

# Hybrid Warfare: A New Phenomenon in Europe's Security Environment

Updated and extended 2<sup>nd</sup> edition





# **Hybrid Warfare: A New Phenomenon in Europe's Security Environment**

Research and presentation paper by Jagello 2000  
in cooperation with Faculty of Social Studies, Masaryk University, Brno  
and European Commission Representation in the Czech Republic

Updated and extended 2<sup>nd</sup> edition

Published by Jagello 2000 for NATO Information Centre in Prague.

Praha – Ostrava 2016

The original version of chapter I of this text was published in Czech in October 2015.

The English version of this text first appeared as part of „Road to Warsaw Security Forum 2015“ proceedings published by the Casimir Pulaski Foundation in Warsaw in 2015.

CATALOGUING-IN-PUBLICATION – NATIONAL LIBRARY  
OF THE CZECH REPUBLIC

Hybrid warfare: A new phenomenon in Europe's security environment. -- Updated and extended 2nd edition. -- Praha ; Ostrava : Jagello 2000 for NATO Information Centre in Prague, 2016. -- 29 stran

„Research and presentation paper by Jagello 2000 in cooperation with Faculty of Social Studies, Masaryk University, Brno and European Commission Representation in the Czech Republic“

ISBN 978-80-904850-5-1 (Jagello 2000)

355.01-022.324 \* 355.45 \* (4)

- NATO
- hybridní válka
- obrana státu -- Evropa -- 21. století
- studie
- hybrid warfare
- state defence -- Europe -- 21st century
- studies

355/359 - Vojenství. Obrana země. Ozbrojené síly [15]

355 - Military science [15]

© Jagello 2000, 2016

ISBN 978-80-904850-5-1

## Table of contents

Foreword to the 2 <sup>nd</sup> edition (2016) <i>Petr Zlatohlávek</i>	7
Introduction <i>Petr Zlatohlávek</i>	9
<b>I. Hybrid warfare: its concept, potential and how to fight it</b> <i>Zdeněk Kříž, Zinaida Bechná, Peter Števkov</i>	10
1. Hybrid warfare as a concept	10
1.1. Working definition of hybrid warfare	10
2. Use of elements of hybrid warfare against Georgia and Ukraine	11
2.1. Georgia 2008	11
2.2. Ukraine 2014–2015	12
3. Is this a new approach? The Czech academic debate on hybrid warfare	13
3.1. State of art on hybrid warfare in Czech academic cycles	14
4. Potential of hybrid warfare	15
5. Venues for future: proposed measures for improving the ability of states to face hybrid warfare	17
6. NATO's response to hybrid threats	18
Bibliography	20
<b>II. Increasing resilience of the Czech Republic to hybrid threats</b> <i>Miroslav Mareš</i>	24
1. Introduction	24
2. Historical experience	24
3. Current threats	25
4. International impact on Czech resilience	25
5. Hybrid threats and hybrid warfare as reflected in Czech strategic documents	26
6. Institutional changes	26
7. The main gaps	26
8. Final recommendations	27
Bibliography	28



## Foreword to the 2<sup>nd</sup> edition (2016)

Based on the success of last year's first edition of Jagello 2000's research and presentation project entitled *Hybrid Warfare: A New Phenomenon in Europe's Security Environment*, we decided to continue this effort also this year. Again in cooperation with the Faculty of Social Studies, Masaryk University, Brno, and European Commission Representation in the Czech Republic, the project resulted into the second, updated and extended edition of our policy paper.

Even more than a year ago there was no doubt that we will have more than enough reasons to develop this project into another year. The international security environment has not been growing any quieter and the spectrum of conflict activities that can be categorized under the hybrid warfare label is widening. And these activities can be observed not only in areas relatively far from the heart of Europe, such as East Asia, Middle East, Georgia or Ukraine (the latter two most frequently mentioned in current hybrid warfare research), but also in NATO member countries, including the Czech Republic. Hybrid threats have thus become one of the main focuses of the NATO Warsaw Summit in July 2016 and its final communique explicitly mentions hybrid threats more than a dozen times.<sup>1</sup>

Although the significance and importance of this topic clearly rises, there are still only a very few Czech sources covering the hybrid threats, which actually strengthened our determination to continue. Last year's first edition of the *Hybrid Warfare: A New Phenomenon in Europe's Security Environment* paper, produced by top Czech experts following research and workshops held at Masaryk University in Brno and NATO Days in Ostrava, is one of initial efforts in the Czech research on hybrid warfare. The publication assessed the concept, introduced definitions and highlighted the topic's relevance for the Czech Republic. Given the domestic and international demand for Czech inputs to the topic, we published the paper also in English, with the English version originally appearing in the proceedings of the Polish prestigious international conference *Warsaw Security Forum 2015*.<sup>2</sup>

The goal of this year's, second edition of the project has been both to assess the dynamic developments in this area over the last year, and mainly to broaden our research to include increasing resilience of the Czech Republic against hybrid threats. That is why we extended the working team to include Czech experts in this specific field (prof. Miroslav Mareš) and also invited international experts to reflect

---

1 Warsaw Summit communique. 9 July 2016.

Available at: [http://www.nato.int/cps/en/natohq/official\\_texts\\_133169.htm](http://www.nato.int/cps/en/natohq/official_texts_133169.htm)

2 *Road to Warsaw Security Forum 2015*. Warsaw: Casimir Pulaski Foundation, 2015

on the development of hybrid warfare in the international arena and its implications for the Czech Republic. After months of preparations the group met at this year's workshop on September 16, 2016, held as part of the expert associated programs of the NATO Days in Ostrava.

The original paper *Hybrid Warfare: A New Phenomenon in Europe's Security Environment* has been amended to include this year's workshop recommendations and is hereby published in its second, updated and extended edition. The new text now includes among other updates the results of the July 2016 NATO summit in Warsaw and a review of the Czech academic research of the hybrid warfare topic. Most importantly, the paper now features a whole new chapter on increasing resilience of the Czech Republic against hybrid threats.

*Petr Zlatohlávek*

*Jagello 2000*



## Introduction

At least since 2014, Europe has been facing a new kind of hybrid security threats which combines a number of different types of warfare - ranging from conventional, irregular or special military units, all the way to informational, economic and cyber means, including acts of terrorism and criminal activity. These threats are no less relevant for the Czech Republic.

Developing an effective response to these threats means not only to present long-term solutions, but it will also require a comprehensive approach of all security forces, next to military and intelligence also police and customs services. In the Czech Republic we still lack a clear definition of hybrid threats as well as a professional discussion of relevant actors dealing with the readiness of security forces (of the Czech Republic) and their ability to adequately respond to these threats. Therefore Jagello 2000 Association, jointly with the Faculty of Social Studies of Masaryk University (FSS MU) in Brno and in cooperation with the European Commission Representation in the Czech Republic, implemented a research and presentation project from May to September 2015, resulting in the current paper on the topic of hybrid warfare.

The first part of the project was a special seminar held in July 2015 at the FSS MU in Brno, involving leading Czech experts on these issues. This seminar resulted in a draft version of the paper with definitions of hybrid threats and best practices for dealing with them.

The second phase of the project was a workshop for representatives of the security forces of the Czech Republic that focused on the practical readiness. The draft version of the paper was introduced to the professional public - the auditorium included representatives of the Ministry of Defense, Ministry of Foreign Affairs, Ministry of Interior, Police, National Security Agency, Customs Administration and academia. The event took place on Friday, September 18, 2015 as part of expert programs associated with the NATO Days in Ostrava. NATO Days in Ostrava are regarded the biggest security show in Europe and is organized by the Jagello 2000 Association in cooperation with all components of the integrated rescue system.

The result of these discussions is presented in the following paper which takes into account inputs and suggestions from the entire course of the project. The authors of the text are Zdeněk Kříž, Zinaida Shevchuk and Peter Števkov from Masaryk University, Brno, Czech Republic.

*Petr Zlatohlávek*

*Jagello 2000*

# **I. Hybrid warfare: its concept, potential and how to fight it**

*Zdeněk Kříž, Zinaida Bechná, Peter Števkov*

## **1. Hybrid warfare as a concept**

The war in Clausewitz's concept is seen as a continuation of the policy of the state by violent means, which are used to force the opponent to execute our will. The primary role in this concept is played by the use of armed violence in its symmetrical or asymmetrical form. To this end all the resources of society are used as later elaborated in the concept of total war. Although hybrid warfare serves the same purpose, namely the achievement of political goals, which can be very diverse, it differs from war in Clausewitz's concept (further referred to as 'classic war') in many different characteristics.

Expert debate about hybrid warfare began in foreign literature long before the Russian invasion of Ukraine. In our opinion, this debate's weakness consists in the fact that the available definitions do not set explicit demarcation criteria for distinguishing between classical and hybrid warfare. If we want to differentiate between hybrid warfare and classic war, the main demarcation criterion, in our judgment is the use of the means that are primarily used to achieve the objectives of war. In hybrid warfare, it is important that non-military means of subversive nature play the leading role. Ideally, an attacking state need not make explicit use of military force. The aim of the attacker is to control the minds of the political leadership and the population of the attacked state through propaganda (psychological operations), deceptive campaigns and intimidation by terror. If military force is used, it is used in secret. Use of demarcation criteria, prioritizing non-military tools of subversion and conducting secret warfare, these aspects clearly distinguish hybrid warfare from other types of war.

### **1.1. Working definition of hybrid warfare**

Hybrid warfare is an armed conflict conducted by a combination of non-military and military means and aiming with their synergistic effect to compel the enemy to take such steps that he would not do of his own accord. At least one side of the conflict is the state. The main role in achieving the objectives of war is played by non-military means such as psychological operations and propaganda, economic sanctions, embargoes, criminal activities, terrorist activities, and other

subversive activities of a similar nature. The attacker's military operations are conducted in secret by irregular forces combining symmetric and asymmetric methods of combat operations against the whole society and, in particular, against its political structures, state authorities and local government, the state economy, the morale of the population and against the armed forces.

## 2. Use of elements of hybrid warfare against Georgia and Ukraine

### 2.1. Georgia 2008

The Russia-Georgia armed conflict in the summer of 2008 broke out at the time of the Beijing Olympics and aroused deep concern in the international community. According to some experts, it was the first armed confrontation between the East and the West after the end of the Cold War. The main aim of Russia was to retain its influence through military operations, to recognize the independence of the regions concerned, and to maintain a significant military presence in those territories. Last but not least, Russia 'buried' the chances of Georgia to achieve NATO membership in the near future, which Georgia has sought since 2002. **In this case, it was not a hybrid warfare within the meaning of the above-proposed definition. It was a war according to the classical definition, in which Russia openly intervened with military force and used some elements of hybrid warfare to prepare and support the conduct of combat operations.** The policy goals of the operation were primarily achieved by military force whereas elements of hybrid warfare (economic sanctions and embargoes, information war, war in cyberspace) played more of a supporting role.

Both sides of the armed conflict waged an intensive information war, making it difficult to separate facts from intentionally disseminated disinformation. This information war was dominated by three main themes:

1. Georgia and especially President Saakashvili were aggressors.
2. Russia was forced to intervene to defend its citizens and to prevent a humanitarian catastrophe (defensive purpose);
3. The West has no legitimate reason for criticizing Russia because Russia simply does what the West did in Kosovo in 1999.

Parallel to the information war against Georgia, cyber war also took place. A total of 38 Georgian websites were attacked, including the website of the Georgian

president, Ministry of Foreign Affairs, National Bank, Parliament, and Supreme Court. These attacks were centrally managed and coordinated.

It is difficult to evaluate the performance of the Russian armed forces, as it is still not entirely clear whether it was a pre-planned and carefully prepared military operation, or whether it was on both sides an unexpected war, for which neither of the conflicting parties were prepared. However, the rapidity of the deployment of Russian military forces in the mountainous terrain, the early opening of a second front in Abkhazia, Russian espionage activities in the region, military provocations on the eve of war, the downing of a Georgian unmanned aircraft and, last but not least, the Russian military exercises in the region ('Caucasus 2008') demonstrate the readiness of Russia to escalate the conflict. The conflict nevertheless revealed many Russian shortcomings, particularly weaknesses in the coordination of ground, naval and air forces. According to available sources, an important role in military operations was played by airborne units and special forces. The reforms announced by the Russian president immediately after the war reflect the intention to improve Russia's ability to effectively lead the campaign by employing modern technologies and operating procedures.

## **2.2. Ukraine 2014–2015**

Russia used and is still using against Ukraine a wide range of military (asymmetric and symmetric), economic, propagandistic, diplomatic and perhaps even cyber means of combat.

The activity of Russian diplomacy, of course, cannot be summed in a text of this scope and purpose, but in brief, we can say that Russia is seeking to weaken Kiev at forums of international organizations, in particular by promoting the federalization of Ukraine. Concerning the economic means, Moscow manipulates the price of imported Russian natural gas and adopts restrictive non-tariff measures on Ukrainian food products. For the Ukrainian economy, the most severe sanction is a ban on the use of Russian air space by Ukrainian airlines.

Russia uses the so-called 'new propaganda' that does not seek to persuade the recipient, but to obfuscate what is truth and what the recipient can trust. To enlist support for the war in the Russian population it uses a broad variety of media channels, particularly state television, which in its coverage of Ukraine can significantly influence the local public opinion. These include Russia Today, Voice of Russia, Sputnik, press agency ITAR-TASS and the agency RIA Novosti. It is also worth mentioning that multiple sources have confirmed the existence of an army

of trolls paid by the government. These are Internet bloggers and debaters who post views preferred by the Russian government to domestic and foreign websites.

Concerning the cyberspace area, several attacks against the Ukrainian government websites and systems have been recorded (e.g. the Ukrainian electoral counting electronic system, the Ukrainian transport network, and attacks on websites of volunteer battalions). However, it is not possible to determine with certainty whether it has been the work of the Russian forces. It is also necessary to emphasize that all cyber-attacks are only the tip of the iceberg. The extent of Russian cyber-attacks using malware or spyware can never be determined with certainty unless Russia discloses this information voluntarily (or if it is leaked).

In the military dimension, Russia and the separatists are able to deploy a wide spectrum of units in the conflict. According to the US Department of Defense, in November 2014 Russia had 7,000 regular troops in Ukraine (excluding the Crimea). To this day, it is alleged that more than 40,000 Russian troops have been rotated in Ukraine. Russia and Russian organizations actively support the separatists (with logistics, material and personnel), who are a combination of the local population, Russian citizens and, occasionally, citizens of many other countries. Without extensive logistical support from the outside, it is impossible for the separatists to conduct combat operations to the extent that we see in eastern Ukraine. Russia is the only country in the region that has the capacity and motivation.

**If we apply the working definition in the introduction, then we can speak of hybrid warfare in particular to describe the Russian occupation of the Crimea and Russian operations until the summer of 2014.** Evaluation of the conflict since the summer of 2014 is not so clear-cut. Since summer 2014, it is quite obvious that regular Russian troops operate in eastern Ukraine and if necessary (e.g. imminent defeat of the separatists) even entire organic military units can be used. Denying this direct participation of the Russian military belongs to the hybrid warfare tools. **On the other hand, the direct military intervention of Russia suggests that hybrid warfare has reached its limits.**

### **3. Is this a new approach? The Czech academic debate on hybrid warfare**

The bedrock of the hybrid warfare concept is that of subversion, which comprises four main stages:

1. demoralization of the target society,
2. destabilization of the target society,

3. precipitation of a crisis in the target society,
4. seizing control of the target society by internal forces acting in concert with the attacker.

This is an old Soviet (Marxist-Leninist) concept, applied towards the West by the USSR throughout its existence. Attacks on the adversary's political authorities, propaganda, fomenting unrest, creating 'people's republics', these are well-known components under the cloak of the new hybrid warfare. Modern information technologies allow multiplication of the effect that brings a new quality and dangerous nature of this phenomenon.

### **3.1. State of art on hybrid warfare in Czech academic cycles**

In the Czech Republic there has been almost no academic debate on hybrid warfare. The first comprehensive attempt to evaluate the current approaches stemming from the international debates on this matter was the article *Critical Looks at Hybrid Wars Concept* by Pavel Zůna in the Czech Military Review in 2010.

In addition to a general overview of Western debates, Zůna's article contains a number of critical complaints. Firstly, Zůna disputes the assessment of the second Israeli war against Hezbollah as presented by American scholar Frank G. Hoffman, whom Zůna cites as the main proponent of the term "hybrid warfare". According to the author, Hezbollah's preparation to the conflict does not vary significantly from historically known practices. He also disputes labeling the Hezbollah as a hybrid enemy. Secondly, Zůna criticizes that Hoffman ignores that the main focus in hybrid wars is not terrain or occupied territories, but the population living on that territories. Finally, based on several historical cases, including the Slovak National Uprising in 1944, Zůna demonstrates that conducting combat operations combining regular and irregular forces does not bring a new concept. As a whole, Zůna points out that the concept of hybrid wars and hybrid threats in particular is based on some not completely clear premises.

Another Czech publication on hybrid warfare appeared in the context of the crisis in Ukraine. Petr Zelenka's paper *Is the conflict in Ukraine a "hybrid war"?* was published in November 2014. Zelenka offers an assessment of the Ukrainian crises and criticizes the absence of a generally accepted definition on hybrid warfare. The author devotes most of his attention to the analyses of Russian actions in Ukraine and less so to the critical assessment of a hybrid war concept. Zelenka sees hybrid war as a middle ground between conventional and guerrilla war. Regarding the uniqueness of the

phenomenon of hybrid wars Petr Zelenka concluded, again, that it is not a new concept.

Similarly, Richard Stojar's article *Conflict in Ukraine and Russia's involvement: A New Hybrid War, or the Application of Classical Methods?* published in the Czech Military Review in 2015, deals with conceptualization of hybrid war only indirectly. Main attention is paid to the analyses of the ongoing Ukrainian Crisis.

Finally, there are academic publications dealing with certain aspects of hybrid warfare. Among them is the article of Miroslav Mares *From Subcultural Groupings's Actors of Hybrid Warfare: Current Trends in Conflicts in Eastern Europe* from 2016, which is studying the issue of formation and operation of sub-cultural actors who can transform into military actors and can be used as a tool of hybrid warfare. Another Czech article, *Neither Conventional War, nor a Cyber War, but a Long-Lasting and Silent Hybrid War* by Nikola Schmidt from 2014, focuses on the analysis of the "cyber" component of hybrid warfare. The importance of information operations and "mental resilience" as a part of national strategy is explained in details. Schmidt argues that the classical distinction between combatants and non-combatants is too simplistic and instead he calls our attention to information operations as a part of a complex nature of hybrid warfare.

Thus, the coverage of hybrid war and hybrid threats in the Czech academic discourse is relatively modest, very much focused on current events in Ukraine and last but not least, the whole concept of a hybrid war is viewed very critically.

#### **4. Potential of hybrid warfare**

**Hybrid warfare in the media space is considered extremely dangerous.**

The proponents of this view usually refer to the Russian general Gerasimov, who claims that hybrid war can disrupt even a well-governed and prosperous state. This optimism (or pessimism, depending on one's perspective) is difficult to sustain in the light of the current empirical evidence. In a security analysis of this phenomenon, it is important neither to underestimate nor to overestimate its possibilities.

The main problem for the defender is to identify the moment when he is the target of a hybrid attack. **Therefore, defence against hybrid warfare depends in the first line on intelligence services and in the second line on an authentic civil society.** To wage a hybrid war aiming to achieve political goals, a number of specific necessary – however not sufficient – conditions must be met. Only their right configuration generates a suitable battlefield for hybrid warfare.

Empirical evidence to date indicates that these are at least the following necessary but not sufficient conditions in isolation:

1. the attacked country has been mismanaged in the long term and it does not fulfil its basic functions,
2. its population is divided along several dividing lines,
3. the potential attacker holds a certain attraction for a part of the attacked-country population and can therefore use soft-power instruments,
4. the attacked country borders the attacker and is unable to effectively control its borders,
5. the attacked country has no dependable allies, and
6. the attacker has a certain degree of credibility in the international community, which allows him to influence the international community with his version of events.

**Even in the case of Ukraine, which is in the post-communist milieu the prototype of a poorly governed state, managed like a company that lays golden eggs for oligarchs, the hybrid warfare succeeded only in the first stage in the Crimea.** However, **by the second stage**, when Russia, encouraged by its success in the Crimea, tried to split Ukraine along the Odessa–Kharkov line, **this concept fatally failed** and the defeat of Russian irregular forces fighting in secret until then in the east of Ukraine had to be prevented by an open intervention of Russian regular forces in the summer 2014. This intervention continues till today, producing negative political, economic and military consequences Russia.

If we think about further potential of hybrid warfare used against the West and the countries close to it, we must take into account that **Russia has lost the element of surprise**. Potential targets of this type of warfare, which in our region means primarily the Baltic States and indirectly NATO, would now be less shocked than in 2014. This is relevant also to the other countries of the West. Whether this conclusion applies to Belarus and the Central Asian countries is a question, however. Some steps taken by Belarus indicate that Lukashenko is aware of these risks.

Hybrid warfare has to be carefully analysed and preparations have to be made for waging it. The Central European countries should devote particular attention to Russia. **A fight against an opponent that wages a hybrid war is the task for the entire society and must be conducted in all areas.** Last but not least, the society must be prepared to make hybrid counterattacks in the area of information war and in cyberspace against the attacker. However, in our opinion, a **much more dangerous form of Russian aggression against members of NATO would be**



**a repeat of the Georgian scenario, especially if it is supported by nuclear threats from Russia.**

## **5. Venues for future: proposed measures for improving the ability of states to face hybrid warfare**

- Strengthen the state's ability to fulfil its basic functions and hence the loyalty of citizens to the state. Public communication, involvement of local authorities (mayors) as an element of dissemination beyond state level, along with creation of school programs and civil education would significantly contribute to this goal.
- Carry out intelligence and analytical activities in order to detect enemy preparations for a hybrid warfare, and, particularly, the launch of hybrid attacks using subversion. It is critically important to identify early indicators of the threat and where it comes from, especially in the very beginning of the conflict cycle.
- Continually single out countries that might resort to hybrid warfare and focus attention on them already in peacetime. Continuously draw up plans of countermeasures of both defensive and offensive nature against these countries in all areas relevant to hybrid warfare.
- Systematically prevent the infiltration of political leadership of the state carried out by agents of influence of a potential hybrid attacker.
- Acquaint the public in a suitable form with influence networks which a potential hybrid attacker constructs in the attacked-to-be country as well as with their modus operandi.
- Strengthen social cohesion of the country. By the active state policy do not allow the creation of variously defined socially excluded areas (e.g. based on ethnicity, religion or social status), which a potential attacker could rely on and which he could exploit in his campaign.
- Develop and build political relations with other potential targets of hybrid aggression. Exchange experience both on appropriate multilateral platforms (NATO and EU) as well as bilaterally. In this respect, more NATO-EU synergy, strategic communication and civil emergency planning is needed.
- In the area of foreign policy, strive to address the threats associated with hybrid warfare in international organizations for collective defence of which the state is a member.

- Reduce to a minimum the necessary level of diplomatic, economic, military and cultural relations with countries that have been evaluated as potential hybrid attackers.
- Develop an adequate form of homeland defence consciousness and educational activities among the population concerning hybrid warfare and ways to face it. Systematically develop cooperation in this area with an authentic civil society.
- Enhance flexibility and the ability of independent action at all levels of state, local government and the armed forces.
- Develop a wide range of capabilities needed for hybrid warfare, particularly intelligence capabilities, including the abilities to operate in cyberspace and to use information operations.
- Build military capabilities to be usable at all types of expeditionary operations and in defending territory, including training programs and defence education initiatives.
- Strengthen the ability of the police to act against irregular and hostile unidentified armed formations fighting incognito at the very moment they attempt to paralyze the authority of state and local government.
- Create legislative conditions to ensure that police forces could be rapidly reinforced on the national territory by the military in their fight against unidentified armed formations at a time when the state has not formally been declared a war.
- Pursue scientific study of the issue of hybrid warfare using the approaches of all relevant scientific disciplines.

## **6. NATO's response to hybrid threats**

Although the concept of hybrid war is not new, it is manifested in novel ways. Thus, it offers a perspective on the complex nature of NATO's security challenges. The above mentioned case studies point out the importance of this concept. The aim of hybrid war is to keep violence "below the radar of traditional collective defense." Countering such threats requires adaptation of NATO's strategy, structure and capabilities in order to timely identify, mitigate and recover from hybrid attacks with minor consequences on the social, political and military cohesion of the Alliance. There is a need of a coherent and comprehensive NATO strategy to counter hybrid threats involving a variety of non-traditional security challenges, including terrorism, migration, proliferation of weapons of mass destruction,

vulnerabilities in energy and raw material supplies, non-state actors and rouge states. This is especially important now, as the diversity, complexity and ambiguity of hybrid threats indicates a significant trend: the paradigm shift from the traditional deterrence toward prevention and resilience.

It is thus not surprising that resilience was one the fundamental topics for the last NATO Summit in Warsaw in 2016. Consequently, resilience has become a core element of collective defense encompassing seven major goals to assure: steadiness of government, security of energy supplies, food and water resources, communication and transportation system and ability to deal effectively with uncontrolled movement of people and mass casualties. NATO's strategy is based on mapping potential vulnerabilities, creation of early warning indicators, improving intelligence and strategic communication along with speeding up decision-making process. As emphasized in the *BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats*, the Alliance must base its strategy on a Comprehensive Approach to countering hybrid threats. An effective counter-hybrid warfare strategy requires political solidarity and agility along with well-tailored military capabilities. Such a comprehensive approach demands more synergy of national instruments of power among NATO member states. Therefore, each member state should augment the skills, practices, and capabilities needed to confront emerging hybrid threats.

*About the authors:*

*Dr. Zdeněk Kříž is Associate Professor, Dr. Zinaida Bechná is Assistant Professor, and Mr. Peter Števkov is PhD Candidate, all at the Department of International Relations and European Studies, Faculty of Social Studies, Masaryk University in Brno.*

## Bibliography

- Aaronson, Michael – Diessen, Sverre – Kermabon, Yves de – Long, Mary Beth – Miklaucic, Michael (2012): NATO countering the hybrid threat. *Prism*, Vol. 4, No. 2, pp 111-124. Available at: [http://cco.ndu.edu/Portals/96/Documents/prism/prism\\_2-4/Prism\\_111-124\\_Aaronson-Diessen.pdf](http://cco.ndu.edu/Portals/96/Documents/prism/prism_2-4/Prism_111-124_Aaronson-Diessen.pdf)
- Asmus, Ronald D. (2010): *A little war that shook the world: Georgia, Russia, and the future of the West*. New York: Palgrave MacMillan. ISBN 978-0-230-61773-5
- BBC (2014): Russia hits West with food import ban in sanctions row. *BBC News*, 7 August 2014. Available at: <http://www.bbc.com/news/world-europe-28687172>
- Chicky, Jon E. (2009): *The Russian-Georgian war: political and military implications for U.S. policy*. Policy paper, February. Washington, D.C.: Central Asia-Caucasus Institute. ISBN 978-91-85937-51-6. Available at: [https://www.files.ethz.ch/isn/99825/jc09russiageorgia\\_\\_2\\_.pdf](https://www.files.ethz.ch/isn/99825/jc09russiageorgia__2_.pdf)
- Bērziņš, Jānis (2014): *Russia's new generation warfare in Ukraine: implications for Latvian defense policy*. Policy Paper, No. 2, April. Riga: National Defense Academy of Latvia – Center for Security and Strategic Research. Available at: <http://www.naa.mil.lv/-/media/NAA/AZPC/Publikacijas/PP%2002-2014.ashx>
- Gerasimov, Valery (2013): Tsennost' nauki v predvideniye. *Voyenno-promyshlennyi kur'er*, No. 8 (476), 27 February 2013. Available at: <http://www.vpk-news.ru/articles/14632>. English translation available at: [http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview\\_20160228\\_art008.pdf](http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf)
- Glenn, Russel W. (2009): Thoughts on „hybrid“ conflict. *Small Wars Journal*, 2 March 2009. [online] Available at: <http://smallwarsjournal.com/mag/docs-temp/188-glenn.pdf> [Accessed 15 November 2016].
- Hoffman, Frank G. (2007): *Conflict in the 21<sup>st</sup> century: the rise of hybrid wars*. Arlington, Va: Potomac Institute for Policy Studies. Available at: [http://www.potomacinstitute.org/images/stories/publications/potomac\\_hybridwar\\_0108.pdf](http://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf)
- International Herald Tribune (2008): Russia says 64 soldiers dead in fight with Georgia. *International Herald Tribune*, 20 August 2008
- Kubeša, Milan – Spišák, Ján (2011): Hybridní hrozby a vývoj nové operační koncepce NATO [Hybrid threats and the development of NATO's new operational concept]. *Obrana a strategie*, Vol. 11, No. 2, pp 5-16. Available

at: <http://www.obranastrategie.cz/cs/aktualni-cislo-2-2011/clanky/hybridni-hrozby-a-vyvoj-nove-operacni-koncepce-nato.html>

Lindley-French, Julian (2015): *NATO and new ways of warfare: defeating hybrid threats*. NDC Conference Report, No 03/15 – May. [online] Available at: <http://www.ndc.nato.int/news/news.php?icode=814> [Accessed 15 November 2016].

McCuen, John J. (2008): Hybrid wars. *Military Review*, March-April, pp 107-113. Available at: <http://www.au.af.mil/au/awc/awcgate/milreview/mccuen08marapr.pdf>

Mareš, Miroslav (2016): From subcultural groupings to actors of hybrid warfare: current trends in conflicts in Eastern Europe. *Vojenské rozhledy – Czech Military Review*, 25 (mimořádné číslo), pp 123-133. Available at: [www.vojenskerozhledy.cz](http://www.vojenskerozhledy.cz)

NATO (2010): BI-SC input to a new NATO capstone concept for the military contribution to countering hybrid threats. [online] Available at: <http://www.act.nato.int/the-countering-hybrid-threats-concept-development-experiment> [Accessed 15 November 2016].

NATO Review (2016): Resilience: a core element of collective defence (2016). NATO Review. 2016. [online] Available at: <http://www.nato.int/docu/Review/2016/Also-in-2016/nato-defence-cyber-resilience/EN/index.htm> [Accessed 15 November 2016].

NATO Secretary General (2015): One of our greatest strengths is our ability to adapt. [Remarks at the ACT Transformation Seminar, Washington DC, 25 March, 2015]. Available at: [http://www.nato.int/cps/en/natohq/news\\_118430.htm](http://www.nato.int/cps/en/natohq/news_118430.htm)

Nemeth, William J. (2002): *Future war and Chechnya: a case for hybrid warfare*. Thesis. Monterey, Ca: Naval Postgraduate School. Available at: <http://hdl.handle.net/10945/5865>

Poroskov, Nikolai (2006): Gonka perevooruzhenia. *Vremya novostei*, No. 75, 28 April 2006. Available at: <http://www.vremya.ru/2006/75/4/150848.html>

Putin, Vladimir (2015): Vystuplenie na ceremonii otkrytija mezhdunarodnogo voenno-tehnicheskogo foruma “Armija-2015” [Army-2015 International Military-technical Forum opening speech], 16 June 2015. Available at: <http://kremlin.ru/events/president/transcripts/49712>

- Rácz, András (2015). *Russia's hybrid war in Ukraine: breaking the enemy's ability to resist*. FIIA Report 43. ISBN 978-951-769-453-7 (web), ISBN 978-951-769-454-4 (print). Available at: <http://www.fiaa.fi/assets/publications/FIIAReport43.pdf>
- Russia Today (2014): 'United continent': European volunteers fighting Kiev troops in Eastern Ukraine. *Russia Today*, 6 September 2014. Available at: <https://www.rt.com/news/183864-ukraine-european-volunteers-fighting/>
- Rühle, Michael (2011): NATO and emerging security challenges: beyond the deterrence paradigm. *American Foreign Policy Interests*, 33, pp 278-282. Available at: <http://www.aicgs.org/site/wp-content/uploads/2012/01/Ruehle-NATO-and-Emerging-Security-Challenges.pdf>
- Putin. Vojna: po materialam Borisa Nemtsova* [Boris Nemtsov's Report on Putin's War in Ukraine] (2014). [online] Available at: <http://www.putin-itogi.ru/putin-voyna/>, available in English at: <http://www.libertas-institut.com/wp-content/uploads/2015/05/EUFAJ-Special-NemtsovReport-150521.pdf>
- Schmidt, Nikola (2014): Neither conventional war, nor a cyber war, but a long-lasting and silent hybrid war. *Obrana a Strategie*, Vol. 14, No. 2, pp 73-86. Available at: <http://www.obranaastrategie.cz/cs/archiv/rocnik-2014/2-2014/clanky/neither-conventional-war-nor-a-cyber-war-but-a-long-lasting-and-silent-hybrid-war.html>
- Sputniknews (2014): Kiev turns to WTO over Russia's restrictions on Ukrainian agriculture imports: ministry. *Sputniknews*, 23 October 2014. Available at: <https://sputniknews.com/business/20141023194491920-Kiev-Turns-to-WTO-Over-Russias-Restrictions-on-Ukrainian/>
- Ștefănescu, Daniel (2015): NATO Strategy to defeat enemy forces in the hybrid war. *Scientific Research & Education in the Air Force*, Vol. 1, pp 113-117.
- Stojar, Richard (2015): Konflikt na Ukrajině a ruský zásah: nový způsob vedení hybridní války, nebo aplikace klasických postupů? [Conflict in Ukraine and Russian action: new way to fight a war or an application of traditional means?]. *Vojenské rozhledy*, Vol. 24 (56), No. 1, pp 26-37. Available at: <http://www.vojenskerozhledy.cz/kategorie/konflikt-na-ukrajine-a-rusky-zasah-novy-zpusob-vedeni-hybridni-valky-nebo-aplikace-klasickyh-postupu>
- Williamson, Murray – Mansoor, Peter R. (eds.) (2012): *Hybrid warfare: fighting complex opponents from the ancient world to the present*. New York: Cambridge University Press.

Zelenka, Petr (2014): Je konflikt na Ukrajině „hybridní válkou“? [Is the conflict in Ukraine a “hybrid war”?]. *Mezinárodní politika*, 6. 11. 2014. [online] Available at: <http://www.iir.cz/en/article/je-konflikt-na-ukrajine-hybridni-valkou> [Accessed 15 November 2016].

Zůna, Pavel (2010): Kritický pohled na koncept hybridních válek [A critical look at the concept of a hybrid war]. *Vojenské rozhledy*, Vol. 19 (51), No. 3, pp 33-45. Available at: <http://www.vojenskerozhledy.cz/kategorie/kriticky-pohled-na-koncept-hybridnich-valek>

## II. Increasing resilience of the Czech Republic to hybrid threats

*Miroslav Mareš*

### 1. Introduction

The Czech Republic currently faces a multitude of hybrid threats and although their influence on security and defence is slightly weaker in 2016 than in two previous years, they come in more sophisticated and increasingly latent forms.

The state's security system has begun to adapt to the new dimensions of threats posed by this rising security challenge. Units within the ministry of interior and ministry of defence are intensively dealing with the topic and outcomes are already available at the government's *National Security Audit of the Czech Republic*. International cooperation in the fight against hybrid warfare is also developing and is likely to dynamically grow in the future.

The aim of this paper is to describe and categorize the most important ways in which the country can develop resilience against current and future hybrid threats, as well as to identify gaps and formulate several policy recommendations in the area. It is important to start with an analysis of the historical legacy and the international impact on the Czech situation.

### 2. Historical experience

Hybrid warfare and other hybrid threats are not novel phenomena—what is subsumed under these terms depends upon definition and conceptualization. Without question, though, the current interconnection of propagandist, subversive, insurgent, paramilitary, espionage, energy manipulation, and similar activities, both within the traditional dimensions of security and in cyberspace, constitutes a new form of hybrid warfare and one which poses a huge challenge to Central European security systems.

Czechoslovakia, as predecessor to the Czech Republic, had direct experience of hybrid warfare at the end of the 1930s, when Nazi Germany began a 'hybrid war' with the help of various Nazi Sudeten German militant organizations and a massive anti-Czechoslovak propaganda campaign. The culmination was the Munich Treaty of September 1938. In 1939 - the combination of pro-German and anti-Polish attitudes was used during the manipulation of the part of the so called Silesian Resistance.



### 3. Current threats

Two main sources of hybrid threats may be identified:

1. Russia's current political regime and the expansionist elements in the Russian political spectrum and their supporters, including the Russian diaspora and political forces that support Russian expansionism abroad, and
2. dogmatic Islamist expansionism, including the political forces that support such expansionism in various countries.

The Chinese have also taken actions against the Czech Republic, but these have so far consisted strictly of propaganda and espionage and are thus difficult to assess as hybrid threats or hybrid warfare.

Subversive activities on the part of Russia have been evident in the Czech Republic throughout the era of the country's independence. Pressure intensified in the latter portion of the first decade of this century, when it was proposed that radar for the US missile defense system be located in the country. Russian propaganda supported the anti-radar movement. Once the Ukrainian crisis started, Russia reinforced its activity with massive trolling by the Kremlin and support of paramilitary groupings.

Islamist hybrid warfare targets Western societies and values, including those of the Czech Republic. The country is well-known as an ally of Israel and the US. The visibility of anti-Islamic sentiment in the Czech Republic is also a risk factor, but the country's strategic importance is lower than that of some Western European countries (such as France, Germany, the UK, etc.) from the standpoint of global jihadism.

### 4. International impact on Czech resilience

The security of the Czech Republic is based on membership in NATO and the EU. Its resilience to hybrid threats is closely tied to the resilience of these two organizations. Most of NATO's reaction to current hybrid threats has come after the Ukrainian Crisis and since the rise of the IS in 2014. The issue is not a significant part of the *Active Engagement, Modern Defence* concept of 2010, but new documents and, mostly, concrete actions have been adopted. Neither the EU security strategy from 2003, nor the *EU Internal Security Strategy in Action: Five steps towards a more secure Europe* included any explicit remarks on hybrid threats. However, *Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy* was adopted in June 2016, focusing on hybrid threats and the appropriate resilience of the EU.

## **5. Hybrid threats and hybrid warfare as reflected in Czech strategic documents**

In 2015, the government of the Czech Republic adopted a new version of the 'Security Strategy of the Czech Republic' which includes a section on hybrid threats (and hybrid threats are given priority ranking in the strategy). The *National Security Audit of the Czech Republic*, a unique attempt to check and control the Czech security system in 2015, includes sections on hybrid threats, and other sections of the document include treatments of the theme of resilience to hybrid threats (in the form of the actions of foreign powers, extremism, terrorism, cyber security, and so on).

## **6. Institutional changes**

These strategic documents create a basis for establishing and restructuring security institutions. A governmental Center for Protection against Hybrid Threats and Terrorism is due to be established within the Ministry of the Interior, and some nongovernmental organizations such as European Values (Evropské Hodnoty) have become active in the field, as well.

Adapting the intelligence services and other parts of the security system (like those that address cyber security) is an ongoing process. Public research institutions including Masaryk University are also active in the area. An example is a publication by two Masaryk political scientists, Miloš Gregor and Petra Vejvodová, entitled *Research report: analysis of manipulation techniques on selected Czech websites* in 2016.

## **7. The main gaps**

While the existence of strategies and bodies focused on countering hybrid threats forms a solid foundation, countering these threats efficiently requires cooperation among all parts of the security system as well as the involvement of democratic civil society. The most important 'weapon' against these hybrid threats is a self-confident democratic society willing to defend both democratic values and its own national identity—and this willingness includes paying taxes and supporting an adequate defense budget.

There is a gap between official policy, though, and the laxity of a large section of society that creates a huge problem for Czech politics and hybrid warfare, one which is further complicated by the strong position of pro-Russian expansionist forces in social media and within the political establishment (and to some extent

within security forces). The Czech defense and homeland security budgets seem underdeveloped in the face of the new challenges presented by hybrid warfare.

## 8. Final recommendations

Three main recommendations to counter hybrid threats:

1. **Flexibly adapt the security system to hybrid threats and hybrid warfare** (strategy and tactics, institutions, legal norms, support from the government for civil society and research), including the clear labelling of these threats.
2. **Systematically improve the security system to encompass all serious threats.** Only a comprehensive system with military and homeland security capabilities will be able to resist both “traditional” and “hybrid” threats. Appropriate funding forms an essential prerequisite.
3. **Dialogue with people.** It is important to explain what hybrid warfare and hybrid threats are and why it is important to counter them. Any persuasive campaign should be open and friendly and directed to the interests of citizens—no repackaged McCarthyism, no inane propaganda. Trustworthy persons must be involved.

*About the author:*

*Prof. Miroslav Mareš is Guarantee of the Study Program Security and Strategic Studies of the Faculty of Social Studies of the Masaryk University, external Advisor of the Steering Committee of the National Security Audit of the Czech Republic.*

## Bibliography

- Borák, Mečislav (1996): Česká diverze na Těšínsku v letech 1938-1939 ["Czech Diversionary Tactics in Tešín during the Years 1938-39"]. *Slezský sborník*, Vol. XCIV, No. 1, pp 45-53.
- European Union (2016): Shared vision, common action: a stronger Europe. A global strategy for the European Union's foreign and security policy. [Brussels: European Union]. Available at: [https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs\\_review\\_web.pdf](https://europa.eu/globalstrategy/sites/globalstrategy/files/eugs_review_web.pdf)
- Evropské hodnoty (2016): Jak ubránit českou demokracii před extremismem? ["How to protect Czech democracy against extremism?"], press release [online]. Prague, 26 May 2016. Available at: <http://www.evropskehodnoty.cz/akce/sireni-extremismu/#more-13130> [Accessed 15 November 2016].
- Giles, Keir (2015): Conclusion: is hybrid warfare really new? In: Lasconjarias, Guillaume - Larsen, Jeffrey A. (eds.): *NATO's response to hybrid threats*. Rome: NATO Defense College, Research Division, pp 321-336. ISBN 978-88-96898-12-3. Available at: <http://www.ndc.nato.int/news/news.php?icode=886>
- Gregor, Miloš – Vejvodová, Petra (2016): *Research report: analysis of manipulation techniques on selected Czech websites*. Brno: Masaryk University. Available at: [https://www.academia.edu/27650969/Research\\_Report\\_Analysis\\_of\\_Manipulation\\_Techniques\\_on\\_Selected\\_Czech\\_Websites](https://www.academia.edu/27650969/Research_Report_Analysis_of_Manipulation_Techniques_on_Selected_Czech_Websites)
- Kural, Václav – Vašek, František (2008): *Hitlerova odložená válka za zničení ČSR* ["Hitler's postponed war to destroy Czechoslovakia"]. Praha: Academia. ISBN 978-80-200-1657-7.
- Ministry of Foreign Affairs of the Czech Republic (2015): Security strategy of the Czech Republic 2015. Prague: Ministry of Foreign Affairs of the Czech Republic. ISBN 978-80-7441-007-9. Available at: [http://www.army.cz/images/id\\_8001\\_9000/8503/Security\\_Strategy\\_2015.pdf](http://www.army.cz/images/id_8001_9000/8503/Security_Strategy_2015.pdf)



## **Hybrid Warfare: A New Phenomenon in Europe's Security Environment**

Updated and extended second edition

Published by Jagello 2000 for NATO Information Centre in Prague.

Jagello 2000, Výstavní 8, 709 00 Ostrava, Czech Republic

Tel./Fax.: (+420) 597-479-208

e-mail: [jagello@jagello.org](mailto:jagello@jagello.org)

[www.jagello.org](http://www.jagello.org)

Executive Editor: PhDr. Petr Zlatohlávek

Design: Ivan Zít

Second edition, 2016

NOT FOR SALE

© **Jagello 2000**, 2016

ISBN 978-80-904850-5-1



## **Working definition of hybrid warfare**

Hybrid warfare is an armed conflict conducted by a combination of non-military and military means and aiming with their synergistic effect to compel the enemy to take such steps that he would not do of his own accord. At least one side of the conflict is the state. The main role in achieving the objectives of war is played by non-military means such as psychological operations and propaganda, economic sanctions, embargoes, criminal activities, terrorist activities, and other subversive activities of a similar nature. The attacker's military operations are conducted in secret by irregular forces combining symmetric and asymmetric methods of combat operations against the whole society and, in particular, against its political structures, state authorities and local government, the state economy, the morale of the population and against the armed forces.