The 15th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT IN THE 21st CENTURY"
Braşov, November 12th-13th 2020

BUILDING RESILIENCE AGAINST HYBRID THREATS. TRANSATLANTIC LESSONS LEARNT FROM STATES AND ORGANIZATIONS[1]

BRÂNDA, Oana-Elena, PhD*,
SAULIUC, Adriana, PhD,**

Lecturer in International Relations, Titu Maiorescu University, Bucharest,
Lecturer in International Relations, Titu Maiorescu University, Bucharest

Abstract:

The aim of the present article is to address the main techniques used by states and international and regional organizations alike (with a special focus on NATO and the European Union) in order to assess hybrid threats and create the appropriate response in the form of resilience. In this regard, examples of good practices taken both from countries confronted with such threats(as was the case of the Baltic countries) as well as from organizations which have devised policies and created an institutional framework to deal with such threats, shall be analysed in order to highlight the most productive approaches.

The article shall be constructed in an ascending manner, beginning with a brief analysis of the hybrid threats, followed by the corresponding reactions taken by NATO and the European Union and their particular perspectives on building resilience, and ending with specific examples of countries which had to manage such threats and prevent them from becoming recurrent, as was the case of the Baltic states.

***Key words**: resilience, threats, hybrid, security,*

1. Introduction

In a world which is profoundly changing , in which the issue of the security of international actors transcends the boundaries imposed by the classical approach, the emergence of the hybrid dimension came naturally. This because, even if the interest of states and international organizations in ensuring security remained the same, developments on the ground revealed the preference of some actors to act in areas less used previously, different from those found in the classical approach of security but which may offer even greater advantages in terms of results and in relation to costs and exposure. Therefore, before defining this term, one should take into consideration that such a threat should be looked at and analyzed from the perspective of the evolving character of contemporary conflicts and taking into account the particularities of so-called hybrid threats. An enterprise as necessary as it is complicated, because the hybrid dimension is profoundly different from everything that international actors have known until recently in terms of security. And this is due to the fact that, generally, a hybrid threat is considered to be linked to a situation in which the attacker is using irregular methods in order to dominate, to counter or to defeat a superior force.

For a more adequate understanding of the term and its manifestation, the Second Lebanon War can be analyzed as an eloquent case, especially that this term was used beginning

[1] Article written in the framework of the internal research project entitled "Limitations of public international law in combatting hybrid threats", developed and funded by the Titu Maiorescu University, 2019-2020.

with 2006, when Hezbollah's actions have been perceived as a new lesson in military strategy, the organisation showing all the elements of hybrid warfare: the simultaneous use of a conventional arsenal, irregular forces and guerrilla tactics, psychological warfare, terrorism and even criminal activities, with support from a multi-dimensional organization, capable of integrating very different sub-units, groups or cells into one united, large force [2]. When the term first appeared in the security sector, "hybrid" referred to a non-state actor with military capabilities exclusively associated before with state actors [3]. Then, the hybrid threat was linked to a state or a non-state actor which had the capacity and apparent willingness to employ a hybrid strategy, while this kind of threat was manifested in activities that fell short of direct conventional military action and that could be conducted for extended periods of time [4].

The explanations meant to shed light on this type of threat, out of the need to counter it, enriched the specialized literature, highlighting at the same time the complexity of hybrid threats. Moreover, every international actor that could become a possible target for such threats addressed them both from a theoretical and practical point of view, by creating mechanisms and structures meant to hinder the aggressive actions listed into this category. Also, in the case of the targets and possible targets, for example the EU, NATO, and their member states, it can be observed that more attention is paid to the so-called hybrid aggressors / adversaries, given the fact that the hybrid aggression is very difficult to manage, and its consequences can be extremely detrimental to the security of international actors.

2. Hybrid threats in the EU and NATO approach

The geographical positioning of the eastern border of the space covered by the two organizations near the sphere of interest of the Russian Federation, inevitably transformed NATO, the European Union and their member states into targets of hybrid threats coming or allegedly coming from Moscow. This was highlighted by the increased attention that these actors paid to hybrid actions, out of the desire to implement effective measures to counter threats in this area.

In the case of the **EU**, important documents and reports mentioned the danger generated by the hybrid threats within the European space, the apprehension of this danger being also found in the security strategies of the member states starting with 2014, when Russia's bellicose actions in Europe highlighted the Kremlin's preference for such practices.

Even if the European Union considers counteracting hybrid threats to be the responsibility of states, more recent developments that have put the EU in front of actions designed to affect its cohesion, stability and attractiveness revealed the need for EU involvement in this dimension. Therefore, an important step was made in 2016, when the EU issued a *Joint Communication to the European Parliament and the Council - Joint Framework on countering hybrid threats: a European Union response*, which outlined the Union's answer to the threat posed by the use of hybrid tactics. At that respective moment, the document acknowledged that the responsibility for national security rested primarily with member states, highlighted relevant existing EU work and presented some new proposals for member state and EU action, including closer coordination with NATO [5]. Two years later, in June 2018, the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, issued a joint communication to the European Parliament, the European Council and the Council entitled *Increasing resilience and bolstering capabilities to address hybrid threats*, which highlighted that activities in the hybrid domain conducted by state and non-state actors continue to pose a

serious and acute threat to the EU and its member states, forcing the EU through the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to invest consistent efforts to build-up the EU's capabilities and effectively support member states to counter hybrid and chemical, biological, radiological and nuclear-related threats, while the same document revealed that some important results were obtained in domains like: strategic communications, situational awareness, strengthening preparedness and resilience, and reinforcing crisis response capacities [6].

Another important step was made by the EU is December 2019, when the European Council adopted a set of priorities and guidelines for the EU cooperation in the field of countering hybrid threats and enhancing resilience to these threats, building on the progress made in recent years. Through this initiative, the European Union called for a ***comprehensive approach to security to counter hybrid threats***, working across all relevant policy sectors in a more strategic, coordinated and coherent way [7], contributing thus to the implementation of the EU's Strategic Agenda for 2019-2024, agreed in June 2019 by the European Council. The document stipulated that one of the European Council priorities was "protecting our societies from malicious cyber activities, hybrid threats and disinformation" [8].

At the European level, important efforts were also made by **NATO,** in order to reduce the threat perceived by states and non-state actors especially from the Russian Federation. For this purpose, after the illegal annexation of Crimea, the North Atlantic Alliance laid the foundations of a strategy in order to counter hybrid warfare. In this regard, NATO aims to gather, share and assess information in order to detect and attribute any ongoing hybrid activity, while an important structure - *Joint Intelligence and Security Division* was assigned to improve the Alliance's understanding and analysis of hybrid threats [9].

In 2019, the *Secretary General's Annual Report* dedicated a section to hybrid threats, highlighting their complex character, as they blur the line between peace and war, so countering such actions is considered a priority for the Alliance. In this regard, besides a coherent strategy, NATO is constantly preparing to counter hybrid threats covering a wide range of actions such as: crisis management exercises, consultations at the level of Allied National Security Advisers, establishing a NATO Counter Hybrid Support team [10], an in depth cooperation with other countries / non-state actors etc., all activities aimed at reducing the threats in a very complex dimension - the hybrid one.

All these activities are in line with the many particular actions devised by states in their efforts to counter hybrid threats. Even though all countries could become victims of hybrid threats, some are more prone than others, as this the case of the United States, which is expecting such threats exercised by some of its most powerful competitors, for example the Russian Federation. In order to preempt such a situation, Washington adopted in December 2017 a National Security Strategy which, in the section entitled "Preserve Peace Through Strength" highlighted that adversaries and competitors became adept at operating below the threshold of open military conflict and at the edges of international law [11], indicating their preference for actions which can be catalogued as part of hybrid warfare. In this regard, lt. Gen. Karen H. Gibson, the deputy director of National Intelligence for National Security Partnerships, considered that hybrid warfare, with all its components, is a reality, and the U.S. military must be ready to confront and deter it [12].

The Russian Federation is also seen as an employer of hybrid techniques by Romania. Its geographical proximity determined it to be very proactive in its approach to hybrid threats.

Thus,vthe National Security Strategy for 2020 - 2024 addressed the issue of Russia's aggression and the threat posed by it, bringing into discussion the improvement of its hybrid instruments in recent years [13]. Deeply concerned about these developments, Romania is fully involved, also from the perspective of the EU and NATO membership, in all initiatives and endeavours initiated in order to counteract hybrid aggressions coming from Russia and elsewhere.

3. Lessons learnt from organizations and states

Apart from evaluating the theoretical response of organizations and states to the issue of hybrid threats, it is highly important to assess also examples of how there organizations and states managed such threats throughout time. As far as the organizations are concerned, until present, none of them has underwent hybrid attacks. However, they seem to have taken a very preventive stand, engaging actively in exercises meant to simulate such attacks and devise the appropriate solutions when necessary. Although these exercises are mere simulations of attacks they serve the purpose of identifying those vulnerable infrastructures that could fall prey to hybrid activity.

A noteworthy example of such an effort is the Chimera Exercise, a tabletop exercise on th issue of hybrid threats, conducted under the auspices of the European Commission in a joint efforts reuniting 24 member states, EEA states joined by Serbia and the Republic of Moldova, EU bodies and representatives of the North Atlantic Organization. The exercise focused on key infrastructures such as public health management and the relation to civil protection/security authorities, and was held between January 30th-31st 2018 in Luxembourg. Its main goals were, among others, to ensure the implementation of existing EU legislation on such threats, with a specific emphasis laid on the existing Joint Framework on Countering Hybrid Threats, as well as the Joint EU-NATO declaration, the support of cross-sector relations in order to identify the precise tools that needed to be used in this regard, as well a fast identification of the risks and vulnerabilities that could render member countries feeble in the face of hybridity; furthermore, since this was an exercise, another goal consisted of testing decision-makers, bodies and countries in their capacity to respond to hybrid threats, rapidly and effectively [14]. The conclusions drawn from this exercise on the readiness of actor reaction highlighted the need for better cooperation with NATO, especially on matters reffering to civil protection and security management. Also, the exercises pointed to the need to develop crisis management strategies for all EU member states that could be activated in order to improve standard reaction procedures.

While the European Union still needs to improve its standing and base of reaction regarding hybrid threats, the North Atlantic Treaty Organization has a more pragmatic approach. Its assistance to member states in response to hybrid attacks consists of monitoring, analysing, exchanging intelligence, and providing shared situational awareness [15]. Owing to the many available resources, as well as its nature as a military and political alliance, NATO establishing in 2018 counter-hybird support teams, focusing on offering case by case assistance. The teams were activated for the first time in 2019 in Montenegro [16], in an effort to shelter it from Russian interferences, as these had happened before. Cyber security is highly essential to NATO and in that regard, the Alliance is relying on the examples of good practices derived from the experiences of the Tallinn-based Cooperative Cyber Defence Centre of Excellence, established in 2008, which holds the annual Locked Shields cyber defence exercise. In addition to that, since 2016, NATO has been holding two types of exercises which deal to a larger or smaller extent with hybrid threats. Firstly, there is the annual Crisis Management Exercise (CMX), focusing on

rehearsing decision-makers responses to various types of threats, including hybrid ones. Secondly, there are the live exercises, such as Trident Juncture [17] or Noble Jump [18]which comprised testing of military capabilities and readiness to respond to any kind of threats, hybrid included.

Another element that needs to be assessed consists in the valuable lessons learnt from the countries that have been confronted with such attacks. Starting with 2006 – the war perpetrated by Lebanon against Israel, the road was opened for other actors to engage in hybrid techniques and threats. It is here that the analysis shall focus on examples of such threats, the countering measures taken by those faced with such threats, as well as on several examples of exercises devised by the European Union and NATO in order to evaluate the steps taken by countries and organization in their management of the threat and prevention techniques. The list is not intent to be a comprehensive one, but rather highlight the essential aspects in the management and prevention process.

From a chronological perspective, the first example that comes to mind is that of the Bronze Soldier attack in Estonia in 2007, which was a wake up call for all European countries that attacks can come in various forms. The issue concerned the decision taken in April 2007 by the Estonian Government to remove the statue of the Bronze Soviet Soldier (a Second World War Memorial) from the center of Tallinn to a graveyard on the edge of the city. The movement sparked protests from the Russian -speaking inhabitants of Tallinn who considered it an offense to the Russian minority - the statue was entitled "Monument to the Russian Liberators of Tallinn" and while the Russians of Tallinn considered it to be a tribute to the Russian fight against Nazism, the Estonians did not share the same opinion as for them the Russians were the oppressors. Street protests occurred, followed almost immediately by cyber-attacks against the online services offered by banks, media outlets and government bodies [19]. ATMs were rendered dysfunctional; newspapers were faced with the impossibility of uploading the news in due time and government websites were affected as well. The attacks lasted for weeks, having all stakeholders involved in a fast-track race to get these utilities up and working. The attacks were launched from Russian IPs and the instructions were delivered in Russian language – however, these were insufficient in building a case of Russian governmental involvement in the attacks. As a result of the attack, Estonia started building its cyber-defense, with its top IT specialists trained by the Estonian Ministry of Defence, vetting them for security purposes and keeping their identities anonymous. In addition to state policies, which include regular trainings on how to deal with a major crisis, should one of the most important utilities fell prey to a cyber-attack, a particular attention was also given to the Cyber Defence Unit of the Estonian Defence League which heightened the training of its volunteers, especially after 2014 annexation of Crimea.

The attack revolving around the Bronze Soldier Memorial of 2007 was the debut of the country's development of cyber competences, which may put Estonia today at the top of the list of countries able to be proactive in their dealing with cyber threats.

The Baltic countries remained a center of interest for the Russian Federation in conducting hybrid threats. In the past years, Latvia, Lithuania and Estonia underwent cyber attacks against their energy grids, raising concerns regarding the security of the latter, as well as the overall security of the North Atlantic Alliance of which the three countries are members [20]. Russian involvement in Baltic power grids was justified by the fact that all three countries are still connected with the Russian network, but are currently undergoing efforts to separate and integrate with the EU network. Apart from these, cyber attacks began in 2015, aiming not to

cause disruptions within the systems, but rather to act as surgical testing of means of action within the respective systems, highlighting the fact that although apparently insignificant at the moment, the attack was meant to create a long term chain reaction that could engender, in terms of weeks leading to months, the demise of not just the first infected system, but also of adjacent and connected others.

The Maersk shutdown of 2017 is such an example of a hybrid threat that created a chain reaction. On June 27th, 2017, the GoldenEye/ Petya virus infected one of the computers of the A.P. Moller-Maersk MAERSKb.CO shipping company. The company is the largest container shipping line and also operator of over 76 port terminals all over the world. As a result of the attack, shipping and management of shipping products was put on hold for several days after the attack. The most severely hit were the shipping terminals of India, Spain, the Netherlands and the United States. As most goods are shipped worldwide, the attack not just damaged the company's computer systems, but also prevented goods (ranging from food to oil and gas products) from reaching the destination in time, due to the impossibility of the computer systems to manage the entrance and exit of goods from ports [21].

While Maersk was considered to be leading in terms of shipping and IT management of transport, the crisis it underwent in 2017 highlighted the fact that the shipping industry worldwide is insufficiently protected against cyber threats. The aim of the attack was not to prevent the average consumer from receiving his/her goods, but rather to point out that all systems based on IT technology can ultimately fail when attacked. Furthermore, any cyber interference with the electronic navigation devices such as the Global Positioning System (GPS) can lead to changes in the course of navigation and even collisions, resulting in loss of life and cargo and even blocking passage routes. Should one such collision occur in critical areas, for instance in one of the highly transited straits, it would result also in the disruption of transport routes, forcing others to find alternative routes, which would imply longer periods of transport, failure of goods (should they be perishable) and higher costs.

This leads one to another example of a hybrid threat perpetrated in 2016, allegedly by North Korea, although there was no confirmation of its involvement. In April 2016, South Korean authorities claimed that North Korea used radio waves to jam the GPS navigation system in the border regions close to South Korea. The jamming affected all types of transportation systems, including air and train traffic. Furthermore, South Korean authorities claimed that more than 70 fishing boats had to return to the ports as they lost GPS signal while at sea [22]. However, this appeared to be no singular event, as since 2010, several other hybrid attacks occurred. While North Korea denied any such involvement, researchers claim that the use of asymmetrical tactics would be the only available solution to successfully wage a war against South Korea[2].

4. Conclusions

The aim of the present article has been to step over the classical analysis of hybrid threats from a theoretical perspective and assess them based on the examples of various international actors dealing with them. It is here that the authors focused on the manner in which different

[2] Franz-Stefan Gady, "Military Stalemate: How North Korea Could Win a War with the US", *The Diplomat*, 10 October, 2017, https://thediplomat.com/2017/10/military-stalemate-how-north-korea-could-win-a-war-with-the-us/.

states and organizations approached hybrid threats throughout time. The role of this investigation is to extract the lessons learnt from the management of attacks and possibly emulate them, to a certain extent, should they occur in real life. No attack resembles the other, as it is influenced by the country in which it occurred, by the specific moment in time and the intended impact. However, it is highly important to establish patterns of response that can be implemented on various occasions, when hybrid activity is involved. On account of the degree of instability and uncertainty that governs the production and manifestation of hybrid threats, international actors, be they states or organizations need to coalesce all available forces to resist the attack. In that regard, public-private partnerships and the engagement of more actors in exercises would be a real asset in shaping state policies on hybrid attack management, which would constitute an advancement for may countries, which are still focused on combatting the threat on a theoretical basis by simply mentioning it in a national security strategy, or any other state related document

References:

[1] Marcin Andrzej Piotrowski, *Hezbollah: The Model of a Hybrid Threat,* Bulletin, No. 24(756), March 2nd, 2015, The Polish Institute of Intrenational Affairs, https://www.files.ethz.ch/isn/188946/Bulletin%20PISM%20no%2024%20(756)%202%20March%202015.pdf, p.1.
[2] Sascha-Dominik Bachmann, Håkan Gunneriusson, *Hybrid wars: the 21st centuryţs new threats to global peace and security,* Scientia Militaria, South African Journal of Military Studies, Vol 43, No. 1, 2015, pp. 77 – 98. doi: 10.5787/43-1-1110, https://ung.edu/institute-leadership-strategic-studies/_uploads/files/bachmann-gunneriusson-hybrid-wars-16-sep-2016-scientia-militaria.pdf?t=1569110400096.
[3] *Hybrid Threats:Overcoming Ambiguity, Building Resilience,* NATO Energy Security, Centre of Excellence, No. 11, 2017, https://enseccoe.org/data/public/uploads/2017/03/zurnalas_no11_sp_176x250mm_3mm_2.pdf, p. 6.
[4] JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL - Joint Framework on countering hybrid threats: a European Union response, Cabinet Office, European Memoranda, http://europeanmemoranda.cabinetoffice.gov.uk/memorandum/joint-communication-to-the-european-parliament-the-council-joint-framework-on-countering-hybrid-threats-european.
[5]*JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL. Increasing resilience and bolstering capabilities to address hybrid threats*, Brussels, 13 June 2018, https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf.
[6]*Countering hybrid threats: Council calls for enhanced common action, European Council, Council of the European Union,* 10 December 2019, https://www.consilium.europa.eu/en/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/.
[7]*A new strategic agenda for the EU 2019 - 2024*, European Council. Council of the European Union, 21 June 2019, https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/.

[8]*NATO's response to hybrid threats,* North Atlantic Treaty Organisation, 8 August 2019, https://www.nato.int/cps/en/natohq/topics_156338.htm.
[9]*The Secretary General's Annual Report, 2019*, NATO Public Diplomacy Division, Brussels, 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf, p. 29.
[10]Aurel Sari and Arnis Lauva, *Hybrid Threats and the United States National Security Strategy: Prevailing in an "Arena of Continuous Competition"*, Blog of the European Journal of International Law, 19 January 2018, https://www.ejiltalk.org/hybrid-threats-and-the-united-states-national-security-strategy-prevailing-in-an-arena-of-continuous-competition/.
[11]Jim Garamore, *Military Must Be Ready to Confront Hybrid Threats, Intel Official Says,* U.S. Dept of Defense, 4 September 2019, https://www.defense.gov/Explore/News/Article/Article/1952023/military-must-be-ready-to-confront-hybrid-threats-intelligence-official-says/.
[12] Kamil Calus, *Romania's new security strategy*, OSW, 15 July 2020, https://www.osw.waw.pl/en/publikacje/analyses/2020-07-15/romanias-new-security-strategy.
[13] ***, *Exercise Chimera. Report on the tabletop exercise on hybrid threats involving public health and civil protection/security authorities*, 30-31 January 2018, Luxembourg, https://ec.europa.eu/health/sites/health/files/preparedness_response/docs/2018_hybridthreatsexercise_en.pdf, pp. 8-9.
[14] Piotr Szymanski, *Towards greater resilience: NATO and the EU on hybrid threats*, 24 April, 2020, https://www.osw.waw.pl/en/publikacje/osw-commentary/2020-04-24/towards-greater-resilience-nato-and-eu-hybrid-threats#_ftn7.
[15]Slobodan Lekic, *First NATO Counter-hybrid warfare team to deploy to Montenegro*, 8 November 2019, https://www.stripes.com/news/first-nato-counter-hybrid-warfare-team-to-deploy-to-montenegro-1.606562.
[16]***, *NATO Secretary General briefs on exercise Trident Juncture*, 24 October, 2018, https://www.nato.int/cps/en/natohq/news_159663.htm.
[17]***, *Noble Jump 19*, https://jfcnaples.nato.int/exercises/noble-jump.
[18]Damien McGuinness, *How a cyber attack transformed Estonia*, 27 April, 2017, https://www.bbc.com/news/39655415.
[19] Stephen Jewkes, Oleg Vukamnovic, *Suspected Russia-backed hackers target Baltic energy networks*, 11 May 2017, https://www.reuters.com/article/us-baltics-cyber-insight-idUSKBN1871W5.
[20]Jonathan Saul, *Global shipping feels fallout from Maersk cyber attack*, Reuters, 29 June, 2017, https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19K2LE.
[21]***, "North Korea jamming GPS signals near South border", *BBC News*, 1 April, 2016, https://www.bbc.com/news/world-asia-35940542.
[22]Franz-Stefan Gady, "Military Stalemate: How North Korea Could Win a War with the US", *The Diplomat*, 10 October, 2017, https://thediplomat.com/2017/10/military-stalemate-how-north-korea-could-win-a-war-with-the-us/