actions in the security area.[102]

The *EU Global Strategy for Foreign and Security Policy,* approved in June 2016, thoroughly discusses the need of an integrated attitude in combining the internal EU resilience with its external actions and urges the formation of links between the defence policy and political measures in the activity areas of home market, industry, law protection, and intelligence services.[103]

In July 2016, in Warsaw, the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization signed a joint declaration that defines seven specific areas including fighting against hybrid threats: early warning/situational awareness; strategic communication; cyber security; and civil–military prepa-

[100] NATO, "Brussels Summit Declaration", July 11, 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm,

[101] European Commission (footnote 34).

[102] European Commission, „Delivering on the European Agenda on Security to Fight Against Terrorism and Pave the Way Towards an Effective and Genuine Security Union", COM(2016) 230 final, 2016 04 20, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/legislative-documents/docs/20160420/communication_eas_progress_since_april_2015_en.pdf, 2017 12 15.

[103] On 28 June 2016, the High Representative for Foreign Affairs and Security Policy F. Mogherini submitted the Strategy to the Presidency of the European Council.

redness and response.[104] In December 2016, the European Union and NATO Councils endorsed a set of 42 proposals for implementation. By the way, just a day before the NATO Summit meeting in July 2018, the President of the European Council, the President of the EC, and the Secretary General of NATO all agreed on the new text of the Joint declaration on EU-NATO cooperation, which also covers cooperation in countering hybrid threats.[105]

In November 2016, the EC, having adopted the *European Defence Action Plan,* launched specific initiatives contributing to the strengthening of the European Union's ability to respond to hybrid threats: the resilience of the supply chain in the defence sector was encouraged and the common market defence sector was strengthened.

In the aftermath of the *European Defence Action Plan,* in June 2017, the European Council established the European Defence Fund, with a proposed financing of 600 million euros until 2020 and after 2020, 1.5 billion euros annually. Hybrid threats are among the areas that can lay claim to the financing.

In fact, the approval of the *Joint System for Countering Hybrid Threats: A European Union Response*[106] was essential in seeking a comprehensive approach to fighting against hybrid threats. For the first time, the European Union considered threats "holistically" and clearly identified what should be done by the EC, the European External Actions Service (EEAS), and member states. Moreover, as regards the Salisbury attack of poisoning of former Russian intelligence agent Skripal and his daughter, the European Council on 22 March 2018 agreed that the EU must strengthen its resilience to chemical, biological, radiological, and nuclear-related risks, including through closer cooperation between the EU and its member states, as well as NATO.[107] The European Council also agreed that "the European Union and its Member States should also continue to bolster their capabilities to address hybrid threats, including in the areas of cyber, strategic communication and counter-intelligence" and invited the EC and the HR to take this work forward and report on progress by the June European Council. As a result, in June 2018, the *Joint Communication to the European Parliament, The European Council and the Council. Increasing Resilience and Bolstering Capabilities to Address Hybrid Threats* was

[104] NATO, „Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization", December 05, 2016, https://www.nato.int/cps/ic/natohq/official_texts_133163.htm, 2017 12 20.
[105] European Commission, „Joint declaration on EU-NATO cooperation", 2018 07 10, http://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf.
[106] European Commission (footnote 34).
[107] European Council, European Council meeting (22 March 2018) – Conclusions, EUCO 1/18, 2018 03 23, http://www.consilium.europa.eu/media/33457/22-euco-final-conclusions-en.pdf

issued.[108] Finally, the European Council, on 28 June 2018, agreed, among other issues, on coordinated EU response to the challenge of disinformation, including appropriate mandates and sufficient resources for the relevant EEAS Strategic Communications teams, stressed the need to strengthen capabilities against cybersecurity threats from outside the EU, welcomed the intention of the EC to present a legislative proposal to improve the detection and removal of content that incites hatred and to commit terrorist acts.[109]

The first important action provided for in the communication *Joint System for Countering Hybrid Threats: A European Union Response* was the urging for member states to start research on hybrid threats, aiming at distinguishing main vulnerability areas, including specific indicators of hybrid threats that might have an impact on national or European-level structures and systems. In the middle of 2017, at the initiative of Lithuania and other countries, the group of the Friends of the Presidency was established, which agreed on the assessing questionnaire of national hybrid threats and countering hybrid threats.

In turn, a very important step was made towards enhancing awareness – *the EU Hybrid Fusion Cell* was established in the intelligence subunit of the EEAS. Member countries appointed national points of contacts for communication with this unit. In order to strengthen strategic communication capabilities, and enhance monitoring of mass media, the *East Stratcom Task Force* was established. At the end of 2017, the EC made a decision to finance the so-called the European Strategic Communications Network.

The *East Stratcom Task Force* managed to achieve much in countering informational threats, however, it is possible and necessary to deter Russia's activity in this area on a much larger scale. Modern risk analysis and big data tools are important in seeking to propose adequate decisions of fighting against activities and pro-active measures (for example, computers with a large amount of data). The mandate and capabilities of the group should be better integrated into the activity of the EEAS and decision-making process. Member states and their representatives should have a possibility to prepare the agenda, support the working group of the *East Stratcom Task Force* and encourage its major role in the EEAS. In order to achieve greater progress in this area, eight EU member states urged the EEAS to considerably expand its activity against

[108] European Commission, „Joint Communication to the European Parliament, The European Council and the Council. Increasing resilience and bolstering capabilities to address hybrid threats", JOIN(2018) 16 final, 2018 06 13, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0016&from=EN.
[109] European Council, European Council meeting (28 June 2018) – Conclusions, Press Release, 2018 06 29, http://www.consilium.europa.eu/en/press/press-releases/2018/06/29/20180628-euco-conclusions-final/.

Russian propaganda and immediately enhance the capabilities of the working group of the *East Stratcom Task Force.*[110]

Seeking to improve the protection of critical infrastructure objects from hybrid threats and resilience to threat actions, the EC, in cooperation with member states and interested parties, undertook necessary measures. Firstly, it started discussions on a set of common indicators. The European Defence Agency undertook to determine shortcomings of joint capabilities and scientific research caused by the links between energy infrastructure and defence capabilities. While implementing the EU maritime security strategy and the EU customs risk management strategy and their action plans, the EC and the High Representative, coordinating the activity with member states, started analysing the ways of responding to hybrid threats, primarily threats related to critical transport infrastructure. Member states, the EU intelligence analysis centre, and related agencies currently determine threats to transport security and provide support in developing effective and proportionate risk-reduction measures.

Among other measures in countering hybrid threats, the attempts of the EC, in implementing the action plan concerning the financing of terrorists should be pointed out. Within 2017, the EC submitted three proposals concerning legal acts including punitive sanctions for money laundering and illegal payments in cash, as well as confiscation and freezing of property.

The HR and the EC, coordinating their activity with member states created a Joint Protocol of Operative Actions and regularly conduct exercises aimed at improving capabilities in strategic decision making while responding to hybrid threats on the grounds of crisis management and integrated political response to crises procedures. The EC and the EEAS announced the *EU Operational Protocol for Countering Hybrid Threats*, which determines the sequence of coordination, linking of intelligence data and analysis, submitting of information for political decision-making exercises and training processes as well as cooperation with partner organizations, primarily with NATO, in case of a hybrid threat. The European Union scenario was tested in practice in the fall of 2017, during paralleled and coordinated EU exercises in interaction with NATO.

In April 2017, a group of EU and NATO members, with the participation of EU and NATO representatives, established, in Finland, the European

[110] Rettman A., „Mogherini urged to do more on Russian propaganda", October 20, 2017, https://euobserver.com/foreign/139573, 2017 12 19.

Centre of Excellence for Countering Hybrid Threats.[111] The Centre, situated in the Baltic Sea region, provides a possibility for the Nordic and Baltic countries, as well as Poland, to make the themes of fighting against mixed threats urgent in a broader context as well as draw attention to security challenges of the Baltic Sea region.

The European Union continued the informal dialogue and strengthened the cooperation and coordination of the activity with NATO in the areas of information about situation reporting, cyber security of strategic communications, and crisis prevention and responding to it in countering hybrid threats (certainly, respecting inclusion principles and the independence of the decision-making process of both organizations – political "sensitivities" in expanding cooperation are not in short supply in both organizations). The establishment of the previously mentioned European Centre of Excellence for Countering Hybrid Threats serves well for fostering cooperation between the EU and NATO.

In 2017, in addition to NATO CMX exercises, the European Union conducted *Paralleled and Coordinated Exercises* (PACE) and in 2018, the EU undertook the leading role. Great attention should be devoted as well as to hybrid elements through a scenario, as it's a cose of NATO CMX. PACE was a good first step, but the ambition of the European Union is a joint exercise with a real scenario, at least to begin with, in the area of hybrid and cyber threats.

With Russia's propaganda actions in Ukraine getting stronger, a group of EU and NATO countries established the group "Friends of Ukraine", where information is exchanged, but at the same time it is a platform for communication activities where campaigns helping to keep the issue of Ukraine on the agenda are developed.

Conclusions

Notwithstanding the fact that the phenomenon of hybrid or asymmetric warfare has been known for a long time and Russia's intervention in Ukraine in 2014 made theoretical considerations of the warfare relevant anew, consensus on the definition of hybrid threats at the theoretical level has not yet been reached. Moreover, the discourse over whether the term "hybrid" is not misleading and corresponds to the reality of modern warfare is still continuing. The survey of

[111] „Lietuva dalyvaus kuriant Europos kovos su mišriomis grėsmėmis kompetencijos centrą", *15min.lt*, 2017 04 11, https://www.15min.lt/naujiena/aktualu/lietuva/lietuva-dalyvaus-kuriant-europos-kovos-su-misriomis-gresmemis-kompetencijos-centra-56-782158, 2017 12 20.

the theoretical discourse provided in the study enabled the formulation of the main elements of hybrid warfare and its manifestations. However, further research is necessary to answer the question of how broadly the spectrum of threats attributed to hybrid should be covered, when is hybrid warfare encountered, and when is it only the operation of individual hybrid influences. The authors of the article did not make it their objective to solve these theoretical (and meanwhile influencing the practical level) aspects and so greater attention was paid to the practical survey and assessment of Lithuania's, the European Union's, and NATO's actions in countering hybrid threats. The on-going debate on the content of hybrid warfare and threats is important in making the (non-)security situation in Europe relevant anew as well as developing capabilities to identify hybrid threats and, particularly, searching for practical means to defend from them (to become resilient) at both the national and beyond national level.

The security of the Baltic Sea region is further determined by the continuing militarization of Russia's Western military district, the activity and aggressiveness of its security policy, the determination to restore its zone of influence in the region and the desire to probe the weakness of the West. With Russia's aggression in Ukraine ongoing, we clearly see that Russia, ever more intensely, invests in non-military measures to achieve its objectives in the region that includes the Baltic countries as well. Russia's activities comprise culture policy, informational and cyber-attacks, encouragement of social discontent, destructive diplomacy, rewriting of history, blackmail policies, etc. Hybrid influences (primarily in the informational space) are directed straight to target groups in different countries, while their employment becomes more and more intensive. There are no objective reasons to state that the hybrid operation strategy and tactics chosen by Russia might change in the short or medium period.

Having surveyed the situation in Lithuania, one can clearly see that Russia-caused hybrid threats are a relevant security challenge calling for complex decisions. The enhancement of coordination must be continued at the national level. Lithuania is only creating the coordination of countering hybrid threats though initiatives strengthening the informational security (limitation of direct propaganda, dissemination of information about propaganda and hybrid threats in Lithuanian portals, monitoring of negative and destructive information in subdivisions of Lithuanian institutions responsible for strategic communication (the Ministry of National Defence, the Armed Forces of Lithuania)) have already been started. It would be worthwhile to take over the experience of other states that pay attention to the management of informational threats and seek to provide strategic documents for countering them. In the case of Lithuania, it would also be relevant to codify disinformation and other hybrid threats in national security documents and establish responsible institutions, which could undertake systemic fighting against

hybrid (primarily informational) threats. In establishing new institutions responsible for informational security, the political will and consensus among the main political forces are important in order to guarantee sufficient human resources, budget subsidies, and adequate division of tasks.

As the Lithuanian case indicates, the enhancement of resilience at the national level is going on rather successfully, but this is only the beginning of a long process. The Government of Lithuania needs to further strengthen its preparedness to counter hybrid threats and adjust the crisis management system to new realities so it could also comprise hybrid scenarios, coordinate the activity of all institutions without exception, and enhance the involvement of society in responding to hybrid threats while strengthening the efforts of Lithuanian institutions on the informational front. Challenges awaiting Lithuania force the country to strengthen the backbone of the state and preclude it from thinking this is temporary and will somehow pass.

An important aspect is the protection of elections and the political system. The situation in Lithuania is not unique here. More and more countries are aware that losing the battle for the protection of democracy itself, without ensuring the essence of the democratic system – the free choice of the people – will, in the future, be more difficult to think about widely protecting against hybrid threats.

Another important aspect is the involvement of society. Unpredictability and ambiguity make hybrid threats more complicated for ordinary citizens to identify. Therefore, the state elite, as well as the mass media, face a complex task to explain these threats as clearly as possible in order to strengthen society's resilience to them. It is necessary to support informational pluralism, invest in enhancing civil consciousness through education and culture (a free, curious, and educated society will not swallow such easily recognizable "bait"; a self-aware community will manage to treat critically the operation of hostile forces), encourage fighting against corruption, energy diversification, and invest in rapid reaction to any disseminated disinformation.

Understanding between the European Union and NATO countries about Russia's hybrid actions keeps growing, as more and more decision makers acknowledge the existence of the hybrid threats phenomenon. Yet, in spite of the growing awareness of Russia's actions, there is no joint top political commitment of the EU and NATO to fight against them in earnest. This issue should top the priorities on agendas. However, not only the political support and awareness are important. It is necessary to invest in effective technical and intellectual means meant for watching hybrid threats, analyse them, refute lies and disinformation in the case of informational attacks, and design critical strategies for countering hybrid threats.

Coordinated EU and NATO countermeasures are necessary. Meetings of the EU and NATO officials, sharing of narratives, etc. do take place, however, this should be done more systematically. In an ideal case, at least an informal coordinating community of the EU and NATO experts constantly exchanging information and experience could be formed.

Certainly, in order to respond to unexpected situations – hybrid threats are typical examples of these – the NATO decision-making process should be faster. The Supreme Allied Commander Europe (SACEUR) should grant the authorization to initiate military readiness and response ahead of time.

In the formats of the EU and NATO, the enhancement of resilience is taken seriously. Yet, thought should be given to the idea of how to coordinate these processes. NATO has already begun to implement the decisions of the Warsaw summit concerning the 7 baseline resilience requirements. At the level of the European Union, so far, national assessments in the area of hybrid threats are only talked about. In this field, a greater coordination is also necessary.

Actions accomplished until now have laid a solid foundation for the inter-institutional and trans-national mechanism of countering hybrid threats; however, its effectiveness, purposefulness of measures and compatibility, remain an object of future discussions. It is important for Lithuania, as well as other states experiencing threats of Russia's hybrid influences, to keep the attention of the international community on this issue.

Understanding between specialists and among political leaders about Russia's hybrid activity is increasing. But we have to constantly expand understanding, we need to exchange experience. Hybrid defence is not a static conventional defence. We need to deepen our knowledge of new methods and tools. Another aspect is that we need to expand the awareness of hybrid practices among EU and NATO societies. It is not difficult to get weaken value foundation by promoting antimigrant moods. It is, however, difficult to restore confidence in state institutions.

Summer 2018