Preventing Hybrid Threats: From Identification to an Effective Response*

Ondřej Filipec**

Summary: This article proposes a model which addresses the issue of hybrid threats in four stages including 1) the analysis and identification of hybrid threats, 2) the designation and selection of tools, 3) building-up resilience and capacities and 4) assessment and evaluation. The article might be considered as an initial contribution to the debate about the build-up of the security architecture at the state level and may provide some inspiration for policy-makers and academia engaged in international security issues. The emphasis is put on "soft" domains of security, especially in relation to the cognitive-emotional element of the hybrid environment which is in the times of Covid-19 and the new Russian hybrid type of warfare becoming increasing significant.

Keywords: Hybrid Threats, Prevention, Hybrid Warfare

1. Introduction

In recent years the security discourse has been consumed with the issue of hybridity including the use of hybrid terms such as hybrid conflict, hybrid warfare, hybrid challenges or hybrid threats. Hybridity has been often used in various contexts and approached mainly from the military perspective. This article focuses on the prevention of hybrid threats merely from the civilian perspective and helps to develop a scheme which might be used for the analysis of hybrid threats and the designation of an effective response. The main aim of the article is to provide a model, which will allow the design of key activities aimed at the prevention of hybrid threats. The model is built on the functional and normative approach to the issue of hybrid threats in four stages: 1) Analysis and identification of

* This article has been written under the grant scheme of Jean Monnet Network Project 611293-EPP-1-2019-1-CZ-EPPJMO-NETWORK "European Union and the Challenges of Modern Society (legal issues of digitalization, robotization, cyber security and prevention of hybrid threats" awarded in 2019 to the Faculty of Law, Palacký University in Olomouc.

** Ondrej Filipec, Ph.D. is a senior lecturer at Faculty of Law, Palacký University in Olomouc, Czech Republic (ondrej.filipec@upol.cz)

hybrid threats, 2) Designation and selection of tools, 3) Building resilience and capacities and 4) Assessment and evaluation.

There are two principal research questions in the article: First, what are hybrid threats and how do they relate to hybrid warfare? And second, how this interrelation might be used to design a model for the effective prevention of hybrid threats *vis-à-vis* hybrid warfare? Here, to answer the question the author is inspired by the work of Sean Monaghan who developed the issue of hybrid threats and hybrid warfare in the context of the continuum of conflict. [1] A response to the research questions provides some clues of how to design effective measures to prevent and supress hybrid threats and build up capacities of the country and societal resilience.

The structure reflects the research design of the article. In the first part hybrid threats are defined in respect to their nature. This part provides several definitions, mainly proposed by military or academia. It also presents several models on how to approach hybridity in terms of threats and warfare. The second part of the article introduces a new model proposed by the author. The model is based on functional logic and due to its abstract nature can be universally applied in approaching hybrid threats. An individual part is dedicated to each of the four stages. It has to be mentioned, that the presented model is not definitive and shall be considered as an initial contribution to the discussion on how to systematize the prevention of hybrid threats as an official part of state policies and state response. The model shall be adapted to specific institutional structure and security architecture.

Since 2015 when the Foreign Affairs Council invited the High Representative to work with the European Commission (and other institutions) to work on a joint framework to help counter hybrid threats, the issue of "hybridity" is on the agenda of the EU.[2] Four priorities accompanied with 22 measures were designed to 1) raise awareness by establishing a dedicated mechanism for the exchange of information, 2) building resilience by identifying potential strategic and critical sectors, 3) preventing, responding to a crisis and recovering by defining effective procedures to follow and 4) stepping up the cooperation and coordination between the EU and NATO as well as other partner organizations. The presented framework is intended to provide "a robust foundation" to support Member states and to set up some guidelines and recommendation in selected

[1] MONAGHAN, S. Countering Hybrid Warfare. So What for the Future Joint Force? *Features*, 2019, vol. 8, no. 2, pp. 82–89.

[2] COUNCIL OF THE EUROPEAN UNION. Outcome of Proceedings. Council Conclusions on CSDP, 18 May 2015, [online]. Available at: <https://www.consilium.europa.eu/media/24520/st08971en15.pdf>

activities.[3] Moreover, hybrid threats are also an important challenge for NATO's security policy.[4] This means, that the umbrella of cooperation has been created at the level of the EU and NATO and now is the time to develop measures and the security architecture at the level of member states. Hopefully, this article will contribute to the debate about its foundations or at least stimulate thoughts about its crucial aspects.

The pandemic of Covid-19, the Chinese propaganda amid the search for a vaccine and the aggressive activities of the Russian Federation demonstrated by its hybrid activities in Ukraine or the poisoning of Alexei Navalny again highlighted the issue of hybrid operations and more generally also hybrid threats. This article focuses mainly on Central and Eastern Europe, especially on the experience of the Czech Republic, which might provide good illustrative examples of hybrid threats. These might be exploited by hybrid operations or what Mikael Wigell calls "hybrid interference".[5] The article is considered as an empirical case study with a significant theoretical dimension due to its abstraction leading to the creation of the theoretical model. Despite the empirical nature provided by reference to various examples, the second part of the study is has a theoretical and partly normative dimension.

2. On the Nature of Hybrid Threats

When one starts dealing with hybrid threats one may simply get confused, as there are various approaches to the issue. When exploring the notion of hybridity we can look at the linguistic which might provide a clue why the notion is understood in different ways. The Merriam-Webster Dictionary provides three definitions of the adjective hybrid: 1) relating to or produced from parents of different species, varieties or breeds; 2) having or produced by a combination of two or more distinct elements: marked by heterogeneity in origin, composition, or appearance; and 3) having two different types of components performing essentially the same function.[6] In the greater abstraction it refers to the contri-

[3] EUROPEAN COMMISSSION. FAQ: Joint Framework on countering hybrid threats, 6. April 2016 [online]. Available at: <https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250>

[4] ZECHERU, T. NATO Challenges in the Context of Hybrid Threats Evolution. *Strategic Impact*, 2015, vol. 55, no. 2, pp. 37–43; KUBEŠA, M., SPIŠÁK, J. Hybrid Threats and Development of NATO's New Operational Concept. *Defence & Strategy*, 2011, vol. 11, no. 2, pp. 5–15.

[5] WIGELL, M. Hybrid Interference as a Wedge Strategy: A theory of External Interference in Liberal Democracy. *International Affairs*, 2019, vol. 95, no. 2, pp. 255-275.

[6] MERRIAM-WEBSTER. Hybrid. Accessed 6. 2. 2020 [online]. Available at: <https://www.merriam-webster.com/dictionary/hybrid>

bution of two or more factors on the subject, which is influenced whose nature is influenced by these factors. Because of several conceptual understandings, the term "hybrid" is even more unclear when used in the social context.

Military historians claim that hybrid warfare involving kinetic and non-kinetic means was used for centuries and that there is nothing new behind the concept. What is new is the re-invention of the term and rather fashion tendency of its use to describe the very complex reality of the modern world of security. One of the first definitions is that of the US Army Chief of Staff who defined hybrid threat as an adversary that incorporates "diverse and dynamic combinations of conventional, irregular, terrorist and criminal capabilities".[7] This definition is quite wide due to the use of general terms allowing it to be covered by a hybrid threat extensive nature of activities. Because definitions using the term "hybrid" tend to be very general, various actors have tried to provide a more precise definition.

For example the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) defines Hybrid threats as *"Methods and activities that are targeted towards vulnerabilities of the opponent. Vulnerabilities can be created by many things, including historical memory, legislation, old practices, geostrategic factors, strong polarization of the society, technological disadvantages or ideological differences"*.[8] The European Council in a press report defined hybrid threats *as a "wide range of methods or activities used by a hostile state or non-state actors in a coordinated manner in order to target the vulnerabilities of democratic states and institutions, while remaining below the threshold of formally declared warfare. Some examples include cyber attacks, election interference and disinformation campaigns, including social media"*.[9] When looking critically closer at the definition, hybrid threats are very close to hybrid warfare, which is not the same, as explained later.

A slightly different definition of hybrid threats is used by the Czech Ministry of Interior defining hybrid threats as *"methods or means used for confrontation/conflict, e. g. wide, complex, adaptive and integrated combinations of conventional and non-conventional tools, open and hidden activities, which are mainly have a character of pressure and undermining activity, which are conducted*

[7] CASEY, G. C. America's Army in an Era of Persistent Conflict. *Army Magazine*, October 2008, [online]. Available at: <https://www.ausa.org/sites/default/files/Casey_1008.pdf>, p. 28.

[8] HYBRID COE. Definition of Hybrid Threats. European Centre of Excellence for Countering Hybrid Threats, 2020 [online]. Available at: <https://www.hybridcoe.fi/hybrid-threats/>

[9] EUROPEAN COUNCIL. Countering hybrid threats: Council calls for enhanced common action. European Council, 10. 12. 2019 [online]. Available at: <https://www.consilium.europa.eu/cs/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/>

by military, semi-military or various civilian actors".[10] As further mentioned methods are exploiting vulnerabilities of the target while the attacker is trying to create an environment in which it is impossible to declare responsibility, the attacker remains hidden and activities are below the level of armed aggression. From a certain perspective, this definition is also close to understanding hybrid threats directly linked to hybrid warfare.

As for academia, the definition used by Mark Galeotti (2016) is most prominent he defined hybrid threats as: *"a style of warfare that combines the political, economic, social and kinetic in a conflict that recognizes no boundaries between civilian and combatant, covert and overt, war and peace ¼ where achieving victory – however that may be defined – permits and demands whatever means will be successful: the ethics of total war applied even to the smallest skirmish"*.[11] Qualitatively, this is the definition of a different nature in comparison to more "technical" definitions of the institutions and political actors directly involved. Mark Galeotti added several more aspects and succeeded in making the definition more general and better matching the nature of hybridity, despite also linking hybrid threats to warfare.

This is, however, the mainstream term. In the literature hybrid threats are often linked to the *hybrid conflict* or *hybrid warfare* or *hybrid challenges*. In this trinity hybrid conflict may be used as the umbrella term for the conflict involving traditional (state) actors with a non-state actor, such as terrorist groups or insurgents. The example of the ISIS serves the issue well. Fighting ISIS was to a certain degree a hybrid conflict, as a number of states together with organizations and NGOs were fighting ISIS which succeeded in creating a quasi-state entity. In this example a regular "underground" terrorist group succeeded in creating a system of institutions, collected taxes, run schools and hospitals etc. Moreover, its fighters employed hybrid warfare which might be characterized by the use of conventional and non-conventional means (ISIS did not respect international norms) and/or the use of traditional and irregular tactics ranging from frontline and guerrilla warfare to warfare in cyberspace. Extensive use of social networks for recreation and propaganda purposes together with the creation of "Cybercaliphate" added a new domain to merely old concepts, which have been known in military studies for decades or even centuries. However, according to Frank Hoffman it was Hezbollah in 2006 during the war with Israel, who demonstrated the best example of hybridity.[12]

---

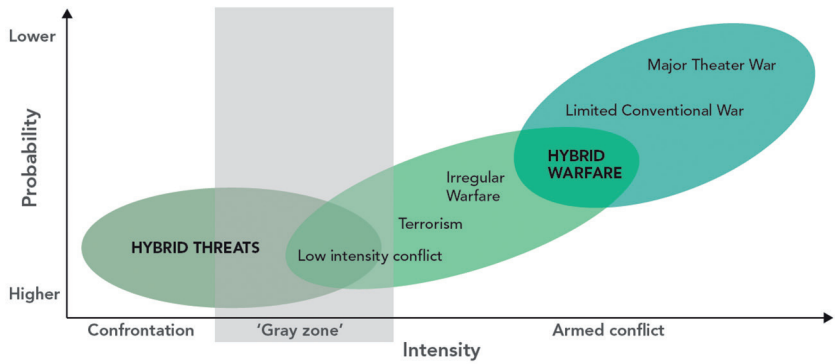
[10] CZECH MINISTRY OF INTERIOR. Co jsou hybridní hrozby? Ministerstvo vnitra, 2020 [online]. Available at: <https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx>

[11] GALEOTTI, M. *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right: Prague:* Mayak Intelligence, 2016.

[12] HOFFMAN, F. G. *Hybrid Threats: Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institte for Policy Studies, 2007.

The military dimension dominates the notions of hybrid conflict and hybrid warfare. This dimension is also present in the term *hybrid challenges*, however the term covers more issues with a different nature and may overlap with *hybrid threats* which are sometimes used as a synonym for *hybrid warfare*. As pointed out by Sean Monaghan, hybrid threats and hybrid warfare are two different things, but the understanding of it may vary. Inspired by Linton Wells[13] and Frank Hoffman[14] Sean Monaghan presented a chart clearly distinguishing between hybrid threats and hybrid warfare (see chart 1).

Chart 1 – Hybrid threats and Hybrid Warfare Shown on s Continuum of Conflict



Source: MONAGHAN, Sean. Countering Hybrid warfare. So What for the Future Joint Force? PRISM, 2019, vol. 8, no. 2, p. 87.

Based on Monahan's hybrid threats differ to hybrid warfare in the terms of conflict intensity and probability. It is merely a set of threats which are present in any security system of a country due to the inability of the state to respond and eliminate roots of the hybrid threats which may arise naturally or that are being created artificially. As a result hybrid threats are merely potential vulnerabilities which might be exploited for confrontation, also involving the employment of hybrid warfare or other means of post-modern conflict.[15] This might be characterized by the absence or low-level of violence.

[13] WELLS, L. Cognitive Emotional Conflict. *PRISM,* 2018, vol. 7, no. 2, p. 6.

[14] HOFFMAN, F. Examining Complex Forms of Conflict: Grey Zone and Hybrid Challenges. PRISM, 2018, vol. 7, no. 4, p. 32.

[15] VALUCH, J., GÁBRIŠ, T., HAMUĽÁK, O. Cyber Attacks, Information Attacks and Postmodern Warfare. *Baltic Journal of Law & Politics*, 2017, vol. 10, no. 1, pp. 63–89.

Linton Wells (2018) highlighted especially the cognitive-emotional dimension of hybrid warfare. The cognitive-emotional conflict is *"a struggle to affect the thoughts and values of people at all levels of an opponent's organization and society, using technical and other informational means, while preserving the resilience of one's own organizations and society, and attracting the uncommitted"*.[16] Critically, the definition highlights the non-violent nature of the conflict, but in some aspects such forms of hybrid warfare may result in riots, protests and uprising and turn violent. Also, hybrid warfare may range from non-violent means to means close to limited conventional war, as seen in the conflict in Ukraine.[17] Nonetheless, in the context of Central Europe the thesis of non-violence applies and cognitive emotional conflict has serious implications for addressing hybrid threats as it is at the core of societal and state vulnerability. For example with a focus on Central and Eastern Europe Vitalie Sîli stresses that hybrid warfare is taking various forms, but there is a need to dedicate a special focus to the manipulation of public opinion, communication undermining the perception of events, interference in political life and the mobilization of large groups of people.[18] This perception is fully in line with the concept of "hybrid interference" by Mikael Wigell.[19]

A very interesting model using a similar logic to Sean Monaghan is a model presented by Mikael Weissmann who had taken into account the different intensities of conflict based on the Swedish strategic map.[20] The map involves various acts which might be classified as peaceful, war or in between in a grey zone (divided in open conflict and crisis). These activities are ranging from "peaceful" partnership, alliance, joint exercises, intelligence to more conflicting like propaganda, hacktivism, assistance, dependence, power demonstration, power projection, intervention, subversion or sanctions to more hostile (cyber-attacks, sabotage, deception, blockade, ultimation to open war), involving limited military operations, invasion, skirmishes or even use of the weapons of mass destruction. The idea of hybridity rests in the intensity of the conflict as between war and peace there is a great grey zone, in which activities may always be interpreted as a misunderstanding when revealed.[21] As a result conductors of hybrid warfare are using various tools which are below the intensity of war and may be interpreted as

[16] WELLS, L., op. cit., p. 8.

[17] VALUCH, J., HAMUĽÁK, O. Abuse of Cyberspace Within the Crisis in Ukraine. *The Lawyer Quarterly*, 2018, vol. 8, no. 2, pp. 94–107; RUSNÁKOVÁ, S. Russian New Art of Hybrid Warfare in Ukraine. *Slovak Journal of Political Sciences*, 2017, vol. 17, no. 3–4, pp. 343–380.

[18] SÎLI, V. Hybrid Threats: Modern Perception and Tactics. *Studia Securitatis,* 2020, vol. 14, no. 1, pp. 37–43.

[19] WIGELL, M., op. cit., p. 255.

[20] WEISSMANN, M. Hybrid warfare and hybrid threats today and tomorrow: towards analytical framework. *Journal Baltic on Security*, 2019, vol. 5, no. 1, pp. 17–26.

[21] Ibid, p. 25.

a "misunderstanding" or any accusation may be labelled as "a provocation". Especially the last scenario is often used by the Russian Federation when operations are triggered, for example in the case of Sergei Skripal poisoning or poisoning of Alexei Navalny, but also in the case of the shooting down of the Malaysian airline's civilian airplane over Ukraine. Despite it seems that the grey zone is central to hybrid warfare (and implicitly also to the hybrid threats), the mutual relationship might be questioned from a conceptual perspective.[22]

A different approach to hybridity is provided by Craișor-Constantin Ioniță. In his study he presents a complex model having hybrid challenges and hybrid threats at the core.[23] This model is unique because it combines several factors of the future security environment from a geographic perspective. In the "Arc of instability", covering most of Africa, Latin America, Asia and Oceania, there are some nuclear armed states, top ten oil reserves, significant drug regions, significant anti-West attitudes and increasing Global interdependence. Moreover, there are emerging global powers, actors using improved anti-access weapons. At the same time, we can observe high urbanization, increased risk of terrorism and crime, relatively frequent earthquakes or famines and diseases. This all contributes to the future security environment. The division is not only between traditional actors or traditional warfare vs. non-state actors and irregular warfare, but also involves a "catastrophic dimension" and disruptive forces.

Despite the great complexity and involvement of the non-military dimension (e.g. societal drivers or environmental issues), the weakness of the model is that it is centred on the third world and focused mainly on the military dimension. However, hybrid threats and hybrid challenges are also the issue of the western world and of its democracies which are developing in a relatively safe and stable environment. For this reason, further parts of the article will focus mainly on the implication of hybrid threats for democracies. Therefore, there will be more focus on the civil rather than the military dimension.

3. Towards Effective Prevention of Hybrid Threats?

The above mentioned models were dealing mainly with hybrid warfare, its potential tools and exploitation of hybrid threats. The look at hybridity was merely approached from outside the state. However, to prevent hybrid threats also requires a look from the inside because many of the roots associated with hybrid

[22] STOKER, D., WHITESIDE, C. Blurred Lines: Grey-Zone Conflict and Hybrid War–Two Failures of American Strategic Thinking. *Naval War College Review*, 2020, vol. 73, no. 1, pp. 1–37.

[23] IONITĂ, C. Is Hybrid Warfare Something New? *Strategic Impact*, 2014, vol. 53, no.4, pp. 61–71.

threats – especially in the context of cognitive-emotional conflict – are domestic and so shall be the primary response. Hybrid threats are often associated with contemporary developments described by the acronym VUCA. At a certain level of abstraction the emergence of hybrid threats may be the result of systemic, institutional and behavioural failures in the volatile, uncertain, complex and ambiguous (VUCA) environment. In other words, no state is able 100 % to address security concerns and prevent the emergence of an environment unfavourable to its vital interests. However, in a certain amount of time the emergence of a hybrid threat is noticed and might be addressed by a systemic response leading to the pacification of the threat or its marginalization. This is the issue of hybrid threats of a domestic nature, however some hybrid threats are exogenous or artificially created and cultivated by external actors, sometimes actors (mainly non-state) itself emerge as a hybrid threat.

From the perspective above hybrid threats have some kind of life cycle: from emergence to getting significance, from maturity to becoming obsolete, disappearing or to the contrary, getting materialized, activated, and exploited. Due to this functional logic, it is possible to design a set of general processes and activities which might help in the prevention of hybrid threats (chart 2).

Chart 2: Set of Activities Aimed at the Prevention of Hybrid Threats

Source: Author

Each of the phases is examined in the individual sub-chapter. However, it is important to mention that the presented model is simplified and in reality, processes might be more complex and demanding. It may also involve more phases or redirections, for example to various levels of strategic planning or to distinguish between the military and civilian dimension. In practice, various institutions will be involved in the process with some link to international organizations, especially those who provide some conceptual frames, capacity sharing etc.

3.1. Analysis and identification of threats

At the beginning of each prevention is analysis of the phenomenon and identification of its most important aspects. In relation to hybrid threats it is worth focusing on causes and consequences: to discover the roots of hybrid threats, factors vital to the threats, revealing their own vulnerabilities, and vectors. At this stage all relevant available data shall be analysed to specify individual threats and gain a deeper understanding of the causes. What is the threat, how does it emerge and what are its characteristics? This is a key activity, which will later help to design and employ relevant tools. Any analysis requires a certain level of expertise. As a result, it is necessary to involve experts who will conduct an in-depth analysis of the threat. Expert involvement will be necessary in all stages leading to the prevention of hybrid threats. It is important to bear in mind that hybrid threats might be explored by hybrid warfare, combining military and civilian tools. It is a warfare which highlighted the role of non-military expertise in areas such as sociology, political science, linguistic, communication, IT, history and other "social sciences" which might be used by the attacker to exploit vulnerabilities of the target, for example by employing disinformation campaigns and propaganda, get influential people on their side, gain control over some important part of economy etc.

Because fields related to hybrid threats are very complex, it is necessary to structure the analysis and demarcate individual domains. For this purpose, analysts are using different schemes named according to the abbreviations of the areas included. Two frequently used schemes are DIME (covering the Diplomatic, Information, Military, and Economic area) or PMESII (Political, Military, Economic, Social, Infrastructure and Information). The schemes might be extended to some specific areas. For example, the Czech Ministry of the Interior is using the DIMEFIL scheme referring to:

- Diplomacy and politics – using influence and pressure created by the official political representation.
- Information – media, social networks and other channels are used to spread manipulation, disinformation and propaganda.

- Military – used as a threat (military presence demonstration), use of military or its individuals, small groups or infiltration of the enemy.
- Economy – used for pressure (custom duties, embargoes, refusal of delivery, prohibiting use of infrastructure, sectoral destabilization, capture of enterprises etc.).
- Finance – currency destabilization, bourse destabilization, adverse influence on financial institutions etc.
- Intelligence – activities of the intelligence services, spying, recruitment of informers or collaborators etc.
- Law – especially public law and legal state: using various activities aimed at attacking value or legal aspects of societal order. For example, supporting unrest by using ethnical, religious or societal conflict lines in society, using large scale terrorist attacks or criminal methods including kidnapping, blackmailing and threating.

The focus on one demarcated area has a clear advantage as it allows the employment of the expert knowledge of a particular specialist. However, it shall be mentioned that the nature of hybrid threats is very complex and in reality, the above defined domains may overlap. Let's build up upon the above provided by the Czech Example. Hybrid warfare in the Czech Republic is mainly associated with Russian influence. Various resources stress, that the Russian embassy in Prague is overstaffed and a significant part of its employees (two thirds out of 137 people) are involved in intelligence activities and espionage against the country.[24] It means that diplomatic and political domains have a direct impact on intelligence due to the foreign influence and limits of the Czech intelligence which is due to the lack of resources unable to counter Russian spies. Moreover, the Russian embassy is a hub of promoting Russian national interests aimed at the economy (another domain). In the Czech case it is the building of the Dukovany Nucler Power Plant, a geo-political bid worth approx. 10 billion Euro and increased dependency for decades. The above-mentioned example well demonstrates, that in analysing hybrid threats (or hybrid interference) experts cannot work in clusters and in-depth analysis of the domains shall be topped by a complex understanding of the threats.

An increasingly important part of the analysis is forecasting and foresight. Under the influence of the bestseller "Superforecasting" by Phillip E. Tetlock and Dan Gardner this part of the analytical process is also gaining a new importance in Central Europe, which is also visible in the project Czech Options

[24] LIDOVÉ NOVINY. Ruská špionská přesilovka. Česko tiše trpí, ruská strana nepokrytě zneužívá disproporce. Lidovky.cz, 5. 9. 2016 [online]. Available at: <https://www.lidovky.cz/domov/ruska-spionska-presilovka-cesko-tise-trpi-ruska-strana-nepokryte-zneuziva-disproporce.A160726_132546_ln_domov_sij>

–inspired greatly by the Good Judgement Project in the USA.[25] Forecasting and foresight is also stressed by Iulian Martin and Lisa-Maria Achimescu. While foresight offers multiple or alternative futures (alternatives how threats will develop) forecasting focuses on the most probable alternative scenario. As put by Martin and Achimescu: *"At both organizational and state levels, a preliminary stage of strategic foresight is necessary in order to determine the most favourable future, in order to correctly and efficiently commit the necessary resources and intelligence according to strategic interests"*.[26] Both foresight and forecasting have an important role in the preparation for future threats. This is particularly difficult in a gradually developing environment and that is why talented experts are needed. Public competitions in forecasting are a good point where to start in the search for people, however, expect skills require training and cultivation. This is why employment of forecasters does not match with pressures on saving and is considered a second order issue despite the fact that their opinion might be crucial for modelling the threats and right designation and selection of tools.

3.2. Designation and selection of tools

Another important step in the prevention of hybrid threats is the designation and selection of tools. Similarly as it is impossible to fight a battle without weapons it is impossible to fight hybrid threats without the appropriate tools and resources. Tools might be civilian, military or hybrid. They might be official and visible, unofficial, or even secret. Also, resources may vary from public to private, from financial and material to non-material. It is evident that the availability of tools will vary state to state, depending on institutional, personal, or financial capacities. For example, in the USA the so called "Intelligence Community" is composed of 17 agencies and offices, including the well known Central Intelligence Agency, National Security Agency, Defence Intelligence Agency to the lesser known such as the Office of Intelligence and Analysis or National Reconnaissance Office. With a budget of more than 60 billion USD and employing100 thousand people the USA has different options for the designation and selection of tools.[27] However, the USA are facing qualitatively different challenges and even its massive apparatus failed to predict and prevent important failures which

[25] GARDNER, D., TETLOCK, P. E. *Superforecasting: The Art and Science of Prediction*. New York: Crown, 2015.

[26] MARTIN, I., ACHIMESCU, L. M. Can Forecasting Ameliorate the Negative Impact of Hybrid Threats? *Strategic Impact*, 2018, no. 1–2, p. 13.

[27] OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. U. S. Intelligence Community Budget, [online]. Available at: <https://www.dni.gov/index.php/what-we-do/ic-budget>

has something to do with hybridity. The attacks on 9/11 are considered one of the biggest failures of the Intelligence community in modern history, merely because the signs of the threat were ignored, and experts were working in clusters.

Next to finances and resources, the selection of tools is also a matter of political culture and national experience. It is obvious that democratic countries will have different attitudes than non-democratic countries. The level of democracy and political culture will have an impact on the involvement of the state: the state cannot penetrate all areas in society and thus more space in democracies will be given to civil society whose tools might fill the gap by qualitatively different approach, then there are the tools operated by a state. In the area of intelligence investigative journalists may play a similar or even more important role than national intelligence. A good example is the Bellingcat group focusing on the online instigation and use of public resources to report about the downing of flight HM-17, Sergej Skripal and Alexei Navany poisoning, military operations in Syria etc. Factchecking and reconstructions of facts might be vital for preventing the adverse effects of information warfare.

Based on classification scheme tools might be created and developed within individual domains (e. g. DIMEFIL). Most of the tools already exists and just require some adaptation or redesign. For example, the institution of diplomatic consultation within the diplomatic domain might serve well in prevention and reaction. Military IT experts might be well used to countering the hostile content on civilian platforms and social networks (information operations on social networks are an integral part of the Russian military doctrine) as the manipulation of public opinion becomes an important part of hybrid warfare and hybrid interference. In this sense social media are an increasingly important tool of information warfare.[28] Especially in the case of referenda and elections the damage caused by foreign influence might be irreversible. This is also the case of Brexit – which was strongly influenced by Russia on the side of leave. The City University of London analysed 10 million twitter messages and found 13,493 false or automatic generated profiles linked to Russia.[29] According to marketing company 89up, the Kremlin directed channels had thirteen times more impressions for all content shared by Leave.EU website, than the official campaign.[30] The effects have both economic and geostrategic importance. As for 2020 the

[28] PRIER, J. Commanding the Trend: Social Media as Information Warfare. *Strategic studies Quarterly*, 2017, vol. 11, no. 4, pp. 50–85.

[29] MORALES, S. Information warfare: feed information with disinformation. *Global Strategy*, 2019 [online]. Available at: <https://global-strategy.org/information-warfare-feed-information-with-disinformation/>

[30] 89UP. 89up releases report on Russian influence in the EU referendum, 2019 [online]. Available at: <http://89up.org/russia-report>

costs for Brexit are calculated around 200 billion Pounds[31] and the future of the EU-UK security partnership is uncertain.

Tools and measures designed in accordance with priorities and goals might be utilized as reactionary or pro-active. Most of them are of a conventional nature: starting with legal regulation and enhancement of moral norms, to economic tools including trade restrictions or sanctions, limit of resources, information media and propaganda intervention, intelligence operations, cultural and diplomatic pressures, use and involvement of proxies, covert operations etc. Addressing hybrid threats usually requires a unique and balanced mixture of selected tools to address the hybrid nature of the threat, minimalize or paralyze its effects and remove the causes, including factors vital for its emergence. While some effects might be neutralized within a short period of time (e. g. neutralization of a foreign proxy), in some cases the roots might be very dense and deeply rooted into the society and their removal will require a long term approach (typically issues related to national mentality, identity, ideology or history which require change of the discourse or paradigm shift). Despite this the Islamic State was defeated on the ground, the roots of this terrorist organization including ideological resources are still deeply rooted within Iraqi and Syrian society.

Threat modelling has a special position among tools , which might share some common characteristic with an experiment. Great models might succeed in modelling and simulating hybrid threats in the safe environment, which is particularly possible in the IT domain with the use of "white hackers" and other domains challenging human skills. In this environment designed tools might be tested, developed and reviewed and when ready verified and deployed in practice. Typical activities conducted within a modelled environment are penetration tests or "stress tests" verifying resilience, existence of capacities and its utilization to address the threat. Despite this domain is most developed in the area of IT, including online tools such as Tutamantic, My App Security, Irius Risk, Mozilla Sea Sponge and dozens of others, IT domain offers a range of threat modelling methodologies (Trike, Process for Attack Simulation and Threat Analysis or Microsoft's STRIDE approach) which might be modified to cover hybrid threats and potential hybrid warfare.

[31] THE LONDON ECONOMIC. Brexit set to cost the UK more than £200 billion by the end of the year. The London Economic, 16. 6. 2020 [online]. Available at: <https://www.thelondoneconomic.com/politics/brexit-set-to-cost-the-uk-more-than-200-billion-by-the-end-of-the-year/16/06/>

3.3. Building resilience and capacities

Resilience and capacities are necessary prerequisites of a country capable of dealing with hybrid threats (or what Mikael Wigell calls "hybrid interference") and prevent internal instability, erosion of democratic institutions or in the case of hybrid interference counterbalancing potential.[32] This is hard, because the selection of effective tools and the building up of resilience and capacities is in democracies bound by the rules of law and democratic principles. Building a resilient society and capacities is a long term process which requires analysis and identification of vulnerabilities and unhealthy developments. Effects of hybrid threats are threatening to weaken the state from inside with a focus on civil society and the attempt to undermine the effectiveness or reputation of public institutions to invoke instability or alternation of forces within the elites favourable to the attacker.

In Central Europe hybrid threats are often used almost as a synonym for hybrid warfare, associated mainly with the Russian Federation.[33] This is given by the geo-political nature of the region which was historically an arena of clashes between western and Russian (Soviet) interests and power aspirations. However, contrary to the 20th century when these aspirations were accompanied by hard power and military interventions, it seems that in the 21st century Russian aspirations have shifted to the on-line environment, diplomacy, and economic activities with geostrategic importance.

Building the resilience of society in Central Europe closely related to the enforcement of identity, especially its historical aspects which goes hand in hand with the refusal of historical revisionism – uncritical adoration of Russia/Soviet history and demonization of the west. The myth of the Red Army liberation and its uncritical glorification is still present in education plans and according to Czech intelligence it helps to create an environment for supporting Russian interests.[34] Unsurprisingly, both the above mentioned narratives are strongly present in pro-Kremlin propaganda on social networks and diplomatic communications. In this regard building resilience requires the development of medial literacy, critical thinking, and quality education in general with a special focus on history, social sciences, medial communication and other relevant fields which are helpful for a better understanding of social reality and the interests of individual actors. From this point of view the building-up of resilience starts at schools and

[32] WIGELL, M., op. cit., p. 255.

[33] This association is very strong in Poland. See for example: BANASIK, M. Building up State Strategic Resistance Against Hybrid Threats. *Journal of Defense Resources Management*, 2017, vol. 8, no. 2, pp. 50–63.

[34] BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. Výroční zpráva Bezpečnostní informační služby za rok 2017 [online]. Available at: <https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2017-vz-cz.pdf>

universities and also involves the most fragile groups – older people and people from excluded groups who might be exploited for promotion of frustration, dissolution, and activation of protest behaviour.

Well educated citizens might help to elect political representation critical towards foreign interference and hybrid threats. As a result the ministry of foreign affairs can launch initiatives to limit foreign influence, ministries of the interior and defence can develop tools and measures preventing the takeover of strategic enterprises or the ministry of education can work on training and curriculum of a new generation more perceptive to hybrid threats. Civil society plays an important role which might well contribute to the building-up of resilience. Various NGOs are active in delivering social services and care – limiting frustration and the potential of protests. Advising NGOs helping people in difficult economic and social situations which has a positive impact on the unhappiness and frustration, which are exploited by propagandists to stimulate protest attitudes. Other NGOs are focused on the development of critical thinking and promotion of medial literacy, factchecking and are complementing the education not provided by the education system. Various associations contribute to the recruitment of experts, think-tanks offer policy advising and sometimes are also involved in surveillance.

Civil society thus has an important role to play in the building-up of resilience and that is why any attempts to restrict its activities shall be considered as a potential threat and feature of unhealthy development. However, the importance of civil society has been noted by strategists and that is why the so called "political NGOs" are subject to restrictions in illiberal or authoritarian regimes while government or regime friendly NGOs are supported and promoted. Moreover, some parts of the civil society are contributing to the erosion of democracy. This is the case of "uncivil civil society" which might in some cases result in the creation of militias or paramilitary organizations linked or sympathizing with foreign powers. The environment of these organizations might be a potential reservoir for people open to promote foreign interests inconsistent with that of the domestic country. The same is valid for disinformation webs and conspiracy platforms which contribute to the spread of distrust in the government, public institutions, promotion of hostile foreign interests and erosion of democracy by attacks on public institutions. The QAnon affair and Covid-19 highlighted the importance to counter disinformation webs as conspiracies might lead to unprecedented events or loss of lives.

Similarly, important is the build-up of capacities to act. Hybrid threats might be latent or developing slowly and thus offering opportunity to act. However, even when considering this advantage the reaction of state institutions is slow and in many cases insufficient. This might be due to a lack of funds, burden of bureaucracy, overlapping responsibilities, lack of leadership, lack of political will etc.

That is why it is necessary to create a complex strategy aimed at hybrid threats, divide tasks and responsibilities, define tools and departments responsible for maintenance and utilization of the tools. Activities of the individual institutions – e.g. ministries or public offices – shall be the subject of coordination and regular evaluation to ensure synergy and maximum effect in addressing hybrid threats. Nonetheless, to establish a coordinated and effective system might be complicated due to the opposition of the political actors involved. Nationalists and populists tend to undermine the intelligence services. For example, pro-Russian Czech President Miloš Zeman on several occasions criticized Czech intelligence pointing at Russian influence in the Czech Republic for being unprofessional[35] and political parties including the Czech communist party or nationalists (Freedom and Direct Democracy Party) underplay hybrid threats and conclusions of intelligence. It is not surprising, that both illiberal political streams are favourable to the Russian Federation and thus promotes a reduction in expenditures on the military, exit from the EU and NATO or restrictions on civil society, which are also visible in Poland or Hungary, two states experiencing illiberal turn.[36]

The human aspect has a prominent position in resilience and capacity building. That is why a lot can be achieved by training and education. More than ever before (partially because activities are going online including social life and individual electronic footprint is increasing) soft skills such as medial literacy, IT skills and critical thinking are of increasing significance and have a potential to become new cleavage in the society. The scandal with Cambridge Analytica clearly demonstrated that personal data might be misused for persuasion and political manipulation, which might be directed against democratic processes and institutions. Prevention of hybrid threats usually focuses on "traditional" strategic sectors such as energy, transportation, defence infrastructure etc. while "soft" sectors were for a long time being ignored, despite some authors mentions the importance of soft sectors as well (e.g. NGOs, riots and demonstrations, press articles and blogs favouring certain ideological frames) and others.[37] As demonstrated by QAnon conspiracy, unsolved intoxication of the environment can result in the division of society and stimulate radicalization, extremism and

[35] DENIK. Jsou to čučkaři, řekl o BIS Zeman. Jeho výroky bude řešit senátní výbor. Deník, 10. 12. 2018 [online]. Available at: <https://www.denik.cz/z_domova/jsou-to-cuckari-rekl-o-bis-zeman-jeho-vyroky-bude-resit-senatni-vybor-20181210.html>

[36] SUYUNOVA, K. The Conflict between the Principles of the National Identity of Member States and Values of European Union Such as Rule of Law, Respect of Human Rights and Liberal Democracy – Case Study of Hungary. *International and Comparative Law Review*, 2020, vol. 20, no. 2, pp. 159–173.

[37] CÎRDEI, I. A. Countering the hybrid threats. *Revista Academiei Fortelor Terestre,* 2016, vol. 82, no. 2, pp. 113–119.

political violence. That is why designers of security architecture shall not ignore soft sectors.

3.4. Evaluation and lessons learned

Every system identifying and responding to hybrid threats shall have internal evaluation mechanisms aimed at effectiveness on several levels. First it is the level of individual tools and its use, then it is the level of individual institutions involved and finally, it is macro level of the whole environment where fulfilment of more general goals might be evaluated. A necessary part of this phase is also learning the lessons learned based on previous experience. This is because one thing is theoretical preparation and plans, another issue is experience with real confrontation. As put by Field Marshal Helmut von Moltke the Elder: "No plan of operations extend with any certainty beyond the first contact with the main hostile force".[38] In other words, strategists and actors employing hybrid warfare are very inventive and innovative in their tools and tactics and addressing hybrid threats (which might be exploited by hybrid warfare) will be to a significant degree a reactive tasks. However, even belated, and limited reaction is usually better than any as the hostile acts may be close to critical threshold of threat: latency may turn into materialization and the materialized threat can cause real problems in society and state.

Next to the evaluation and lessons learned from actors directly involved a focusing on the evaluation and surveillance within individual fields which might also lead to fruitful lessons being drawn. For example, cyber-attacks on hospitals might reveal a systemic flaw which might be addressed in the legislative, institutional build-up[39] and responsive efforts.[40] However, many observations are less technical and less formal. When conducting research on one of the hospitals attacked by ransomware, one of the actors was disappointed about the lack of the fora or networks to share practical IT experience, managerial experience, or lack of shared solidarity among stakeholders at the same level. In other words, breaches and failures are treated individually, without the utilization of good experience by sharing and improvement of the system. It is necessary not only to evaluate and

[38] VON MOLTKE, H. G. *Moltke on the Art of War: Selected Writings*. In: HUGHES, D. J., BELL, H. New York: Presidio Press, 1996, p. 92.

[39] NAPETVARIDZE; V., CHOCHIA, A. Cybersecurity in the Making – Policy and Law: a Case Study of Georgia. *International and Comparative Law Review*, 2019, vol. 19, no. 2, pp. 155–180.

[40] VALUCH, J., HAMUĽÁK, O. Use of Force in Cyberspace. *International and Comparative Law Review*, 2020, vol. 20, no. 2, pp. 174–191; FERNICOLA, G. Once Upon a Time in Cyberspace: A Grim Reality about the Dangers of Cyberwarfare. *International and Comparative Law Review,* 2020, vol. 20, no. 2, pp. 77–96.

draw lessons learned, but also on a case by case basis to "distil" aspects which might be used to improve the system on the level of planning or capacity building.

As shown in chart 2, prevention of hybrid threats is a never-ending circle and data mined in the final stage by evaluation and lessons learned are vital for different phases of the cycle. Because the environment is developing data from the last stage might be used for initial analysis and identification of threats, which shall be conducted on a regular and systematic basis. Next to the evaluation system and lessons learned it is critically important to utilize the gathered information at the political level. The effectiveness of any regime depends on the quality of information and how effectively they are processed into policies. When misinformation and lies penetrates the system, then the efficiency of public institutions is undermined. Low quality information in the system creates a visible gap between official policies and reality. This is common for all regimes non-democratic and democratic alike. In the final days of World War II Adolf Hitler was moving virtual units on the map, which were destroyed weeks ago. Communist leaders mismanaged the Chernobyl disaster because flaws in the system failed to provide them reliable information. This example best demonstrates the gap between science and politics. Also, the effectiveness of democratic institutions relies (among others) on the quality of information processed. The Covid-19 pandemic again highlighted this importance.

The Covid pandemic was a critical moment with a potential to destabilize European societies. On one hand there was a force "sticking" people together in the terms of solidarity and help, on the other side there were attempts to polarize society and promote unhappiness with political institutions. The pandemic highlighted the chronic problems of disinformation and propaganda – the tools that are exploiting and cultivating cognitive-emotional conflict and can invoke and shape protest attitudes of citizens which might have destructive consequences. The challenge is how to protect democratic institutions without compromising democratic values, civic liberties, freedoms, and human rights on one side and to ensure the building-up of capacities and societal resilience on the other. More multidisciplinary research will be required in these areas.

4. Conclusion

The main aim of the article was to provide a model, which will allow the design of the key activities aimed at the prevention of hybrid threats. The model was built on the functional and normative approach to the issue of hybrid threats in four stages: 1) Analysis and identification of hybrid threats, 2) Designation and selection of tools, 3) Building resilience and capacities and 4) Assessment

and evaluation. There were two principal research questions: First, what are the hybrid threats and how they relate to hybrid warfare? And second, how this interrelation might be used to design a model for the effective prevention of hybrid threats *vis-á-vis* hybrid warfare?

As pointed out in the first chapter hybrid threats and hybrid warfare are two different things, despite being related as hybrid warfare may exploit hybrid threats. The article proposed a complex model for responding to hybrid threats by highlighting a set of activities in the individual stages of the process. During the stage of analysis and identification of hybrid threats, several schemes were presented to conduct analysis, also with reference to forecasting and foreseeing. In the second stage designation and selection of tools was debated including the tools for modelling the threat. In the third stage some tips were provided for building the resilience and capacities and the same is valid for the fourth stage. Because many conceptual documents and approaches focus on traditional domains of security, this article was dealing mainly with examples associated with "soft" domains of security – e.g. public opinion manipulation, disinformation, and propaganda – having close to cognitive-emotional understanding of hybrid threats and hybrid warfare.

This article is an initial contribution to the debate and further research might be done on related aspects. For example: how to effectively implement processes designed in the second part of the article within the security architecture of the state? how to effectively divide responsibilities and powers among individual institutions? Or: how to implement individual activities to create an effective response to hybrid threats without compromising democratic values?

List of references

89UP. 89up releases report on Russian influence in the EU referendum, 2019 [online]. Available at: <http://89up.org/russia-report>

BANASIK, M. Building up State Strategic Resistance Against Hybrid Threats. *Journal of Defense Resources Management*, 2017, vol. 8, no. 2, pp. 50–63.

BEZPEČNOSTNÍ INFORMAČNÍ SLUŽBA. Výroční zpráva Bezpečnostní informační služby za rok 2017 [online]. Available at: <https://www.bis.cz/public/site/bis.cz/content/vyrocni-zpravy/2017-vz-cz.pdf>

CASEY, G. C. America's Army in an Era of Persistent Conflict. *Army Magazine*, October 2008, [online]. Available at: <https://www.ausa.org/sites/default/files/Casey_1008.pdf>, p. 28.

CÎRDEI, I. A. Countering the hybrid threats. *Revista Academiei Fortelor Terestre,* 2016, vol. 82, no. 2, pp. 113–119.

COUNCIL OF THE EUROPEAN UNION. Outcome of Proceedings. Council Conclusions on CSDP, 18 May 2015, [online]. Available at: <https://www.consilium.europa.eu/media/24520/st08971en15.pdf>

CZECH MINISTRY OF INTERIOR. Co jsou hybridní hrozby? Ministerstvo vnitra, 2020 [online]. Available at: <https://www.mvcr.cz/cthh/clanek/co-jsou-hybridni-hrozby.aspx>

DENIK. Jsou to čučkaři, řekl o BIS Zeman. Jeho výroky bude řešit senátní výbor. Deník, 10. 12. 2018 [online]. Available at: <https://www.denik.cz/z_domova/jsou-to-cuckari-rekl-o-bis-zeman-jeho-vyroky-bude-resit-senatni-vybor-20181210.html>

EUROPEAN COMMISSSION. FAQ: Joint Framework on countering hybrid threats, 6. April 2016 [online]. Available at: <https://ec.europa.eu/commission/presscorner/detail/it/MEMO_16_1250>

EUROPEAN COUNCIL. Countering hybrid threats: Council calls for enhanced common action. European Council, 10. 12. 2019 [online]. Available at: <https://www.consilium.europa.eu/cs/press/press-releases/2019/12/10/countering-hybrid-threats-council-calls-for-enhanced-common-action/>

FERNICOLA, G. Once Upon a Time in Cyberspace: A Grim Reality about the Dangers of Cyberwarfare. *International and Comparative Law Review,* 2020, vol. 20, no. 2, pp. 77–96. DOI: https://doi.org/10.2478/iclr-2020-0004

GALEOTTI, M. *Hybrid War or Gibridnaya Voina? Getting Russia's non-linear military challenge right: Prague:* Mayak Intelligence, 2016.

GARDNER, D., TETLOCK, P. E. *Superforecasting: The Art and Science of Prediction*. New York: Crown, 2015.

HOFFMAN, F.G. *Hybrid Threats: Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies, 2007.

HOFFMAN, F. Examining Complex Forms of Conflict: Grey Zone and Hybrid Challenges. *PRISM*, 2018, vol. 7, no. 4, p. 32.

HYBRID COE. Definition of Hybrid Threats. European Centre of Excellence for Countering Hybrid Threats, 2020 [online]. Available at: <https://www.hybridcoe.fi/hybrid-threats/>

IONITĂ, C. Is Hybrid Warfare Something New? *Strategic Impact*, 2014, vol. 53, no.4, pp. 61–71.

KUBEŠA, M., SPIŠÁK, J. Hybrid Threats and Development of NATO's New Operational Concept. *Defence & Strategy*, 2011, vol. 11, no. 2, pp. 5–15.

LIDOVÉ NOVINY. Ruská špionská přesilovka. Česko tiše trpí, ruská strana nepokrytě zneužívá disproporce. Lidovky.cz, 5. 9. 2016 [online]. Available at: <https://www.lidovky.cz/domov/ruska-spionska-presilovka-cesko-tise-trpi-ruska-strana-nepokryte-zneuziva-disproporce.A160726_132546_ln_domov_sij>

MARTIN, I., ACHIMESCU, L. M. Can Forecasting Ameliorate the Negative Impact of Hybrid Threats? *Strategic Impact*, 2018, no. 1–2, p. 7–15.

MERRIAM-WEBSTER. Hybrid. Accessed 6. 2. 2020 [online]. Available at: <https://www.merriam-webster.com/dictionary/hybrid>

MONAGHAN, S. Countering Hybrid Warfare. So What for the Future Joint Force? *Features*, 2019, vol. 8, no. 2, pp. 82–89.

MORALES, S. Information warfare: feed information with disinformation. *Global Strategy*, 2019 [online]. Available at: <https://global-strategy.org/information-warfare-feed-information-with-disinformation/>

NAPETVARIDZE, V., CHOCHIA, A. Cybersecurity in the Making – Policy and Law: a Case Study of Georgia. *International and Comparative Law Review*, 2019, vol. 19, no. 2, pp. 155–180. DOI: https://doi.org/10.2478/iclr-2019-0019

OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE. U. S. Intelligence Community Budget, [online]. Available at: <https://www.dni.gov/index.php/what-we-do/ic-budget

PRIER, J. Commanding the Trend: Social Media as Information Warfare. *Strategic studies Quarterly*, 2017, vol. 11, no. 4, pp. 50–85.

RUSNÁKOVÁ, S. Russian New Art of Hybrid Warfare in Ukraine. *Slovak Journal of Political Sciences*, 2017, vol. 17, no. 3–4, pp. 343–380.

SÎLI, V. Hybrid Threats: Modern Perception and Tactics. *Studia Securitatis,* 2020, vol. 14, no. 1, pp. 37–43.

STOKER, D., WHITESIDE, C. Blurred Lines: Grey-Zone Conflict and Hybrid War–Two Failures of American Strategic Thinking. *Naval War College Review*, 2020, vol. 73, no. 1, pp. 1–37.

SUYUNOVA, K. The Conflict between the Principles of the National Identity of Member States and Values of European Union Such as Rule of Law, Respect of Human Rights and Liberal Democracy – Case Study of Hungary. *International and Comparative Law Review*, 2020, vol. 20, no. 2, pp. 159–173. DOI: https://doi.org/10.2478/iclr-2020-0022

THE LONDON ECONOMIC. Brexit set to cost the UK more than £200 billion by the end of the year. The London Economic, 16. 6. 2020 [online]. Available at: <https://www.thelondoneconomic.com/politics/brexit-set-to-cost-the-uk-more-than-200-billion-by-the-end-of-the-year/16/06/>

VALUCH, J., GÁBRIŠ, T., HAMUĽÁK, O. Cyber Attacks, Information Attacks and Post-modern Warfare. *Baltic Journal of Law & Politics*, 2017, vol. 10, no. 1, pp. 63–89. DOI: https://doi.org/10.1515/bjlp-2017-0003

VALUCH, J., HAMUĽÁK, O. Abuse of Cyberspace Within the Crisis in Ukraine. *The Lawyer Quarterly*, 2018, vol. 8, no. 2, pp. 94–107.

VALUCH, J., HAMUĽÁK, O. Use of Force in Cyberspace. *International and Comparative Law Review*, 2020, vol. 20, no. 2, pp. 174–191. DOI: https://doi.org/10.2478/iclr-2020-0023

VON MOLTKE, H. G. *Moltke on the Art of War: Selected Writings*. In: HUGHES, D.J.; BELL, H. New York: Presidio Press, 1996.

WEISSMANN, M. Hybrid warfare and hybrid threats today and tomorrow: towards analytical framework. *Journal Baltic on Security*, 2019, vol. 5, no. 1, pp. 17–26.

WELLS, L. Cognitive Emotional Conflict, *PRISM,* 2018, vol. 7, no. 2.

WIGELL, M. Hybrid Interference as a Wedge Strategy: A theory of External Interference in Liberal Democracy. *International Affairs*, 2019, vol. 95, no. 2, pp. 255–275.

ZECHERU, T. NATO Challenges in the Context of Hybrid Threats Evolution. *Strategic Impact*, 2015, vol. 55, no. 2, pp. 37–43.