



A Changing Security Paradigm. New Roles for New Actors – The Russian Approach

Mirosław Banasik

University of Lower Silesia, Wrocław, Poland, <http://www.uls.edu.pl>

Abstract: The success of the Russian Federation in Ukraine and the annexation of Crimea attest to the fact that the hybrid warfare constitutes an effective tool for achieving political objectives. This article evaluates the nature of hybrid warfare based on theoretical publications on the art of war and doctrinal documents of the Russian Federation, and characterizes the practical dimensions of hybrid warfare. It can be concluded on that basis that hybrid warfare and organized crime constitute real threats to European safety and security. International organizations such as NATO and the European Union so far have not drawn up neither the strategy nor effective tools for countering these phenomena.

Keywords: Hybrid warfare, organized crime, threats, Russian Federation, NATO, European Union.

Introduction

In 2014, the Russian Federation conducted two separate phases of operations in Ukraine. Despite substantial differences in the objectives of and methods used within the operations, it is worth noting that their natures have much in common. Both operations were planned and conducted in accordance with the doctrine followed by Gerasimov and on the basis of the concept hybrid warfare. The successes achieved indicate that hybrid war is an effective tool that enables the Russian Federation to realize its strategy and achieve its national goals. On the other hand, it should be recognized that, in breaching the territorial integrity of Ukraine during annexation of Crimea, international law was violated. Nonetheless, Russia was able to reach its goals by using hybrid tactics and without issuing an explicit declaration of war, and exerts pressure with regular army sub-units stationed along the border with Ukraine. This proves its

determination to use armed force when non-military measures fail.¹ Through its actions, Russia gives rise to concerns among neighboring countries who have issued official notice of the use of hybrid warfare against them.² Moreover, Russia is attempting to give its geostrategic position and autocratic, centralized regime superpower status. Its approach to large-scale conflict involves coordinated diplomatic, informative, cybernetic, economic and military operations, and the core of its strategy aims at impacting on the center of gravity of an adversary in all possible dimensions, while maintaining self-protection.³ In western publications the model of planned aggregate impact in various spheres is often referred to as “unconventional or political war.”⁴ Large-scale destabilization of neighborhoods, multiplicity of ambiguous, masked threats and tough, unambiguous aggression not only have a negative influence on regional security, but also cause internal divisions within international organizations.⁵

This article aims to assess the hybrid threats to European security. The article presents the results of research developed by exploring the following issues: 1) How is the concept of hybrid warfare expressed and what role does organized crime play in hybrid warfare? 2) What kind of challenges and threats does hybrid warfare pose for NATO and the EU and what is the reaction of these organizations to it?

Hybrid Warfare in Theory and Practice

Hybrid warfare as a particular combination of conventional and irregular operations has been known for centuries. Since ancient times, one of the main aspects of military warfare has been correctly recognizing the current situation and adapting one’s conduct accordingly.⁶ It is unavoidable that, while the nature of war is unchangeable, the methods of warfare as well as the methods of winning have undergone some transformation to certain extent.⁷ Modern armed forces must face up to new challenges, risks and threats, including asymmetric ones. Hybrid operations can be a combination of select forms of

¹ Dave Johnson, *Russia’s Approach to Conflict – Implications for NATO’s Deterrence and Defence* (Rome: NATO Defense College, 2015), 2.

² Mike Winnerstig, *Tools of Destabilization. Russian Soft Power and Non-Military Influence in the Baltic States* (Stockholm: FOI, 2014), accessed June 15, 2015, www.foi.se/en/Search/Abstract/?rNo=FOI-R--3990--SE.

³ Johnson, *Russia’s Approach to Conflict*, 2.

⁴ Frank Hoffman, *On Not-So-New Warfare: Political Warfare vs. Hybrid Threats* (4 August 2014), 2, accessed June 15, 2015, <http://www.isn.ethz.ch/Digital-Library/Articles/Detail/?id=182335>.

⁵ *Countering Hybrid Threats*, Food-for-thought paper, European External Action Service (EEAS), Council of the European Union, 8887/15 (Brussels, 13 May 2015), 2.

⁶ Sun Tzu, *Sztuka wojny* (Gliwice, 2004).

⁷ John Keegan, *A History of Warfare* (London, 1993), 11.

symmetric⁸ and asymmetric wars⁹ in which the sides involved conduct classical military operations and make firm attempts to take control of the local people in the combat area, while simultaneously ensuring security and stability.¹⁰

Frank Hoffman claims that the characteristics of hybrid wars are frequent terrorist acts and various forms of criminal activity.¹¹ He defines hybrid warfare as involving an adversary who simultaneously and adaptively uses an integrated combination of conventional weapon and irregular tactics, terrorism and criminal elements in the arena of war in order to reach political goals.¹² The definition above indicates two types of actors: state and non-state ones, applying a broad range of models of war, although it should be understood that many of these models are applied simultaneously. Hoffman accords significant importance to the role of organized crime in the hybrid warfare. The existence of a large number of objects makes coordinating these operations challenging. It is not clear whether the war model is attached to one object or whether all objects are associated with one model. Is a structural or an operational model more important? Certainly, simultaneity of action does indeed matter. In turn, it is not clear whether criminal actors are the participants or the source of financing. The definition completely loses its meaning in the case of operations that do not involve violations. It does not refer to the use of diplomatic, economic, or financial instruments, subversive operations, non-governmental organizations, information operations, the use of false portals and internet addresses (trolls) or newspapers and radio and television stations. Nathan Freier, John McCuen, and Helmut Habermayer propose similar definitions. The core of these definitions can be boiled down to the possibility of the simultaneous and effective deployment of various forms of warfare.¹³ NATO proposes a very general definition of hybrid threats, suggesting that these stand out by virtue of their multidimensional character. However, it says nothing about organized

⁸ Piotr Gawliczek and Jacek Pawłowski, *Zagrożenia asymetryczne* (Warsaw: AON, 2003), 11.

⁹ John Russell, "Asymmetric Warfare," in *The Big Issue: Command and Combat in the Information Age*, ed. David Potts (London: Strategic & Combat Studies Institute, 2002), 120–122.

¹⁰ John J. McCuen, "Hybrid Wars," *Military Review* 2 (2008), 108.

¹¹ Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars* (Virginia: Potomac Institute for Policy Studies Arlington, 2007), 5.

¹² Frank G. Hoffman, "Hybrid vs. compound war. The Janus choice: Defining today's multifaceted conflict," *Armed Forces Journal* (October 2009), accessed May 28, 2015, <http://www.armedforcesjournal.com/hybrid-vs-compound-war>.

¹³ Nathan P. Freier, *Strategic Competition and Resistance in the 21st Century: Irregular, Catastrophic, Traditional, and Hybrid Challenges in Context* (Carlisle, PA: United States Army War College, Strategic Studies Institute, 2007); McCuen, "Hybrid Wars," 107–113; Helmut Habermayer, "Hybrid Threats and a Possible Counter-Strategy," in *Hybrid and Cyber War as Consequences of the Asymmetry: A Comprehensive Approach Answering Hybrid Actors and Activities in Cyberspace*, ed. Josef Schröfl and Bahram M. Rajaei (New York: Peter Lang, 2011), 249–272.

crime. Hybrid threats are threats that involve the possibility of simultaneous and adaptive application of conventional and unconventional measures in order to reach the objectives intended.¹⁴ The concept of counteraction against hybrid threats made against NATO requires a complex approach promoting the coordinated deployment of all available Allied resources, i.e. diplomatic, economic, intelligence resources, etc.

New options of waging war and resolving crisis situations are given in the 2010 Military Doctrine of the Russian Federation and they tend to refer to the characteristics of present-day conflicts. The doctrine hints at the integrated use of military and non-military instruments alongside their resources. It highlights the cosmic and informative dimensions. It assumes that the information war allows political objectives to be reached without the use of armed force or that it can shape the conditions for the use of armed force.¹⁵ In the 2014 Russian doctrine on asymmetrical operational methods, it was revealed that the doctrine allows an adversary's advantage to be eliminated, in a conflict situation, by the participation of irregular subdivisions of the armed forces and private military companies.¹⁶ The use of political and social powers, providing management and finances from outside,¹⁷ was stressed as an important factor. The changes in view of Russian strategists in terms of conducting war are reflected in the articles and public speeches written and given by the Chief of General Staff of the Armed Forces of the Russian Federation, General Gerasimov. In February 2013, he wrote that, in the twenty-first century, it is possible to observe the blurring of borders between war and peace in terms of the classical understanding of these notions. From this perspective, one should recognize that various operations pursued by the Russian Federation in the diplomatic, economic, and military realms, as well as in terms of subversive operations and the organized crime which takes place in Baltic States, Black Sea, and Mediterranean region, should be interpreted as an element of a campaign that has been implemented for a long time and that is only broadly defined.¹⁸

Leszek Sykulski highlights that sabotage groups taking part in operations cannot possess any identification markers and that their members cannot be

¹⁴ Michael Miklauci, "NATO Countering the Hybrid Threat," 23 September 2011, accessed June 3, 2015, <http://www.act.nato.int/nato-countering-the-hybrid-threat>.

¹⁵ *The Military Doctrine of the Russian Federation* (approved by Russian Federation presidential edict on 5 February 2010), 7, accessed May 31, 2015, http://carnegieendowment.org/files/2010russia_militaryDoctrine.pdf.

¹⁶ Juliusz Sabak, "W Rosji Powstają Prywatne Armie," *Defence24*, 28 June 2014, accessed May 31, 2015, http://www.defence24.pl/news_w-rosji-powstaja-prywatne-armie.

¹⁷ *Military Doctrine of the Russian Federation*, December 30, 2014, accessed May 31, 2015, <https://www.offiziere.ch/wp-content/uploads-001/2015/08/Russia-s-2014-Military-Doctrine.pdf>.

¹⁸ "British Defense Minister Says Russia's Putin Poses 'Danger' to Baltic States," *The Moscow Times*, 19 February 2015, accessed June 16, 2015, <http://www.themoscowtimes.com/article.php?id=516203>.

treated as members of an armed force under international law. A situation of this nature enables the initiating state to distance itself, officially speaking, from these types of operations when events spin out of control.¹⁹ War is not declared, but merely starts with obscure, unpredictable events (no well-known schemas). On the basis of the color revolution as experienced in North Africa and the Near East, he argues that within a period of a few months or even days, a well-functioning state can be subject to immense upheaval, experience humanitarian catastrophe, or even fall into civil war as a result of armed conflict and foreign intervention.²⁰ The above-mentioned concept leads one to the conclusion that Russia is able to overthrow and destroy for example Baltic States without direct large-scale military intervention.

Gerasimov states that the significance of non-military measures is fluid and their effectiveness, in many cases, surpasses the use of regular weapons. Moscow does not have to bring its military units onto a state's territory in the event of what it dubs civil war. It can, however, use substitute methods. One of these may be armed combat, e.g. by the special forces, which can defend the interests of Russian citizens in the territory of one of the countries of Russian impact. It can also finance organizations that are involved in the conflict and act in the name of Russia. These actions can attempt to create a permanent threat and long-lasting weaknesses, through organized crime for instance, in countries of low economic potential. Consequently, Russia may also encourage minorities to take further steps in playing legally a larger role within the state, or even encourage and support separatists to create illegally an independent, separate state, such as those appearing in Ukraine. In this way, the Russian Federation could influence nations, discourage them from joining NATO and the European Union, and conversely, lay down conditions for integration into Russia and the Eurasian Union.²¹

Gerasimov pays a lot of attention to conducting special operations against internal opposition in order to create a continuously acting front across the entire hostile state, supported by information operations. Regular armed forces can be used under the cover of peace operations in a specific stage of conflict only, and only then for the achievement of an ultimate victory. Gerasimov sees the role and significance of political, diplomatic, economic and other impact factors, with the assistance of organized crime, including, for example, those of a secret nature, as well as the use of international non-state organizations, as

¹⁹ Leszek Sykulski, "Rosyjska koncepcja wojen buntowniczych Jewgienija Messnera," *Przegląd Geopolityczny* 11 (2015): 109, accessed May 28, 2015, http://przeglad.org/wp-content/uploads/2014/12/Przegląd_Geopolityczny_tom_11.pdf.

²⁰ Valery Gerasimov, "The Value of Science in Prediction," *Military-Industrial Kurier*, 27 February 2013, accessed May 31, 2015, <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/>.

²¹ Michael E. Lambert, "Hybrid War at Work in The Post-Soviet Space," *Estonian World*, 24 May 2015, accessed June 14, 2015, <http://estonianworld.com/security/hybrid-war-at-work-in-the-post-soviet-space/>.

the ways in which to reach political and military objectives.²² Gerasimov has dubbed future wars as new generation wars or *non-linear wars* in which the right of the other would be applicable. Military operations would start in peacetime with small units and with the application of aggression below the level of all-out war. New generation wars will involve non-contact clashes between accurately maneuvered hybrid units and precise strikes on the military and civil infrastructure aimed at defeating the armed forces of the adversary and weakening its economic power.²³

The actions of the Russian Federation present a great challenge for NATO because the Russian approach to the conflict undoubtedly includes measures of a political, diplomatic, economic, and non-linear nature, without the use of force, so that hybrid operations and organized crime are conducted below the level of a declared war. With regard to Russian involvement in Ukraine, one theory should be that plans assume the use of armed force and large groups of armies at the borders with Ukraine.²⁴ If so, from a Moscow standpoint, the fiasco of a non-military, non-linear hybrid campaign in the strategic interest would be followed by a sudden escalation of the conflict through the use of armed force and the option of shifting the conflict from a non-military to a military stage of the conflict. Conflict escalation by the large-scale use of armed force will prove that Moscow is ready for warfare with the West. For NATO it will constitute a great challenge because the more instable and volatile the security environment, the greater, according to Gerasimov's pronouncements, the reaction time between taking political-diplomatic measures and taking military measures.²⁵ Russia also has the capacity to coordinate military and non-military operations across a wide spectrum of potential crisis situations. It allows for a combination of the autocratic system of power and a specialized process of decision making and thus improves the civil-military command and control system. Large-scale exercises indicate that the Russian command and

²² Valery Gerasimov, *The role of the General Staff in the defence of the country in accordance with the new regulations on the General Staff approved by the President of the Russian Federation*, speech at the meeting of members of the Academy of Military Sciences on 26 January 2013, accessed May 31, 2015, <http://www.avnrf.ru/index.php/vse-novosti-sajta/620-rol-generalnogo-shtaba-v-organizatsii-oborony-strany-v-sootvetstvii-s-novym-polozheniem-o-generalnom-shtabe-utverzhdyonnyim-prezidentom-rossijskoj-federatsii>.

²³ Valery Gerasimov, *The Value of Science is in Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*, Originally published in *Military-Industrial Kurier*, February 27, 2013, accessed May 31, 2015, http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

²⁴ Heidi Reisinger and Aleksandr Golts, *Russia's Hybrid Warfare – Waging War below the Radar of Traditional Collective Defence* (Rome: NDC, 2014), accessed June 12, 2015, www.ndc.nato.int/news/current_news.php?icode=732.

²⁵ Gerasimov, *The role of the General Staff in the defence of the country in accordance with the new regulations on the General Staff*.

control system allows the country to reach the ability to simultaneously direct and control large military operations, and some small ones, within a short space of time.²⁶ Events in Ukraine also suggest that the Russian approach to armed conflict include preparation for intimidation by leveraging its nuclear capabilities and treating them as cover, as well as protecting subdued territory through non-military and military operations. In the light of the arguments cited above it is obvious that, according to the concepts put forward by the military leaders of the Russian Federation, it is to be expected that operations will occur with the use of non-military measures, i.e. diplomatic, political, economic, and informational ones, in connection with military measures, i.e. kinetic, non-kinetic, conventional militaries, special militaries, paramilitary forces, non-nuclear weapons (conventional precision-guided missiles) and nuclear weapons.²⁷

Coordinated and synchronized Russian operations involving the application of many different instruments create strategic ambiguity. Russia uses complex, multidimensional impact factors to deliberately send the wrong signals and mask its real intentions, confound adversaries, impede decision-making processes and make their response ineffective. Resorting to non-linear and asymmetric operations can escalate ambiguities, distort the chronology of operational order as known and may cause many difficulties in recognizing the pattern of aggression. Consequently, post factum (after a couple of years) one may discern that pressure was intentionally applied, e.g. that diplomatic pressure, pressure in terms of energy supply, the deployment of organized crime elements or encouragement of ethnic divisions were part of a long-standing campaign. Observation of the conflict in the Ukraine indicates that the presence of “green men” does not denote the beginning of a conflict in the slightest: rather, it is more of an indicator of the end of the first stage that is usually of a military nature. According to assessments of Gerasimov’s doctrine it denotes a violent escalation in which the dominating player can apply regular force.²⁸

Russian operations in Ukraine unambiguously indicate that the security environment in Europe has become unpredictable. The aim of Russian hybrid impact and organized crime is to pressurize and destabilize neighboring countries without needing to seize the territory. Combining and synchronizing camouflaged military operations lead to the surprise effect and hinder an adequate reaction, especially for international organizations operating on the premise that a consensus must be reached. Hybrid warfare is unpredictable because it is simple and cheap for the external aggressor, but has expensive and negative effects for the defending parties.²⁹ Blackmail in terms of the use of nuclear

²⁶ Johnson, *Russia’s Approach to Conflict*, 9.

²⁷ Ibid.

²⁸ Ibid., 12.

²⁹ Nicu Popescu, *Hybrid Tactics: Neither New Nor Only Russian* (European Union Institute for Security Studies, 2015), 2, accessed June 12, 2015, www.iss.europa.eu/uploads/media/Alert_4_hybrid_warfare.pdf.

weapons by the Russian Federation (annexation of the Crimea) as well as the application of militaries as a large-scale, conventional weapon, and creating frozen conflicts (eastern Ukraine) along with organized crime, present a substantial challenge to the security of the Euro-Atlantic area. Preventative operations are essential to nip large-scale crises in the bud. The division of roles between the target state, states on the western borders of the Union and other allies, as well as between NATO, EU and the UN, should be clearly marked out.³⁰

NATO in the Face of Hybrid Threats

Taking into consideration the arguments mentioned above, there can be no doubt of the importance of the issue of hybrid warfare and organized crime for the international community, regardless of whether the tactics applied are old or new. The momentum and scale of military operations conducted by the Russian Federation are deliberately restricted and maintained at an ambiguous level: namely, the level below regular, open war.³¹ The aim of subliminal aggression lies in achieving goals, with ambiguity creating difficulties in reaching a decisive consensus within international security organizations. NATO has many difficulties in a response because the level of aggression is kept mounting below that of the criteria for classical threats and the response must be coordinated, including non-military institutions. In the aspect of the military operation that was held in the Crimea and that was not an armed aggression but a new form of operational warfare it is possible to raise a question: are the current NATO legal provisions and available reaction instruments adequate to the requirements of the contemporary warfares called by Gerasimov the warfares of a new generation? Jānis Bērziņš questions the relevance of Article 5 in a situation lacking an armed attack. He wonders what NATO would do if Russia defended the rights of Russian-speaking minorities residing in Baltic States with other methods and referred to democratic law for self-determination as evidenced in Kosovo or in Crimea. How should one respond to a situation of this nature: politically or militarily? He subsequently argues that NATO armed forces would probably be inclined to fight, but that it is highly likely that this would be blocked by politicians.³² There is much concern as to whether armed forces possess the capabilities needed to withstand new forms of hybrid opera-

³⁰ Merle Maigre, "Nothing New in Hybrid Warfare: The Estonian Experience and Recommendations for NATO," Policy Brief (German Marshall Fund of the United States, 2015), 4, accessed June 12, 2015, <http://www.gmfus.org/publications/nothing-new-hybrid-warfare-estonian-experience-and-recommendations-nato>.

³¹ Stanisław Koziej, "Musimy się przygotować na wojnę hybrydową," *Newsweek Polska*, March 2, 2015, accessed May 28, 2015, <http://polska.newsweek.pl/koziej-musimy-sie-przygotowac-na-wojne-hybrydowa,artykuly,358198,1.html>.

³² Jānis Bērziņš, *Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy* (National Defence Academy of Latvia, 2014), 8, accessed June 4, 2015, <http://www.naa.mil.lv/~media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx>.

tions and organized crime and as to the application of non-kinetic forms of fighting: it would probably be difficult to reach a consensus on this matter.³³ Undoubtedly, breaches of the applicable provisions of international law and the existence of legal doubts as to the relevance of Article 5 on the part of NATO will have serious implications for the strategies of nations on the eastern flank. The more often that Baltic States are subject to the Russian campaign of strategic communication including information, psychological operations, operational misleading etc., the more these implications will increase. These states should not wait until NATO begins to act: rather, they should change their national security strategies to be able to respond to the hybrid threat in the best way, and seek to reduce their vulnerabilities. Such a defense would include a mix of preparedness, deterrence, and responsiveness. Indeed, the perception of threats is not universally the same, and neither is the assessment of threats. Despite the actions taken by member nations, NATO, as an organization, is obliged to draw up a concept detailing which bases should be involved within the strategy of withstanding hybrid threats and organized crime. In my opinion, the alliance should also adopt a new strategic concept that better reflects views of the security threat posed by Russia (NATO's current strategic concept was adopted in 2010). In the experts' of international law assessment remains a matter of recalling the decisions of Article 5, and if it will be necessary to make deeper changes in the Washington Treaty. In conclusion one can say that effectiveness of withstanding threats is dependent on quickly developing and implementing doctrinal documents, training people in them, and, first and foremost, changing the mentality of military leaders.

Of course, while it was not NATO that caused the crisis in Ukraine, nobody probably expected the Alliance to become militarily involved. Ukraine is not a NATO member and nobody at all would like direct confrontation with Russia. Secondly, the war was not explicitly declared, so officially Russia was not a party involved in the conflict. Without a doubt, and in connection with the issue of the distortion of the international security environment, everyone expected NATO to take the plunge and place the hybrid threats coming from Eastern Europe high on the agenda at the NATO summit in Wales. This did not happen, and Islamic State of Iraq and Levant (ISIL) turned out to be a priority. NATO is attempting to adapt to the new challenges posed by hybrid war and organized crime, but, nevertheless, one can certainly say that these actions are inadequate. There remains a lack of specific information in terms of the military response. The problem could be partly solved by the joint development and implementation of strategy with the EU, specifying which tasks NATO is responsible for. It is worth remembering that, for NATO, the most pressing threat is the one posed by ISIL. For NATO, the challenge is to determine an appropriate ratio of resources and tools dedicated to the threats coming from the East

³³ Nicholas Watt, "UK seeking to ensure Russia sanctions do not harm City of London," *The Guardian*, March 3, 2014, accessed June 12, 2015, www.theguardian.com/world/2014/mar/03/uk-seeks-russia-harm-city-london-document.

and the threats coming from the South. NATO has to assess the structure of the Very High Readiness Joint Task Force (VJTF) as it should be flexible and capable of adapting to a broad range of hybrid threats and organized crime. It should include specialist units. New capabilities will also be required, including the ability to combat organized crime, wage war in cyberspace, conduct psychological operations, to counteract propaganda, support local societies and more. The key will be building situational awareness in the regions in which the missions are taking place, and this can be provided by intelligence and military reconnaissance.

European Union in the Face of Hybrid Threats

Russian aggression as seen in the annexation of Crimea presents a serious challenge both for international organizations and international law. Russia deploys large-scale well-coordinated operations of a hybrid nature in a sophisticated manner, leading to destabilization and the breaching of the territorial integrity of Ukraine, which is still destabilizing the surrounding environment. The EU has not issued an outright response to the events. One of the culprits for this is the lack of a definition of hybrid warfare and an unambiguous understanding of the concept of its usage. Nevertheless, official EU documents do mention the characteristics of this new phenomenon and explain the context of its use. Similar to NATO, the EU points out the variety of the impact instruments applied. Hybrid warfare is described as centrally planned and directed, hidden and open, aggression using military and non-military measures that include: intelligence operations, organized crime, cyberspace operations, and economic pressure as well as the use of regular armed force. Using hybrid tactics, the attacking party tries to discredit and destabilize its adversary through repression and subversion. It also uses a variety of forms of sabotage, destabilizing the functionalities of communication devices and devices that transport energy. The aggressor can reach its goals by inspiring separatist groups or hiding aggression under the cover of humanitarian intervention. The element inherent to all hybrid campaigns is large-scale disinformation aimed at painting a false picture of a situation in the eyes of society. All the above-mentioned undertakings are not accidental. They are used as part of a unified strategy targeted at reaching political impact or even domination over the state.³⁴ The most important aspect of hybrid war in the assessment of the EU is generating ambiguity both within the society of the attacked state and within international society. The aim of information impact is the masking of what is currently happening in order to lose the ability to recognize the border between war and peace. Omnipresent ambiguities and a lack of explicit attributes on the part of the aggressor can paralyze the mobilization of an effective reaction and defense because it is not clear who, in fact, stands behind the attack. What is

³⁴ *Countering Hybrid Threats*, Food-for-thought paper, European External Action Service, 2.

more, ambiguities can divide the international community and, primarily, slow down and limit the scope of reaction to aggression.³⁵

The European Union states that hybrid threats and organized crime will undergo evolution along with the development of new technologies. It considers that action should also be taken to protect sensitive elements of the security system of a state. A psychological defense against hybrid warfare and organized crime lies in gathering complex reconnaissance of the effects that can result from hybrid warfare, and then building a system capable of withstanding the threats. It seems to be true that a hybrid strike is designed and oriented to attack the most vulnerable elements of a state. In the case of Ukraine, critically vulnerable areas included:³⁶ 1) Weak government, state institutions and corruption; 2) Weak security structures and state defense; 3) Marginalization of Russian-speaking populations; 4) Heavy dependency on the Russian gas and oil supplies.

The defense system of Ukraine, similar to that of other EU member states, was traditionally designed to defend against regular armed force perpetrating state borders. It transpired that it did not meet the requirements laid down by non-state actors conducting what could be termed *proxy war*. It proved the hypothesis that sensitive areas and areas crucial for the functioning of the state are: the economy, the energy and fuel sector, critical infrastructure, the financial system, the communication system, and transport. In this regard, the securing of energy provision by supplying new energy from outside and diverting its source will be particularly important for the EU. Recognizing one's own weaknesses constitutes the foundation upon which to build an effective security and defense system to protect against hybrid threats and organized crime.³⁷

In counteracting hybrid threats, one must consider the aggressor's conviction in the consequences of its actions and the price it will have to pay for them. A deterrent can be established in two ways: firstly, the consequences of sanctions can be expressed by subversive operations and as a result can cause large damage to the attacking party, with the outcome that an attack turns out to be economically unviable. Secondly, the level of critical infrastructure can be increased significantly and prepare society for the consequences of an unpredictable, negative event. There is a big area for improvement in searching the methods of cooperation between the EU and NATO, and in preparing a complex set of tools for countering hybrid threats. Integrating the actions of these organizations into common doctrine could become the fundamental pillar of deterrence in the future.

In conclusion, it should be stated that the complexity of hybrid threats and organized crime require a strategy based on which policy should be shaped and

³⁵ Ibid., 3.

³⁶ Ibid., 4.

³⁷ Ibid., 5.

guidelines for taking inherent actions within the EU should be drawn up. The conclusions drawn from the debate on hybrid threats must be reflected in a new EU security strategy. If the EU and NATO common strategy for countering hybrid threats fails to be developed, the EU strategy should be complementary with the NATO strategy. The common strategy of countering hybrid threats is a big chance for improving relations between the EU and NATO. It shall constitute the basis of the mutual support. With regard to counteracting hybrid threats, EU common security and defense policy should form the basis for the exchange of intelligence information, the development of new capabilities, including situational awareness, conducting training sessions and exercises. The priority for the EU is establishing a cell collating information on hybrid threats. It will play a key role in issuing warnings about threats and preparing a suitable response. Communication strategy will be significant in underlining the message directed at the Russian Federation as well as in preparing responses to any disinformation.

Conclusion

It seems unlikely that Russia's armed forces will cross the NATO border, nevertheless, it should be expected that Russia will try to destabilize both NATO and the EU with non-military operations. An effective response to hybrid operations and organized crime will require coordinated actions on the part of both organizations. In order to provide this, it is essential to possess common doctrine to counteract hybrid threats. NATO should play the role of leader in areas such as preparing a military response, intelligence and deterrence and in emergency intervention. It seems that, in a time of peace, the best deterrence is the permanent presence of NATO militaries on the territory of the nations most at threat. The EU should take responsibility for counteracting organized crime in cyberspace, energy and migration policy and propaganda. It is necessary to seek out synergies for the integrated deployment of the instruments at the disposal of both organizations.

A substantial challenge for both organizations and member states, especially those most at threat, will be the reduction in sensitivity and vulnerability to hybrid threats. Neither NATO nor the EU guarantee the absolute security of member states in the face of hybrid threats and organized crime, but these organizations will surely help in building resistance to them. Particular countries should develop and implement their own non-standard strategies for the national security which enable self-countering both the classic threats and hybrid ones, as well as modifying their own defensive structures. Absolutely crucial are the capabilities and provision of resources needed for their gathering. The capabilities of countering hybrid threats should provide the opportunity for deterrence operations, preparation for defense and effective response in case they occur.

About the author

Mirosław Banasik (b. 1960) currently works at the University of Lower Silesia in Wrocław (Poland). He holds a PhD in the humanities, is a certified Colonel in the Polish Armed Forces, and a graduate (Postgraduate Studies) of the National Defense University of Warsaw and the NATO Defense College in Rome (Italy). He has held a range of command and staff posts. Inter alia, he was the Deputy to the Polish National Military Representative to SHAPE (Supreme Headquarters Allied Powers Europe). His academic interests include issues related to national and international security and crisis management.