EU - NATO COOPERATION TO COUNTER HYBRID THREATS

Snežana Nikodinovska-Stefanovska, PhD[1]
Marjan Gjurovski, PhD
Faculty of Security, Skopje, University "St. Kliment Ohridski", North Macedonia

Abstract: The current and foreseeable security landscape looks increasingly 'hybrid' in nature. Hybrid operations and tactics combine military and non-military as well as covert and overt means, including cyber-attacks, disinformation campaigns, use of irregular groups and regular armed forces, espionage, sabotage, economic pressure and personal coercion. The strategic aim of such activities is to blur the lines between peacetime, crisis and conflict – to sow doubt and to foment divisions. The speed, scale and intensity of hybrid threats have increased in recent years. Responsibility for building resilience against, and responding to, hybrid attacks lies primarily with individual states. However, it is impossible to deal with the range of such threats alone. Given the multitude of domains and individuals potentially affected, as well as the cross border nature of many hybrid activities, more cooperation is required at all levels. Being prepared to prevent, counter and respond to hybrid attacks, whether by state or non-state actors, is a top priority for NATO as well as for the EU. The purpose of the article is to explain the meaning and the content of hybrid threats and hybrid warfare, having in mind that various definitions of hybrid threats and warfare exist, as well as the cooperation between EU and NATO in countering them. To explain the meaning and the content of hybrid threats and hybrid warfare various definitions of the security analysts and practitioners, policy-makers as well as international organizations and bodies will be analysed. Also, in order to examines and explain recent development of the EU-NATO cooperation in countering hybrid threats official documents of both organizations will be analyzed. Countering hybrid threats has quickly become a central vehicle for strengthened cooperation between NATO and the European Union, based first on mutual interest. The analysis of complex challenges facing the EU and NATO led both organisations to develop a comprehensive approach that blends all relevant actors and available instruments: military forces, diplomacy, humanitarian aid, political processes, economic development, and technology. NATO and the EU could create an effective institutional tandem that has a wide range of both political and military instruments at its disposal.

Keywords: security, hybrid warfare, hybrid threats, European Union, NATO.

1 snikodinovska@gmail.com

INTRODUCTION

Hybrid threats have become the 21st security challenge for Western countries. They reflect significant change in the nature of international security. The picture of the security environment is not simply black or white. It is complex, multi-layered and multi-dimensional. Thus, analysis of what has changed, how it is changed and what does it mean for democratic states is at the core of understanding the nature of the current security environment in Europe.

Six major changes are driving hybrid threats to the fore. The first is the changing nature of world order. The post-Cold War era has ended. Relational power[1]– that is the power to change others' beliefs, attitudes, preferences, opinions, expectations, emotions and/ or predispositions to act – is today more important than material power.

Second, the world sees a new type of network-based action. The internal and external dimensions of security are interconnect more strongly than they were in recent decades.

Third, fast developing technologies give rise to new domains like cyber space where national and international rules of the game have to be created.

The changing domain of information space, and the media landscape, is the fourth major change affecting today's security environment. The Internet has become a new battlefield where rules are not still formulated.

The fifth change is the changing nature of conflict and war. In today's wars, soldiers should not die and civilian casualties should be avoided. This has led to the debate about the blurred lines between war and peace.

Finally, there is generational change. The Cold War and even the post-Cold War era are behind us. The Cold War had two very distinct features, which underpinned a clear world order: superpower relations – and the ideological struggle between communism and capitalism – dominated, while the fear of nuclear war guided many security policy decisions. During the post-Cold War era, globalization, emphasizing ideas of integration and interdependence, became the fashionable way of describing the world. Today's new generation is a digital generation informed by two contradictory trends – cosmopolitanism and neo-nationalism. Historical memory also changes along with generations, which leaves space for the political manipulation of historical events.

The changes in Europe's security environment raise important questions regarding the responses of the international organisations. When a country is attack by conventional land, sea or air forces, it is usually clear how to best respond. What happens when it is attacked by a mixture of special forces, information campaigns

1 Relational power is the perception of one unit's ability to influence others in a specific bilateral or multilateral relationship. https://www.google.com/search?ei=ZFEHXYS-J5qo1fAP4bqc2A8&q=relational+power&oq=relational+power&gs_l=psy-ab.3..0i203l10.51954.54415..55803...0.0..0.291.1065.0j4j2.....0....1..gws-wiz.WtLlCLvnX58

and backdoor proxies? What is the best response and how can international security organisations like NATO and EU adapt to these attacks?

In response to the changing security environment, the EU and NATO need new strategies or policies. The new world requires a strategic relationship instead of a set of military-technical arrangements between the EU and NATO. This might also have consequences for the capacities that the two organisations should be able to deploy. What should be the priorities for each of them? How can the capacities of the EU and NATO be synchronised in order to realise a more systematic, coherent and efficient response by Europe and North America to the changing world?

THE "HYBRID THREATS" AND "HYBRID WARFARE" - INTRODUCTION TO THE TERMS

Security analysts and practitioners have a tendency to coin new terms, which capture the challenges they are facing. Terms such as 'low-intensity conflicts', 'failed' or 'fragile' states, 'asymmetrical' threats or even, for that matter, 'comprehensive approach' are all relevant examples. 'Hybrid threats' and 'hybrid warfare' are potentially, another case in point.

As hybrid threats to international security have been evolving, their use in scholarly and policy debates has become a source of on-going confusion. In many instances, it can be noticed that the concepts such as 'hybrid threat' and 'hybrid war' or 'hybrid warfare' are used randomly, without even providing a working definition for the terms. This has led to the further confusion of the policy-makers instead of much needed conceptual clarification. The very term 'hybrid' refers to something heterogeneous in origin or composition (a mixture or a blend), or something that has "two different types of components performing the same function" (Merriam Webster Online Dictionary).

The concept of 'hybrid threats' is not new. The term appeared at least as early as 2005, and was used specifically to describe Hizbollah's strategy in the 2006 war with Israel. The concept of hybrid threat has been revived in relation to Russia's actions in Ukraine and the ISIL/Da'esh campaigns going far beyond Syria and Iraq. However, elements of hybridity can be traced in many other dimensions of the current security environment.

Hybrid threat is a phenomenon resulting from the convergence and interconnection of different elements, which together form a more complex and multidimensional threat. The term 'hybrid threat' is a metaphor that captures complexities and dilemmas related to a changing global environment. As such, it is a useful concept that embraces:

- the interconnected nature of challenges (i.e. ethnic conflict, terrorism, migration, and weak institutions);
- the multiplicity of actors involved (i.e. regular and irregular forces, criminal groups); and

- the diversity of conventional and unconventional means used (i.e. military, diplomatic, technological).

In an analysis devoted explicitly to what he called "not-so-new warfare," Frank Hoffman, of the U.S. National Defense University, defined the hybrid threat as, "Any adversary that simultaneously employs a tailored mix of conventional weapons, irregular tactics, terrorism, and criminal behavior in the same time and battlespace to obtain their political objectives" (Hoffman , 2014).

According the definition of the European Center of Excellence for Countering Hybrid Treats (Hybrid CoE) hybrid threats can be characterized as coordinated and synchronized action that deliberately targets democratic states' and institutions systemic vulnerabilities, through a wide range of means. Activities exploit the thresholds of detection and attribution as well as the border between war and peace. The aim is to influence different forms of decision-making at the local (regional), state, or institutional level to favor and/or gain the agent's strategic goals while undermining and/or hurting the target (Hybrid threats, n. d.) .

Definition used in Joint Communication of 6.4. 2016 (JOIN(2016) 18) is: Hybrid threats can be characterised as a mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological, information), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of open organised hostilities.[2] There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity with the intention to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalise, recruit and direct proxy actors can be vehicles for hybrid threats.

The document titled 'NATO 2020', prepared by a group of 'wise persons' for the 2010 NATO Lisbon Summit note the 'hybrid variations' of threats (NATO 2020, 2010: 15). The 2014 NATO Wales Summit Final Declaration refers to 'hybrid warfare threats' where "a wide range of overt and covert military, paramilitary, and civilian measures are employed in a highly integrated design" (Wales Summit Declaration, 2014). Furthermore, the 25 June 2015 Statement by NATO Defence Ministers talks about 'hybrid threats', for which "we will seek close coordination and coherence with the European Union's efforts in this field" (Statement by NATO Defence Ministers, 2015).

For a threat to be of a 'hybrid' nature it needs to be the product of multiple ways to threaten or attack its intended target – much as a hybrid species is produced by combining different breeds or varieties. It is therefore the mix of different methods – conventional and unconventional, military and non-military – that makes a threat hybrid. In this sense, not all contemporary threats are hybrid. Terrorism, cybercrime, trafficking and extortion are not *per se* hybrid in nature;

2 This definition is, also, used in JOINT STAFF WORKING DOCUMENT EU operational protocol for countering hybrid threats 'EU Playbook' (SWD(2016) 227 final)

they may become so depending on how (and to what extent) they are pursued using multiple tactics simultaneously (Anderson & Tardy, 2015:.2).

In general terms, hybrid threats are characterized by:

- the combination of conventional and unconventional, military and non-military, overt and covert actions;
- the aim of creating ambiguity and confusion on the nature, the origin and the objective of the threat;
- the ability to identify and exploit the vulnerabilities of the targets;
- the capacity to keep the level of hostility below the 'threshold' of conventional war (Anderson & Tardy, 2015:2).

Since the start of the Ukrainian conflict, a new buzzword has dominated the international security debate: hybrid warfare. Russia's recent behavior and actions are often refer to as 'hybrid warfare'. They have been an effective and sometimes surprising mix of military and non – military, conventional and irregular components, and can include all kinds of instruments such as cyber an information operations. It is the combination and orchestration of different actions that achieves a surprise effect and creates ambiguity, making an adequate reaction extremely difficult, especially for multinational organizations that operate on the principle of consensus.

However, hybrid warfare is not a new invention by Russia. The idea of using unconventional means and actors in conflict is not new. In fact, it is as old as warfare itself. [3] In his speech, NATO Secretary General Stoltenberg reiterated that '… the first hybrid warfare we know of might be the Trojan Horse, so we have seen it before" (Stoltenberg, 2015). According to P.M. Breedlove"… new things are how these tools that we have recognize from before are now put together and used in new ways to bring new kinds of pressure" (Breedlove , 2015).

Propaganda, economic blockades and covert activities have been used in many international confrontations in combination with full-scale war. Both World Wars in the previous century serve as examples. What is new in the 21st century is the greater effect of hybrid warfare due to the innovation in means and methods combined with increasing economic global interdependencies. The internet and the media offer unprecedented scope for generating domestic support as well as influencing the 'opponent'. The cyber domain is not just a modern realm for espionage; it can also be used offensively, for example to disrupt communication

3 For example the Cambridge publication „Hybrid Warfare *Fighting Complex Opponents from the Ancient World to the Present*" shows that the combination of different tactics and combats is not a modern military strategy but existed even during the ancient world, it is the term that is newer (Murray&Mansor, 2012). Nicu Popescu in his paper "Hybrid Tactics: neither new nor only Russian" says that such combinations of unconventional tactics "are as old as war itself" and Western states used to use them effectively on the tactical level themselves. (Popescu, January, 2015) Similarly Michael Kofman and Matthew Rojansky in their article "A Closer Look at Russia's 'Hybrid War'" (Rojansky, 2015, p. 2) say that the term is „as old as warfare itself". Some of the mentionable examples of hybrid warfare are the conflicts of Hezbollah movement in Lebanon, Georgia, Russian invasion in Afghanistan, Spanish Guerrillas during Napoleon's Spanish invasion and many others.

networks or other essential enablers for combat forces. Distance and time offer no protection against such a threat – this is very different from the classical danger posed by armies and fleets. In addition, closing the valve of a gas pipeline can paralyse society in a country that is largely dependent on energy imports.

A critically important aspect of hybrid warfare is to generate ambiguity both in the affected population under attack as well as in the international community. The aim is to mask what is actually happening on the ground in order to obscure the differentiation between war and peace. This ambiguity, the lack of full attribution, can paralyze the ability of an opponent to react effectively and mobilize defense as it becomes unclear who is behind an attack. Even more, ambiguity can divide the international community, limiting the speed and scope of a response to the aggression.

General Valery Gerasimov, Russia's Chief of General Staff, whose often cited 2013 article stated that, "the rules of war have cardinally changed," and that the effectiveness of "non-military tools" in achieving strategic or political goals in a conflict has exceeded that of weapons. According to General Gerasimov, this new generation of warfare includes the following elements:

- Military action is started during peacetime (without declaring war);
- Non-contact clashes between highly maneuverable specialized groups of combatants;
- Annihilation of the enemy's military and economic power by quick and precise strikes on strategic military and civilian infrastructure;
- Massive use of high-precision weapons and special operations, robotics, and technologically new weapons;
- Use of armed civilians;
- Simultaneous strikes on the enemy's units and facilities throughout all of its territory;
- Simultaneous battles on land, air, sea, and in the information space;
- Use of asymmetrical and indirect methods;
- Management of combatants in a unified information system (Gerasimov, 2013).

COUNTER HYBRID THREATS: A CHANCE FOR NATO AND THE EU TO WORK TOGETHER?

Countering hybrid threats is about gaining new understanding of such threats and the innovative use of existing capabilities, many of which – like economic development, the fight against corruption or eliminating poverty – reside in nonmilitary governmental and intergovernmental agencies, private sector and international nongovernmental organizations. The analysis of complex challenges facing the EU and NATO led both organizations to develop a comprehensive

approach that blends all relevant actors and available instruments: military forces, diplomacy, humanitarian aid, political processes, economic development, and technology.

Since 2016, NATO and the European Union have identified countering hybrid threats as a priority for cooperation. Acknowledging the need for dialogue and coordination with likeminded partners in countering hybrid threats, the EU's joint communication (JOIN (2016) 18 final) and "EU Playbook" (SWD (2016) 227 final) [4] identified a number of areas for closer EU-NATO cooperation, including situational awareness, strategic communications, cybersecurity, and crisis prevention and response. Namely, in 2016, the European Commission and the EEAS developed a joint framework on countering hybrid threats, containing 22 actions for member states and the institutions that set out ways to recognize hybrid threats, improve awareness thereof, and take steps to build resilience (Nikodinovska-Stefanovska, 2018:74-75). Although the actions are by no means exhaustive, the framework established a clear ambition to make countering hybrid threats an EU priority. The most tangible effects were the establishment of a Hybrid Fusion Cell as part of the EU Intelligence and Situation Centre, and a European Centre of Excellence for Countering Hybrid Threats in Helsinki.

The commitment to a deeper partnership with NATO in countering hybrid and cyber threats was also expressed in the European Union global strategy of June 2016. At the European Council on 28 June 2016 EU - NATO cooperation was discussed. It contributed to the adoption of the EU-NATO Joint declaration at the NATO Summit in Warsaw (8-9 July 2016).

Hybrid threats also rose to the top of NATO's agenda following the appearance of "little green men" in Crimea in 2014, which created an acute awareness of how military force could be used in the Euro-Atlantic area below the legal threshold of war. NATO was quick to adopt a strategy to counter hybrid threats based on a horizontal "all-of-NATO" approach. Similarly, to the European Union, NATO has created a capability to monitor and analyze hybrid threats, based in the intelligence community and cooperating with other NATO authorities. Furthermore, NATO has established counter hybrid support teams that can be sent in support of the Allies upon their request, in preparing and responding to hybrid activities (NATO's response to hybrid threats, 2018).

NATO Secretary General Jens Stoltenberg and European Commission and Council Presidents Jean-Claude Juncker and Donald Tusk signed a joint declaration in Warsaw in July 2016.The joint declaration set out a "common set of proposals" with 74 concrete actions, many of which focus on hybrid threats, building resilience in cyber security, and strategic communications (Nikodinovska-Stefanovska, 2018: 75-76). A second joint declaration agreed in Brussels in July 2018

4 This document is prepared in order to implement Action 19 of the Joint Framework, which foresee a "common operational protocol between Member States, the Commission and the High Representative is to outline effective procedures to follow the case of the hybrid threat, from the initial identification phase of the attack to the final phase of the attack, and mapping the role of each Union institution and actor in the process".

provided an additional focus on military mobility, counter-terrorism and resilience to risks posed by chemical, biological, radiological and nuclear agents (Joint Declaration on EU-NATO Cooperation, 2018).

In addition to giving NATO-EU cooperation a long-awaited platform of common interest, countering hybrid threats has led to some other important new developments in the European Union. The European Commission and the EEAS have set up an inter-service group for countering hybrid threats that meets regularly at different levels. This group – designed to ensure common awareness of events and processes throughout European institutions relevant to countering hybrid threats – is a promising first step towards a comprehensive model for security-related challenges. Ideally, it could lead to a more solid platform for civil and economic preparedness, cyber security and other inherently multi-sectoral issues.

Furthermore, the European Council Friends of the Presidency Group for Countering Hybrid Threats (FoP) has been awarded an extended and significantly broadened mandate, stretching through the next four presidencies until June 2020 (Cooperating to counter hybrid threats, 2018). Whereas the initial FoP mandate from 2017 was very limited, the new one call for an overview of ongoing EU efforts on countering hybrid threats, so as to spot shortfalls, avoid duplication, and support political decision making across Council bodies. By the end of the new mandate, the FoP could even become a permanent body responsible for maintaining cross-sectoral awareness and – similarly to NATO's Civil Emergency Planning Committee – supporting member states' civil preparedness and thereby their resilience against hybrid threats (Insitutional Framework for Countering Hybrid Threats, n.d., point.6).

One key field where cooperation between the European Union and NATO should be intensified is training and exercises. Multi-faceted, complex exercises that test the ability to respond to hybrid threats below the threshold of war would be a particularly ideal area for the two organisations to explore their strengths and weaknesses, and perhaps discover complementarities. In September, an informal meeting of the North Atlantic Council (NAC) with the EU Political and Security Committee (PSC) included a hybrid scenario-based discussion facilitated by the Hybrid CoE (Insitutional Framework for Countering Hybrid Threats, n.d., point.7). This initiative should become a recurring element of future NAC-PSC deliberations, and other joint meetings as appropriate.

Joint exercises could also be designed to link up functional counterparts in EU and NATO institutional structures around a mutually relevant hybrid threat scenario, supported by the CoE. Furthermore, the NATO School in Oberammergau and the European Security and Defence College could open up their training courses for selected EU and NATO staff respectively (Insitutional Framework for Countering Hybrid Threats, n.d., point. 8).

CONCLUSION

Countering hybrid threats has quickly become a central vehicle for strengthened cooperation between NATO and the European Union, based first on mutual interest. Hybrid threats are diverse and ever changing, and the tools used range from fake social media profiles to sophisticated cyber attacks, all the way to overt use of military force and everything in between. Hybrid influencing tools can be employed individually or in combination, depending on the nature of the target and the desired outcome. As a necessary consequence, countering hybrid threats must be an equally dynamic and adaptive activity, striving to keep abreast of variations of hybrid influencing and to predict where the emphasis will be next and which new tools may be employed.

To counter hybrid threats the EU has a wide range of instruments at its disposal, from sanctions, trade agreements and imposing anti-trust charges to CSDP missions and operations. However, the effectiveness of EU counter-measures will largely depend on successful coordination of all policies, tools and means available to the EU and its member states. The common policy framework for countering hybrid threats is an important prerequisite for such coordination.

NATO should consider a more flexible policy and strive to deter prospective adversaries with a wide range of instruments. By partnering with the EU and expanding its set of instruments, the Alliance will be able to tackle the threat from multiple angles. What is more, it may be even able to prevent it.

The EU seems the organisation best suited to complement NATO's crisis management efforts, as it offers a diversity of instruments that can be employed in hybrid warfare. NATO and the EU could create an effective institutional tandem that has a wide range of both political and military instruments at its disposal. The NATO Summit in Wales acknowledged the EU as a strategic partner of the Alliance. Moreover, the common threat of hybrid warfare within the Euro-Atlantic area presents a solid opportunity to develop this partnership even further.

The EU and NATO can become a stronger force by coordinating and cooperating with each other more closely. The new challenges and threats leave no other choice. It is the primary responsibility of all member states of both organisations to make this happen, by setting aside the heritage of the past and by focusing on the strategic needs of today and tomorrow.

REFERENCES

1. Anderson, J. J. & Tardy, T. (2015, October). Hybrid: what's in the name? *Brief Issue*, 32.
2. Breedlove, M. P. (2015, March 24). Le général Breedlove et the Hybrid War. Accessed on May 16, 2019. https://www.dedefensa.org/article/le-general-breedlove-et-the-hybrid-war

3. Cooperating to counter hybrid threats. (2018, November 23). *NATO Review magazine*. Accessed on May 25, 2019. https://www.nato.int/docu/review/2018/Also-in-2018/cooperating-to-counter-hybrid-threats/EN/index.htm

4. Gerasimov, V. (2013, February 27). "The Value of Science in Anticipating" [in Russian], Military-Industrial Courier. Accessed on April 20, 2019. http://www.vpk-news.ru/articles/14632.

5. Hoffman, F. (2014, July 28). "On Not-So-New Warfare: Political Warfare vs. Hybrid Threats," War on the Rocks (blog). Accessed on May 10, 2019. http://warontherocks.com/2014/07/on-not-so-new-warfare-political-warfare-vs-hybridthreats/.

6. Hybrid threats. The European Centre of Excellence for Countering Hybrid Threats. Accessed on May 10, 2019. http://www.hybridcoe.fi/hybrid-threats/

7. Insitutional Framework for Countering Hybrid Threats Accessed on Jun 30, .2019. http://www.information-book.com/warfare-hybrid-threats/hybrid-threats/

8. Joint Communication to the European Parliament and the Council JOIN (2016) 18 of 6.4.2016, Joint Framework on countering hybrid threats – a European Union response.

9. Joint Declaration on EU-NATO Cooperation. (2018, July 8-9). Accessed on May 20,.2019. https://www.nato.int/cps/en/natohq/official_texts_156626.htm?selectedLocale=en

10. JOINT STAFF WORKING DOCUMENT EU operational protocol for countering hybrid threats 'EU Playbook' (SWD (2016) 227 final).

11. Kofman, M.& Rojansky, M. (2015) . A Closer look at Russia's "Hybrid War". Accessed on April 15, 2019. https://www.files.ethz.ch/isn/190090/5-KENNAN%20CABLE-ROJANSKY%20KOFMAN.pdf

12. Merriam Webster Online Dictionary, Accessed on April 15, 2019. http://www.merriam-webster.com/dictionary/hybrid

13. Murray, W. & Mansoor, P. (2012) Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present, New York: Cambridge University Press.

14. NATO 2020: assured security; dynamic engagement. (2010, May 17). Accessed on April 25, 2019. https://www.nato.int/strategic-concept/expertsreport.pdf

15. NATO's response to hybrid threats. (2018, Jul 17). Accessed on May 20, 2019. http://www.nato.int/cps/en/natohq/topics_156338.htm

16. Nikodinovska-Stefanovska, S. (2018). EU Policy on Fighting Hybrid Threats, *Security, Political and Legal Challenges of Modern World,* Conference proceedings, Bitola, 70-79.

17. Popescu, N. (2015, January). "Hybrid Tactics: neither new nor only Russian". Accessed on April 25, 2019. https://www.iss.europa.eu/.../hybrid-tactics-neither-new-nor-only-russian

18. Statement by NATO Defence Ministers. (2015, June 25). Accessed on April 25, 2019. https://www.nato.int/cps/en/natohq/news_121133.htm?selectedLocale=en

19. Stoltenberg, J. (2015, March 20) "Zero-sum? Russia, Power Politics, and the Post-Cold War Era, Brussels Forum.

20. Wales Summit Declaration, (2014, September). Accessed on April 15, 2019. . https://www.nato.int/cps/en/natohq/official_texts_112964.htm