Conceptualisation of Hybrid Interference in the Czech Republic: How to Make it a Practically Researchable Phenomenon?[1]

MIROSLAV MAREŠ, JOSEF KRAUS, JAKUB DRMOLA

sciendo

Politics in Central Europe (ISSN 1801-3422)
Vol. 18, No. 3
DOI: 10.2478/pce-2022-0015

Abstract: *The text focuses on the definition and reconceptualisation of the concept of hybrid interference, traces the use of the concept in Czech security documents, presents the historical development of the use of the concept and then seeks a practical conceptualisation applicable towards research on the resilience against it. This conceptualisation includes a narrower definition of the concept, which is necessary for the real application, graspability and researchability of resilience in the context of the Czech environment. We arrive at a framework of hybrid interference that we believe to be more practical and useful, mostly due to its higher clarity and precision. Furthermore, we believe that definition of hybrid interference which is agnostic towards sectors, actors and specific tools used during such activities is preferable and more likely to remain universally relevant than those relying on enumeration and itemisation.*

Keywords: ***hybrid interference, definition, security forces, armed forces, asymmetric warfare, conceptualisation, theoretical framework***

Introduction

The word 'hybrid' has seen a lot of momentum in the area of security research in recent years. Common terminology now includes hybrid strategies, hybrid threats, hybrid operations and others. These are not new concepts or strategies;

1 This article was written within the research project 'Resilience of the Armed Forces and Armed Security Forces to Hybrid Threats' (VJ01010122) funded by the Ministry of the Interior of the Czech Republic / Strategic Support Programme for Security Research in the Czech Republic 2015–2020 (IMPACT 1).

in reality they have been used for a long time, but they have only recently been incorporated conceptually and in terms of security documents. However, from the point of view of security and political science, they are still living and unanchored concepts that are experiencing considerable dynamism. The breadth of the areas that it affects or that are affected by the concept is increasingly wide and more and more phenomena are being labelled as 'hybrid'. The concept has become so all-encompassing as to become essentially meaningless. We consider this state of affairs to be problematic, especially in terms of its practical usefulness within real research or practical applications.

This multiplicity of meanings and coexistence of parallelly-understood narratives of what actually and really is 'hybrid' is already commonly understood and subjected to critical analysis by other authors, both within the Czech Republic (Stojar 2017; Daniel – Eberle 2021) and internationally (for example Arutunyan 2021; Meyers 2016; Murat – Liégeois 2021; Van der Venne 2021). We generally acknowledge and agree with this criticism and further elaborate on some aspects of it below. But our main point is not just to add our criticism to an already large volume of it, but to also seek a solution. We therefore consider it desirable to define this concept more precisely, which is the main aim of this text.

Furthermore, within the context of Czech security terminology and the Czech security community, we consider the term hybrid interference to be the most appropriate overall term, which in our opinion best describes the phenomenon under study. The text presents other terms used in the Czech environment, which appear in security documents or are used by the professional community. Their explanation, definition and focus on the concept of hybrid action is one of the initial intentions of the article. In the following pages we present a brief excursus dealing with the concept and our efforts to get a firmer grasp of it. These should lead to a more rigorous discourse as well as enable practical research in this field. This conceptualisation study represents an initial contribution to the discussion regarding the terminological and definitional refinement of hybrid action with a possible overlap into real-world political science and security research, so that the concept under investigation can be grasped and applied not only at the theoretical level but also directly in practice. An example suitable for the application of the concept is given here as the resilience of security forces and armed forces as typical targets of hybrid interference by an enemy power.

Security documents of the Czech Republic

The Czech Republic has a system of security documents (strategies and related plans, concepts, etc.), which are basically hierarchically organised and interconnected. Although they show a departmental approach, they are generally designed to have an impact on the entire spectrum of public administration. Moreover, they are based on documents of international organisations of which

the Czech Republic is a member. However, the NATO Strategic Concept, which was adopted in 2010, did not deal with hybrid threats (NATO 2010). The Security Strategy of the Czech Republic, which will be described below, preceded the EU Strategic Document on Foreign and Security Policy of 2016 in its date of adoption (hybrid threats are mentioned there as one of several types of threats without further specification) (EU 2016). It is also worth mentioning another document from the EU Security Union Strategy (EU 2020) which addresses hybrid threats in several places and mentions that hybrid attacks might come from state and non-state actors targeting critical infrastructure, information security and political stability. Even the relatively broad definition of hybrid threats by the Centre of Excellence for Combating Hybrid Threats has not yet made a significant impact on the security terminology of the Czech Republic (Hybrid CoE 2021).

The Security Strategy of the Czech Republic is the document with the highest political (not legal) force in the Czech security sphere. Its latest version from 2015 contains important passages on hybrid warfare, which was a reaction to the then developing crisis in Crimea and eastern Ukraine. In 2016, a unique document 'outside of the hierarchy' of the strategies and concepts outlined above was also prepared, namely the National Security Audit, which included a chapter on hybrid threats. This chapter was under the responsibility of the Ministry of Defence, while the entire document was under the responsibility of the Ministry of Interior and was approved by the government. In 2021, the government then approved a specialised strategy document prepared by the Ministry of Defence called 'National Strategy for Countering Hybrid Operations'.

It is therefore possible to perceive differences in terminology (hybrid warfare – hybrid threats – hybrid action), but in principle these terms are used synonymously in the above-mentioned documents of Czech state provenance (although in the scientific literature their differentiation can also be found). In order to define the meaning of hybrid action, the essential elements of the concept or definition in these documents will be taken into account.

The Security Strategy of the Czech Republic works with the concept of 'hybrid warfare methods', which, according to the Strategy, combine 'conventional and unconventional military means with non-military tools (propaganda using traditional and new media, intelligence disinformation actions, cyberattacks, political and economic pressure, sending unmarked members of the armed forces)' (The Government of the Czech Republic 2015: 11).

The National Security Audit (Ministry of the Interior of Tthe Czech Republic 2016: 127) works with the concept of hybrid threats and then develops it under the complementary concept of a hybrid campaign. Specifically, it states:

> *'Even the elementary definition of a "hybrid threat" points to the fact that it cannot be conceived in the same sense as most other threats, where each one represents*

a threat in more or less only one dimension. What we mean by a hybrid threat is primarily the method, the way in which the confrontation or conflict is conducted. This method of conflict management represents a broad, complex, adaptive and integrated combination of conventional and unconventional means, overt and covert activities, primarily of a coercive and subversive nature, carried out by military, paramilitary and various civilian actors. The purpose of a hybrid campaign is to exploit the weaknesses of the adversary; to mask the pursuit of legitimate objectives; to prevent a clear interpretation of events and the discovery of their interconnectedness; to complicate or directly prevent the identification of the perpetrator and to obscure his intentions; to complicate, destabilize or directly paralyze the decision-making process, thereby preventing a timely and effective response by the attacked. The hybrid attacker plots and carries out activities that harm the vital, strategic or general security interests of another actor, while seeking to create an environment where responsibility for these activities cannot (at least formally) be clearly attributed to him or can only be done in a very difficult and speculative manner (the concept of plausible deniability). A hybrid attacker will try to keep its activities below the threshold beyond which the international community would consider armed aggression. It will probably try to avoid direct military confrontation, but it must be assumed that it will incorporate the use of military means in some form in its hybrid campaign.'

Subsequently, the DIMEFIL model is used in the National Security Audit (Ministry of the Interior of the Czech Republic 2016: 128) to further define this when it specifically states:

'A hybrid campaign can combine a number of classic tools from the aforementioned spectrum of spheres of influence, or dimensions of power – DIMEFIL:

D) diplomacy/politics – exerting influence and exerting pressure through the speech and actions of the official political representation;

I) Information – media, social networks and other means of dissemination of information, their manipulative use, disinformation campaign and propaganda;

M) armed forces – this may be overt use as a threat (demonstration of military presence and readiness) or direct combat use or various forms of covert deployment of individuals, small groups and infiltration of the invaded state using them;

E) economy – various forms of economic coercion (imposition of tariffs, embargoes, denial of raw materials or energy supplies, prohibition of the use of transport or transportation routes, destabilization of key industries, enterprises, etc.);

F) financial sector – destabilisation of the currency, stock and bond markets, banking sector, influencing key financial institutions;

I) Intelligence – activities of intelligence services, espionage, recruitment of collaborators (especially state or political officials) for anti-state activities;

L) public order and the rule of law – the use of various subversive activities attacking values, legal and other aspects of the social order, e.g. inciting unrest in the invaded country by exploiting ethnic, religious or social divisions in society, or the use of a wide range of terrorist attacks and other typically criminal methods (e.g. kidnapping, extortion and intimidation).

Cyberspace has a specific position in relation to the above-mentioned tools – it represents an environment where the different dimensions of power intersect, and its importance for the functioning of states and economies is critical.

Cyber attacks can affect and threaten the functioning of public administration, critical infrastructure (electricity supply, etc.), the financial sector, can threaten the security of important facilities, are a means of espionage, disinformation campaigns, etc.'

The National Strategy for Countering Hybrid Interference defines hybrid interference as follows:

'... covert and overt activities of state or non-state actors (the originators of hybrid action) directed against vulnerable elements of the democratic state and society. Hybrid actors use political, diplomatic, informational, military, economic, financial, intelligence and other tools to undermine democratic institutions, rule of law processes and internal security. Hybrid activities also use legal and legitimate-looking tools to achieve hostile objectives and act against the interests of the Czech Republic. The speed, scope and intensity of hybrid activities are increasing, including as a result of the development of new technologies' (Department of Defense 2021: 3).

According to this strategy, the Czech Republic is

'exposed to hybrid interference in the following areas in particular:
a. the ideological basis of the society and the constitutional organization of the state,
b. economy,
c. security and defense' (Department of Defense 2021: 6).

For clarity, the specifications of these areas are given in the following table.

Taking a comprehensive look at the definitions in all the documents mentioned here, it can be stated that the definition of hybrid threats or hybrid action is very broad and basically includes everything or almost everything anywhere on the spectrum between declared war and friendly mutual relations between the Czech Republic and any other non-allied state. This is a very broad concept that complicates scholarly conceptualisation and, in turn, helps politicise these terms. They are subject to a completely free and subjective interpretation and can be used to cover everything from terrorism, cyberattacks, financial manipulation and military exercises.

Table 1: Specification of areas within which the Czech Republic is exposed to hybrid effects.

The ideological basis of the society and the constitutional organization of the state	Overt or covert influence on political structures (including political parties) and the political decision-making process, the courts, the police, the armed forces, the media and public opinion, aimed at destabilizing or splitting society and undermining citizens' confidence in the ideological basis of the country and the constitutional and legal order of the state, including constitutional institutions and the democratic process.
Economic interests of the state	The Czech Republic's dependence on supplies of strategic raw materials from abroad (oil, natural gas, nuclear fuel) and the openness of the Czech economy and its orientation towards exports and foreign investment and loans in strategic sectors of the economy or leading to strategic dependence on their providers. It may seek to dominate strategic sectors of the economy and individual key enterprises, including those that are part of the Czech Republic's critical infrastructure. Hybrid interference may also manifest itself through the private sector's use of modern technologies and technological solutions, such as 5G networks or artificial intelligence, originating from countries with different ideological orientations. Corruption, the interconnection of diplomacy, trade and espionage, or acting in the interests of a foreign power are also risks in this context.
Security and Defence	The security of the Czech Republic may be threatened by the overt or covert use of armed violence directed, for example, against the military engagement of the Czech Republic in NATO and EU missions, operations and other activities, or by the aggressive deployment of intelligence services or special forces of other states on the territory of the Czech Republic. Hybrid interference may include the mobilisation of interest groups (religiously, ethnically, nationally or linguistically defined) or criminal groups to act against the security interests of the Czech Republic and to disrupt public order. There is also a risk of hybrid interference aimed at slowing down or paralyzing decision-making processes in the field of defence and security, including in the context of collective defence within NATO and political and military cooperation within the EU.

Source: Ibid p 6.

This breadth and ambiguity can be (and often is) used (or even abused) by political actors in a self-serving manner and to label events that would not have been perceived as such just a few years ago. In practical politics, Russia and China or their allies are commonly considered to be the main actors of hybrid interference in the Czech Republic (this does not come directly from the documents, although it can be understood from their context). The specificity of contemporary international relations and the state of technology development are also often emphasised, which supposedly qualitatively differentiate the current hybrid interference from the earlier use of similar methods for similar purposes. We are sceptical of this temporocentrism and believe that if there is a practical and objectively researchable concept of hybrid engagement, it should be applicable in the past and in the future and should not depend on the current political situation or its normative assessment.

Historical perspective

In addition to the above-described and very broad concept of hybrid interference, the situation is further complicated by the temporal variability of this concept. The volatility of this family of concepts is well illustrated by their dramatically different understanding in the 1990s and the first decade of the 21st century compared to their understanding today. The Ukrainian crisis since 2014 is a significant break. In the original concept, represented for example by Robert G. Walker (1998) or Francis G. Hoffman (2009), hybrid warfare represents a purely military threat. Indeed, it is a 'hybridisation' of conventional warfare with unconventional operations. This has been seen both as a complex threat that the armed forces must learn to counter (for example, in counterinsurgency), but also as a capability that NATO armies should themselves develop to be able to combine both types of operations flexibly (conventional frontline warfare together with special operations in the enemy's rear). Economic, diplomatic or disinformation aspects did not figure in this original concept of hybrid warfare at all.

It should also be pointed out that, at least in this concept, this is not a new phenomenon and there are many examples of such hybrid warfare in history – from the Roman-Germanic struggles around the turn of the century, through the American War of Independence in the 18th century, to the Vietnam War in the second half of the 20th century (Williamson – Mansoor 2012).

The new understanding of hybrid threats, which is the basis for the Czech security documents cited above, emerged after 2014 in direct relation to the Russian intervention in Ukraine.[2] Analysis by Daniel and Eberle (2018, 907) mapped this process and the relevant actors – 'bureaucrats, NGOs, academics, journalists' – that shaped it. The factor of the combination of conventional and unconventional armed forces in combat operations was thus neglected, and non-military and non-violent (or at least less violent) forms of conflict, such as propaganda, embargoes or attacks in cyberspace, which are intended to destabilise society, came to the fore. It is therefore possible today to actively wage a 'hybrid war' without firing a single shot, contrary to its original understanding.

From the above, it is clear that hybrid warfare is a concept that is both highly fluid and young in time, but also attempts to capture forms of conflict that are already historically familiar and for which various other names have been used – for example, Kennan's (1948) 'political warfare' is a very similar concept, but one that is now largely neglected. It is worth noting that the concept of political warfare has been advocated in relation to Russian activities abroad without

2 Paradoxically, the Russian perception, on the contrary, considers the Euro-American activities in revolutionary Ukraine and the subsequent economic and political pressure on the Russian Federation as a manifestation of the 'gibridnyja vojna', which is, of course, led by the West (Korybko 2015).

the direct use of military force by Mark Galeotti (2020), one of the 'academic architects' of the concept of hybrid warfare.

Practical conceptualisation for research purposes

For the purposes of academic research on hybrid interference and resilience against it, it is necessary to reduce this broad, unstable and ambiguous definition and to focus primarily on those elements that relate to the acceptance of distrust in the ideological values and constitutional institutions and processes of the Czech Republic (or any other state), and therefore the willingness to defend them, and on the potential abuse of one's own abilities and possibilities of these elements in crises in which hybrid action intensifies. At the same time, this concept needs to be practically graspable and realistically investigable, as no research method is able to provide satisfactory, and most importantly useful, answers if the phenomenon under investigation is completely amorphous, vague and could represent practically anything.

For the purpose of more precise and useful conceptualisation, we therefore propose defining hybrid interference as one that meets the following characteristics:

– its objectives are contrary to the security interests of the state targeted by the hybrid interference, while in our context, those defined by the Security Strategy of the Czech Republic would be crucial;

– the hybrid actor's effort is to ensure that these activities are not perceived as a threat, do not trigger any additional security measures, or remain below a certain threshold of response (for example, below the threshold of a state of war, crisis measures, or securitisation (Buzan – Weaver – de Wilde 1998));

– it is implemented as deniable, i.e. the originator of the action uses such methods or intermediary actors in order to plausibly deny responsibility, deny the very existence of such action, deny their hostile nature, or their own involvement;

– it actively destabilises the attacked component of the state and disrupts their function, so it is not merely information gathering;

– its aim is primarily (not exclusively) the psychological impact on the attacked components and their internal disintegration at the systemic and structural level, it is not simply the destruction (physical elimination) of their individual parts.

Our interpretation of the above definitional features also implies that some traditional activities that fall within the provenance of intelligence services, such as espionage or sabotage, may fall outside this definition of hybrid interference. The collection of information on targets of interest (in whatever form) does not in itself have a subversive or destabilising effect, and the information gathered in this way can only subsequently be used for such hybrid operations.

Moreover, this is standard practice for most state actors around the world, targeting not only hostile or non-allied actors, but also allied countries. We view the recruitment of agents in the same way, which in itself may not automatically have a disruptive and destabilising effect on surrounding elements. It is only their subsequent activation, which can of course have a strong psychological and disruptive impact, that we would describe as a hybrid interference.

Similarly, sabotage aimed at destroying a facility, infrastructure or equipment cannot be considered implicitly hybrid if its goal is merely to deny the enemy the asset being destroyed. On the contrary, the situation is reversed if the primary objective of such sabotage is precisely a psychological and destabilising effect. By the same logic, we judge possible assassinations and other similar activities where the goal is not the physical elimination of the target, but the psychological effect on the target audience. It must be added immediately that in reality these two levels may often intersect and overlap, or it may not be entirely clear what the real objective of the attributed attack was, etc. The researcher should first and foremost look for the original intent of the unacknowledged operation, but if this cannot be proven with certainty, the activity can be classified or defined according to its real impact – i.e. whether it was primarily to damage property or eliminate the targeted person, or whether the effect was clearly psychological and influencing the sentiments and behaviour of the targeted society, or whether it causes, for example, the erosion of state sovereignty.

The concept also excludes a number of activities of a diplomatic nature, especially if their aim is merely to pursue one's own interests without disrupting the functioning of the components of another state. Therefore, similar activities of a military nature, for example so-called military diplomacy, or of an economic nature linked to the military or security sector, for example supporting arms exports to another country or one's own arms manufacturers in participating in foreign tenders, can also be excluded. Such support through influence activities of an informational, psychological or even corrupt nature is a common practice, often even admitted. However, if the purpose of these activities was, for example, to buy, control and then cripple the arms industry in the target country or to weaken defence capabilities by supplying deliberately defective material, then this would already fall within our definitional framework of hybrid interference.

Conclusion

In our view, the key strength of our concept is that it is fundamentally agnostic to the specific instruments, actors, environments or sectors of hybrid interference. Thus, it does not matter whether the threats are military, ideological, economic, cultural, or belonging to any other sector, or whether they take place in or outside of cyberspace, or whether the originator is a state, non-state or any

other actor.[3] It is the intended and real effects of such actions that are important, not the specific methods used. This maintains sufficient breadth to work with activities of different nature and in different domains, while also allowing for coverage of future and new forms of activities that are not yet known. This also makes it possible to work with hybrid resilience in its full spectrum and without having to segregate or typologise threats that are often multidimensional and cover several sectors or domains at the same time. This feature, in our view, represents a major practical advantage over the enumerated definitions that have prevailed to date.

Compared to the concept of hybrid action as defined in the National Security Audit by the DIMEFIL model, our concept is therefore much narrower, and some phenomena are thus dropped from it. In particular, these are some forms of diplomatic, economic and intelligence activity (unless there is a deliberate psychological effect towards the subversion of the attacked part of the state) and the direct and open deployment of combat forces (as they lack deniability). We are aware that this puts some phenomena so far potentially understood as hybrid (at least according to some concepts) out of scope, but for the practical application of the concept we believe this is desirable and a narrower definition of hybrid interference is necessary.

The narrowing down of the concept of hybrid threats and hybrid interference presented by us may also contribute to finding more effective way to build applied resilience to these threats. If almost everything is defined as 'hybrid', except for conventional wars and wars waged with weapons of mass destruction, then resilience against hybrid interference can in principle be identified as the entire security policy. A narrower concept of hybrid interference and hybrid threats, on the other hand, can target what specific nature of such action, thus enabling more effective security policies.

Given the high topical relevance (and controversy) of this topic, we also hope that this article will serve as a springboard for further scholarly debates on this concept and its continued refinement, as we do not expect it to be a definitive and immediately universally accepted treatment of this concept.

References

Aratunyan, Anna (2021): "Let's Admit it: The Hybrid War Concept Is Useless." *The Moscow Times*, Nov 23, 2021: available at https://www.themoscowtimes.com/2021/11/22/lets-admit-it-the--hybrid-war-concept-is-useless-a75623.

3 This is further supported by the ability of such aims-oriented conceptualisation to cover all three narratives of hybrid warfare as identified by Daniel and Eberle (2021: 439).

Buzan, Barry – Waever, Ole – de Wilde, Jaap (1998): *Security: A new framework for analysis*. Boulder: Lynne Rienner Publishers, 1998. viii, 239.

Caliskan, Murat – Liégeois, Michel (2021): "The concept of 'hybrid warfare' undermines NATO's strategic thinking: insights from interviews with NATO officials". *Small Wars & Insurgencies*, 32 (2), 295–319, DOI: 10.1080/09592318.2020.1860374.

Daniel, Jan – Eberle, Jakub (2018): "Hybrid Warriors: Transforming Czech Security through the 'Russian Hybrid Warfare' Assemblage". *Czech Sociological Review*, 54 (6), 907–932. doi: 10.13060/00380288.2018.54.6.435

Daniel, Jan – Eberle, Jakub (2021): "Speaking of hybrid warfare: Multiple narratives and differing expertise in the 'hybrid warfare' debate in Czechia". *Cooperation and Conflict*, 56 (4), 432–453. https://doi.org/10.1177/00108367211000799.

Department of Defense (2021): *National Strategy for Countering Hybrid Operations*: available at https://www.mocr.army.cz/assets/informacni-servis/zpravodajstvi/narodni-strategie-pro-celeni-hybridnimu-pusobeni.pdf (21 April 2022).

EU (2016): *Shared Vision, Common Action: A Stronger Europe*. available at https://www.databaze-strategie.cz/cz/eu/strategie/globalni-strategie-zahranicni-a-bezpecnostni-politiky-eu-2016 (21 April 2022).

EU (2020): *EU Security Union Strategy: connecting the dots in a new security ecosystem*: available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605 (21 April 2022).

Galeotti, Mark. (2020): *Russian Political War: Moving Beyond the Hybrid*. London: Routledge.

Government of the Czech Republic (2015): *Security Strategy of the Czech Republic*: available at: https://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf (21 April 2022).

Hoffman, Frank G. (2009): "Hybrid Warfare and Challenges". *Joint Force Quarterly*, 52 (1): vailable at https://smallwarsjournal.com/documents/jfqhoffman.pdf (21 April 2022).

Hybrid CoE (2021): *Hybrid threats as a concept:* available at: https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/ (21 April 2022).

Korybko, Andrew (2015): *Hybrid Wars: The Indirect Adaptive Approach to Regime Change*. Moscow: RPFU: available at https://orientalreview.org/wp-content/uploads/2015/08/AK-Hybrid-Wars-updated.pdf (21 April 2022).

Kennan, George F. (1948): *The Inauguration of Organized Political Warfare*: available at https://digitalarchive.wilsoncenter.org/document/114320.pdf (21 April 2022).

Meyers, Reinhard (2016): "White Knights versus Dark Vader? On the problems and pitfalls of debating hybrid warfare". *Online Journal Modelling the New Europe*, (21), 3–28.

Ministry of the Interior of the Czech Republic (2016): *National Security Audit:* available at https://www.vlada.cz/assets/media-centrum/aktualne/audit-narodni-bezpecnosti-20161201.pdf (21 April 2022).

NATO (2010): *Active Engagement, Modern Defence*: available at https://www.nato.int/lisbon2010/strategic-concept-2010-eng.pdf (21 April 2022).

Stojar, Richard (2017): "Vývoj a proměna konceptu hybridní války." *Vojenské rozhledy*. 2017, 26 (2), 44–55. DOI: 10.3849/2336-2995.26.2017.02.044-055.

Van Der Venne, Timothy (2021): "Old Wine, New Bottles: A Theoretical Analysis of Hybrid Warfare". *E-International Relations*: available at https://www.e-ir.info/2021/11/30/old-wine--new-bottles-a-theoretical-analysis-of-hybrid-warfare/.

Walker, Robert G. (1998): *SPEC FI: the United States Marine Corps and Special Operations*. Storming Media. Naval Postgraduate School Monterey CA.

Williamson, Murray – Mansoor, Peter (2012): *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*. New York, NY: Cambridge University Press.

***Miroslav Mareš** is a professor at the Department of Political Science, Faculty of Social Studies, Masaryk University, specifically in the Security and Strategic Studies programme. From 2001 to 2008 he was a forensic expert in the field of criminalistics. E-mail: mmares@fss.muni.cz; ResearcherID: ID S-6477-2019.*

***Josef Kraus, Ph.D.,** graduated from the Faculty of Social Studies of Masaryk University with a Bachelor's, Master's and Doctoral degree in Political Science. He continues to work there as an assistant professor and head of the Security and Strategic Studies programme at the Department of Political Science. At the same time, he also works at the International Institute of Political Science. He is a member of the editorial board of the journal Vojenské rozhledy. His professional interests include security issues in the Middle East region with a focus on the Islamic Republic of Iran and research on state terrorism. E-mail: jkraus@fss.muni.cz; ResearcherID: S-8905-2019.*

***Jakub Drmola, Ph.D.** currently works at the Department of Political Science at the Faculty of Social Studies of Masaryk University in Brno, specifically in the field of Security and Strategic Studies, where he completed his education. He is also a graduate of the bachelor's degree programme in Systems Engineering and Computer Science at the Faculty of Political Science of the BUT. He focuses on cyber threats, hacktivism, terrorism and the impact of modern technologies on security. E-mail: jdrmola@mail.muni.cz; ResearcherID: V-8599-2019.*