ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

Publisher
http://jssidoi.org/esc/home

INTEGRATED SECURITY STRATEGIES IN THE CONTEXT OF HYBRID THREATS IN THE SLOVAK REPUBLIC*

Antonín Korauš [1], Patrícia Krásná [2], Stanislav Šišulák [3], Stanislava Veselovská [4]

[1,2,3] Police Academy in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia
[4] Pan-European University in Bratislava, Faculty of Economics and Entrepreneurship, Tematinská 10, 851 05 Bratislava, Slovakia

E-mails: [1]antonin.koraus@akademiapz.sk; [2]patricia.krasna@akademiapz.sk; [3]stanislav.sisulak@akademiapz.sk; [4]stanislava.veselovska@paneurouni.com

Received 29 July 2023; accepted 29 September 2023; published 30 September 2023

Abstract. The presented study results from qualitative research conducted within the national project "Increasing Slovakia's resilience to hybrid threats by strengthening public administration capacities". Its content reflects the fulfilment of the main goal – identifying four pillars that need to be understood in connection with the concept of hybrid threats and a specific focus on the Police Force or members of the Police Force as well as experts from practice from the National Security Office. The authors also examine the definitions and conceptualisation of hybrid threats, which subsequently led them to identify the key features appropriate for the framework of the chosen research. When preparing this study, theoretical scholarly knowledge from the professional literature and the practical experience of experts from practice were processed. The authors also drew on facts they acquired during guided interviews conducted between May and July 2023 with members of the "first contact" point of the Police Force, general crime investigators, future Police Force members, students of the Police Force Academy in Bratislava and experts from practice, to gain insights and also to detect ambiguities in connection with the concept of hybrid threats.

Keywords: security; hybrid threat; Police Force; hybrid threat actors; hybrid threat tools; hybrid threat domains; hybrid threat phases; students

Reference to this paper should be made as follows: Korauš, A., Krásná, P., Šišulák, S., Veselovská, S. 2023. Integrated security strategies in the context of hybrid threats in the Slovak Republic. *Entrepreneurship and Sustainability Issues*, 11(1), 233-250. http://doi.org/10.9770/jesi.2023.11.1(14)

JEL Classifications: F52, H56, K22, K32

Additional disciplines: Security

* *The contribution was created within the national project "Increasing Slovakia's resilience to hybrid threats by strengthening public administration capacities", project code ITMS2014+:314011CDW7. This project is supported by the European Social Fund.*

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

1. Introduction

The presented study reflects on the need to ensure the building and maintenance of the security of the Slovak Republic through knowledge of the concept of hybrid threats by members of the Police Force. Over the past decade, several comprehensive strategies focused on reducing the risk of specific security threats, economic growth, improving social security and cyber security, and environmental protection have been formulated at the national level. However, the application and financing needed to carry out these strategies and concepts must be more synchronised and coordinated. No sufficiently effective system to help coordinate relevant actions and activities in the field of security and crisis management is present aside from those that are currently provided, managed and coordinated in a time of war or a state of war by the Government of the Slovak Republic and the Ministry of Defence of the Slovak Republic (Concept of the Security System of the Slovak Republic 2023).

The study reflects on the need to conduct ongoing research but also on facts that were studied in the research of the authors collective (Mazaraki, Kalyuzhna and Sarkisian 2021) based on results showing that a transformation of modern interstate conflicts is taking place in the direction of their acquiring hybrid features. These hybrid signs and manifestations are understood to be a process that employs different means of coercion, predominantly non-military. The authors also state that an urgent task for countering hybrid threats is to assess the probability of danger arising from the multi-application dimension of hybrid threats.

The above results from several changes that occurred and are still occurring within the security system of the Slovak Republic. Security as an essential feature of the existence of any state or community deserves direct and adequate attention because if we ignore building and sustaining it, presence in a society without security becomes impossible. During the processing of the study, our focus was on identifying four pillars that must be understood in connection with the concept of hybrid threats, with a specific focus on the Police Force and members of the Police Force. In the framework of the above-stated, emphasis of this study is also put on the definitions and conceptualisation of hybrid threats, which subsequently led to the identification of key attributes appropriate for the framework of the researched knowledge.

Knowledge of the concept of hybrid threats – dangers that are occurring more and more often in the perception of security not only in Slovakia but also in the global environment – needs to be studied scientifically to find the individual parallels it brings with it and to process them both on a theoretical and a practical level. It is essential that the results of the conducted research are presented at scholarly forums and thus support discussions linked with the effective building and maintaining of security in Slovakia, including thorough knowledge of hybrid threats by members of the Police Force. Suppose we want to investigate the effectiveness of any law or system. In that case, we must define the essential conditions (presuppositions) that allow us to consider whether investigating the system's effectiveness makes any sense. The first condition is the existence of minimally one system (Čentéš, Vojtuš 2020). In our case, this is precisely the security system and the securing of a state where the individual, institution or community will not feel threatened.

The police force is a critical element that plays a significant role in ensuring the state's security. “The Police Force is an armed security force that fulfils tasks in matters of internal order, security, the fight against crime, including its organised and international forms, and the tasks that arise for the Police Force from the international obligations of the Slovak Republic” (§ 1, par. 1 of Act No. 173/1993 Coll. on the Police Force, as amended). For these reasons, knowledge is explicitly focused on the perception of this problem by members of the Police Force themselves, i.e. students of the Police Academy in Bratislava and experts from applied practice.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

Suppose the concept of hybrid threats is known to the direct actors of security and law. In that case, there is an explicit assumption that security development will also be supported. It is also important to realise that the dangers present today and threaten the security of states need to be approached with scientific and practical knowledge. Every emerging problem, in theory, needs to be approached scientifically and practically because this is an effective means for ensuring the relevant core contexts that affect building a secure state. International cooperation made on a broad spectrum is essential. Still, the joint coordinated fight against these threats must be based on precise knowledge and understanding of hybrid threats and their danger. International cooperation must be based on explicit knowledge of hybrid threats and their dangers.

2. Theoretical background

Given the global effect of hybrid threats, coordinated international cooperation is necessary. The focus should, in particular, be on information exchange, cooperation and organising joint exercises with other countries to strengthen skills for a collective response to hybrid threats (Glänzel and Thijs 2017; Drelich-Skulska and Domiter 2020; Wadjdi, Tambayong, and Sianturi, 2023).

Hybrid threats are not new concepts; they are not even exclusive to the 21st century. The renowned Chinese general Sun Tzu referred to the strategy of using indirect warfare, deception and false information as early as the 6th century BC in his work *The Art of War*, where he stated that the best war is the one that never begins).

Given the ambiguity and lack of consensus in interpreting the essence of hybrid threats and their concept, it is crucial to interpret the primary attributes of hybrid threats and their related contexts clearly and unequivocally. In common understanding, a hybrid threat is perceived as a characteristic of a particular idea or situation that is unclear or has multiple meanings (Mumford and Carlucci 2023). Securing and defending a state against hybrid attacks is too complex to be divided into strict categories, so it is necessary to develop knowledge about the interoperability of law enforcement agencies in the context of hybrid threats (Birkemo 2013). This is due to the significant role that security forces play in building resilience against hybrid threats (Mattingsdal, Espevik, Johnsen and Hystad 2023).

The author summarises the achievements of the international conference titled “Interagency and International Cooperation in Countering Hybrid Threats” (Yanakiev 2019). The articles in this volume cover a broad range of issues related to NATO, the EU and national experiences in research and practical activities for countering hybrid warfare. The author presents an expert assessment of the institutional need for capabilities to combat hybrid threats and possible ways to contribute to their integration between different agencies.

In the context of the need for implementing systemic measures at the state level, it is crucial to focus on the area of public administration, which is purposefully understood in the broadest sense as the “process of transforming public policies into outcomes” (Kettl 2018). According to Giannopoulos et al. (2018), public administration exists to implement laws and rules. While this concept is theoretically clear, it can be challenging to apply it in practice. First, when interpreting the law to put it into practice, administrators may unintentionally make value judgments that can have a political character. Second, public administration naturally contributes to policymaking by evaluating and formulating new policies. Based on the conceptual framework of Giannopoulos et al. (2018), the tools of state and non-state actors in hybrid threats for influencing, destabilising and disrupting the performance of public administration include foreign direct investment, support for social unrest, manipulation of the migration discourse, exploitation of weaknesses in public administration, promotion of corruption, exploitation of legal thresholds, exploitation of blind spots in the law, ambiguities, gaps and the creation of confusion. In terms of activities, this involves influencing, destabilising and disrupting the performance of public administration (Korauš, Kurilovská and Šišulák 2022).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

The dataset is from the meta-analysis carried out in the article "Responses to digital disinformation as part of hybrid threats: a systematic review on the effects of disinformation and the effectiveness of fact-checking/debunking using the EU-HYBNET Meta-Analysis Survey Instrument for Evaluating the Effects of Disinformation and the Effectiveness of counter-responses" (Arcos and Smith 2021). The above also has its justification, associated with the unknown or little-known phenomenon of hybrid threats. Although hybrid threats have been a part of communities since ancient history, their global perception has become evident only recently. Newness, however, is not what determines the necessity of a scientific concept.

Relevant proof of the importance of coordinating the operational work of law enforcement agencies within the European Union as well as in third countries is the European Multidisciplinary Platform Against Criminal Threats (EMPACT), which brings together specialists – law enforcement agencies, courts, European Union agencies and others – who together build safe countries and a safe Europe (Bazarkina 2022). It is crucial to be aware that all dangerous types of criminality have exceptionally strong defence mechanisms, which, on the one hand, make it difficult to detect illegal criminal activity and, on the other hand, means law enforcement agencies and courts are faced with a need for evidence, which they must subsequently overcome when proving criminal activity (Szabová and Vrtíková 2022).

Security, which is provided on a daily level by members of the Police Force, is a key article that needs to be assessed, taking into account academic research and professional discussion. Scholarly publications that treat the building and maintenance of security should generalise essential facts and emphasise the specifics that need to be examined and evaluated.

Hybrid threats are undoubtedly a phenomenon that affects and endangers security. Professional publications focused on this issue specify, assess and clearly define their specific elements or their associated contexts. Therefore, we consider reflecting on our study's data as justified, too.

In the context of hybrid warfare, the vital question of the adequacy of the response to its challenges looms ahead. Ukraine, as well as the countries of the EU and NATO are facing new threats that demand that democracies change their activities to find new forms and methods of ensuring national security. Hybrid warfare as an undeclared war takes place with the integrated use of military and non-military instruments, which principally changes the nature of war (Bratko, Zaharchuk and Zolka 2021).

From the above, it is evident that when learning the essence of the risks arising from hybrid threats, the police and security authorities should welcome the opinions of citizens and society regarding the risks – their origin and existence – encoded in these activities. Experts from the practical environment, particularly police and security authorities, reveal, investigate and evaluate how these activities are assessed and their competencies and responsibilities for predicting or controlling these subjects. They also predict what kind of negative consequences will result from carrying out hybrid threats and what results and effects will appear. They further determine whether it is possible to implement hybrid threats when carrying out countermeasures, and if so, then what kind, when and where – especially for conducting police and security activities (Buzalka 2012). A summary of the issue of hybrid threats is also provided by research, in which the goal was to identify the main components of the EU's approach in combatting hybrid threats. The author concludes that the "open architecture" of the theory of hybrid threats enables vast possibilities for interpreting hybrid threats and thus improving practical measures and theoretical approaches to security problems that arise in a society (Bazarkina 2021).

We also point out that it is essential to reflect on the study of hybrid threats from several points of view. We have chosen to respond to security and its provision, but the economic, sociological or political points of view are also essential. Hybrid threats are often studied extensively in the literature dealing with international relations. However, given the authors' other aims in studying the issue of hybrid threats and their professional focus, we can also mention research on the changing paradigm of security from the economic point of view (Balcaen, Du Bois

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)
and Buts 2022). The pioneer in this area was Pieter Balcaen, who focused on this field and laid the foundations for its further development.

3. Research Methodology

Our research aimed to look at the essence and importance of knowledge of the four pillars, which need to be understood in connection with the concept of hybrid threats in general, but also in a specific focus on active members of the Police Force and experts from applied practice – from the workplace for hybrid threats and disinformation. This workplace fulfils the intention of the EU and the government of the Slovak Republic to systematically monitor, evaluate, analyse and react to operations aimed at spreading potentially harmful information. These aims were set with a view to precise research and reflecting on emerging questions in theory.

The research methodology we conducted focused on a specific sequence aimed at knowledge of specific contexts. When carrying out the research, the primary specifics needed to be addressed in the framework of further research were determined through scholarly methods, analysis, synthesis, deduction, observation, comparison and generalisation. The determined research questions were the most important element when investigating the selected issue. At the same time, these research questions helped in a purposeful and comprehensive perception of the concept of hybrid threats and their perception in building and ensuring the security of the Slovak Republic. We will answer the specific research questions subsequently and adapt the structure of our article accordingly. The research questions devised based on theoretical knowledge and knowledge from applied practice were as follows:

1. *"Why is it important that security, but also threats to it, be perceived in connection with the development of current threats?*
2. *How do "first contact" police officers, Police investigators, students of the Police Academy in Bratislava – future members of the police – and experts from applied practice – perceive the essence of hybrid threats?*
3. *What basic pillars forming the concept of hybrid threats are important for understanding hybrid threats?*
4. *How is it possible to effectively build the awareness of students of the Police Academy in Bratislava – future members of the Police Force – regarding the issue of hybrid threats? Is it necessary to ensure international cooperation in building purposeful education within the security forces following the danger of hybrid threats?*

The first research question contains two logical and content-related questions for a better overview and acceptance of logical connections. When identifying the key questions and deficiencies detected by applied practice, we further directed our research towards a specific study of the theoretical but also primarily practical nature of defining the fundamental pillars of hybrid threats and the importance of their knowledge Police Force by members. Subsequently, through analysis, synthesis, a study of the professional literature and investigation of the theoretical nature of hybrid threats, specific associations related to the four basic pillars of hybrid threats need to be identified when defining the concept of hybrid threats and are essential for understanding hybrid threats and their purpose, were defined. Based on the research results, measures will be proposed on both the theoretical and practical levels to avoid the negative impact of hybrid threats on society and to create possibilities for preventing hybrid threats.

As part of the research, from May to July 2023, guided interviews were conducted using pre-formulated questions based on the research questions and the essence, or four pillars, of the concept of hybrid threats among:

- active members of the Police Force – 50 "first contact" police officers with more than 3 years of experience who are in contact with citizens daily,
- 48 Police Force investigators of the general crime department with more than 4 years of experience,

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

- 120 students of the Police Academy in Bratislava, who are clearly expected to be active members of the Police Force after graduation and
- experts from applied practice from the National Security Office, who fulfil tasks related to the identification of hybrid threats and have been in their position for more than 3 years. These experts supplemented our scholarly knowledge and the findings from controlled interviews with members and future members of the Police Force with relevant facts.

The mentioned sample of respondents was selected to find relevant facts about the knowledge and perception of the issue of hybrid threats by active as well as future members of the Police Force, who will share to an increased extent in maintaining and building the country's security. Guided interviews were also conducted based on previous experiences to determine the most important findings that will help when conducting further research.

These principle relevant facts also helped lecturers prepare and construct topics in the scope of lifelong education for members of the Police Force and public administration employees, which is also currently running as part of the national project "Increasing Slovakia's resilience to hybrid threats by strengthening public administration capacities", whose main aim is to increase Slovakia's resistance to the effects of hybrid threats by introducing a complex set of measures, including optimising processes in public administration entities, adjusting the regulatory framework, increasing capacities and acquiring new competencies and skills by organs of public administration. The project is being implemented by the Ministry of the Interior of the Slovak Republic in cooperation with four partners: the Police Academy in Bratislava, the Ministry of Defence of the Slovak Republic, the Ministry of Foreign Affairs and European Affairs of the Slovak Republic and the Office of the Government of the Slovak Republic.

When processing the presented study, we also accepted the fact that the analysis of hybrid threats, the pillars important for understanding hybrid threats, the building and maintaining the security of the Slovak Republic, including knowledge of the concept of hybrid threats within the Police Force, requires an interdisciplinary approach, which means creating a logical link between the strategy being built and the selected tactics being used.

3. Results and discussion

After assessing the acquired knowledge, the perception of the meaning and essence of hybrid threats is important for the country's development and, of course, for the perception of its security. Hybrid threats are often perceived as a modern danger threatening individual countries' safety and security. Still, it must be pointed out that hybrid threats were also present in the distant past, though insufficient attention was paid to them. With the ever more frequent endangering of the security of individual countries, including through hybrid threats, awareness of their constructs and importance have begun being asserted among the broad professional and lay public.

It is important that hybrid threats are gradually beginning to be presented at scientific forums, and through various studies and scientific projects, its essential facts, which affect the security environment not only in specific countries but also from the global security point of view, are being determined. This is also perceived in applied practice, as was determined during the guided interviews. The security environment worldwide has undergone several principle changes in recent years, resulting in a change in already known conventional threats, which have acquired an entirely new dimension and increased intensity due to the development of technology. It is important to emphasise the need at all times and under all circumstances to anticipate security breaches, including attacks that threaten at the national and transnational levels.

Why is it essential that security and its threats are perceived in connection with the development of current threats? How do "first contact" police officers, police investigators, students of the Police Academy in

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

Bratislava – future members of the police and experts from applied practice – perceive the essence of hybrid threats?

As mentioned, the international security environment is dynamically changing and developing, and the development and progression of hybrid threats are also directly related to this fact. "Security" has been mentioned several times, but no definition has been provided. Security, as such, has yet to be clearly defined. There are several definitions of the term and its content; however, it is possible to say that security is an exceptionally complex and multidimensional phenomenon containing many areas and dimensions. Among them are international and national security. In general, however, it is a state when the given actor – an individual or a state – does not feel danger or imminent threat. Different countries understand the concept of security differently, which was also one of the outputs of the guided interviews. For this reason, the perceptions of the hybrid threats themselves also differ. This fact also prompted us to devote ourselves to the basic pillars of hybrid threats during the research.

Security is an important part of every society, and its specific perception is only possible if we also know the individual dangers that can disrupt its construct. The best guarantee of security, peace, development and stability are states respecting democratic values and human rights, which function predictably in an international framework based on rules. Observing the principles and standards of international law and rules of conduct provides basic protection, particularly for smaller states (Conception of the Security System 2023).

The perception of security on the part of our respondents differed within the framework of specific opinions. Still, in the overall overview, all the respondents – 100% – understand what security is. The next question we asked aimed at determining the perception of current threats that can negatively affect security. We asked respondents directly about their perception of hybrid threats in terms of their professional and future professional classification, and 40% of them – 30% students and 10% members of the "first contact" Police Force – said they had never encountered this term. This confirmed for us the need to address the issue of hybrid threats.

One of the essential forms that effectively support responsibility and consistency when applying elements that ensure awareness of the existence of and fight against hybrid threats is education in the form of training and courses, but also the inclusion of this topic in university curricula in specialised subjects. Education and awareness of the possibilities of threats are one way to prevent them or minimise their impact.

Awareness, cooperation of competent subjects on a multidisciplinary level and continuous progress in preventing threats at the national or international level are key, as confirmed by experts from practice. An element for increasing Slovakia's resistance to hybrid threats is also to increase the level of security awareness of the public and public authorities about the risks associated with hybrid threats. It is essential that the academic community, including the researchers themselves, address this issue with a clear element of thoroughness and importance.

The first research question we formulated confirmed that it is necessary to find key answers for the subsequent interpretation and knowledge of hybrid threats in society. During the guided interviews, we also came to believe that members of the Police Force and future members of the Police Force need to acquire such predispositions, based on the results of quality research and practical experience, that will help them secure their tasks in the most adequate conditions possible. A total of 90% of active Police Force respondents welcomed that someone is interested in whether they are aware of hybrid threats and that they can discuss with someone the effectiveness of building security in the context of the possible occurrence of hybrid threats in our country. However, historical contexts also need to be taken into account, as do the current state of the law, knowledge of theory and the need for applied practice and national and international legal aspects, while also considering the need for a high guarantee of the protection of fundamental rights and freedoms (Čentéš and Šanta 2018).

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

What basic pillars forming the concept of hybrid threats are important for understanding hybrid threats?

The next question we asked respondents related to the basic pillars that, in our view, need to be understood in connection with hybrid threats. With this question, only 5% of the respondents, specifically the investigators, could name the four basic pillars of hybrid threats. This indicates that this issue needs to be discovered, and knowledge regarding hybrid threats needs to be deepened. We then consider it justified, also in connection with the above, to define these four pillars of hybrid threats: actors, tools, domains and phases. For an illustrative example and a more precise understanding, we present these four pillars graphically in Figure 1.

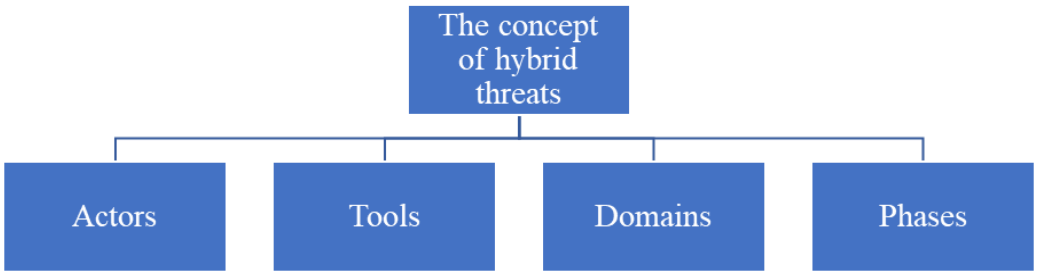

Figure 1. The concept of hybrid threats.

Source: Authors' processing according to the available scientific literature.

Actors of hybrid threats

For our study, we differentiated the actors of hybrid threats, i.e., direct initiators, into state and non-state actors. These hybrid threat actors use different tools to achieve strategic aims. We consider it essential to point out that to achieve their goals, actors use various tools aimed at one or more important domains, but also at the sensitive interface of these domains, and they thus become significantly more dangerous for the defence strategy of individual states (Chambers 2016). They endeavour to achieve the target either by direct or gradually using various forms of fraud and through communication interactions (Arcos, Gertrudix, Arribas and Cardarilli 2021). As an example, we note that sanctions are, above all a financial tool that can be considered an alternative to military tools. Still, they also have an important diplomatic and, with all probability, economic impact for both parties. On the other hand, a well-conducted intelligence operation can reduce the enemy's military capabilities without affecting a diplomatic solution. In most attacks, it is possible to recognise the primary dimension, but sometimes it is intentionally hidden and thus remains unknown (Filipec 2022).

One of the several common features characterising the actors of hybrid threats is that all such actors make a maximum effort to attack the rules of legal principles, that is, the basic values of democracy. Legal principles are the basis of criminal law and general law (Kurilovská 2013). During the last decade, "strong and ambitious authoritarian regimes that systematically suppress political pluralism and the free sustainability of power have increasingly applied the same international principles" (Walker and Ludwig 2017).

It is evident from the above-stated that achieving goals is not only about competition or the defeat of competing states but also includes non-state actors whose practices are not aimed at the military acquisition of territory but at gaining control over the population. Globalisation and digital networks enable actors of hybrid threats to the free flow of information between every individual with Internet access and have brought incredible opportunities and challenges. Thus, under hybrid threats, we also often find a presentation of a creative method of connecting new and old tools, which becomes an important tactical instrument of action for those who lack the skills or opportunities to assert their strategic interests otherwise. This type of power can also be labelled the power of the

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)
weak. If a more fragile actor can purposefully combine the attack tools he has available, he can attack even the strongest opponent (Van Raemdonck and Meyer 2022)

Such a combination of attack tools helps the actor achieve his strategic aim without being detected, without resistance, and without reacting to the attack. At the same time, using the power of hybrid threats permits the actor to minimise the risk of open conflict. Therefore, hybrid threat actors are often inclined to influence the decision-making process itself, the decision-making centre, within their target. We can speak, for example, of business operations, decisions of individuals during elections, decisions of those who practice and shape policies and legislation, who perform activities in the public interest, in the state interest, etc. An actor's activities can be successful even if he uses only some elements of hybrid threats; therefore, it is undoubtedly necessary to investigate and monitor the initial stages of the influence of hybrid threats through their actors.

In connection with hybrid threat actors, during the guided interviews, we reflected on the need to define the actors themselves, as well as their specific activities, because exactly half of the respondents, i.e. 50%, were able to state that hybrid threat actors can be divided into state and non-state actors, though only twenty respondents could define their specific activities.

Instruments of hybrid threats

When conducting conflicts, tools from the whole spectrum of methods known under the acronym DIMEFIL – the basic tools of DIME [Diplomacy, Information, Military and Economics] in the environment of FIL [Financial, Intelligence and Law enforcement] – are applied.

- D – diplomacy/politics – applying influence and exerting pressure verbally and by acts of official political representation;
- I – information – media, social networks and other means of disseminating information, their manipulative use, disinformation campaign and propaganda;
- M – military force – this may be an open threat, a demonstration of military presence and alertness, direct combat use or various forms of covert deployment of individuals, small groups and infiltration of the attacked state using them;
- E – economy – various forms of economic pressure – the imposing of customs duty, an embargo, the denial of supplies of raw materials or energy, a ban on the use of transport or a transport route, destabilisation of crucial industries, businesses, etc.,
- F – finance – destabilisation of a currency, stocks and bonds markets, the 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 attacked country using ethnic, religious or social dividing lines in a society, or using a wide range of terrorist attacks and other typically criminal methods, for example, kidnapping, blackmail and intimidation (Filipec 2022).

The essential fact is that these tools are interconnected to achieve the most effective impact. If the actors use several tools effectively, it becomes necessary to react adequately to the given situation and to be able to predict their subsequent course of action. It therefore follows from the professional literature that hybrid threats are carried by actors in different environments (Sanz-Caballero 2023). The essence of the individual tools was discussed within the guided interviews with the respondents, who emphasised the importance of knowing these tools in their current and future use.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

It was confirmed that the research sample was selected appropriately because the confrontation of suggestions from future and current Police Force members predicted facts that still need to be resolved within the research. This is also evidence that identifying risk and danger in relation to a specific hybrid threat shows the concrete details and consequences of the hybrid threat, which may have an additional negative nature. According to certain indications, the carrying out hybrid threats by the identity of risks can usually be predicted (Hullová 2020). It can be stated that the action of hybrid threats is conditioned by the intention of the addressee to assess risks because carrying out hybrid threats is an intentional activity; that is, it is not an accident that occurs without a cause.

Domains of hybrid threats

Domains comprise another important pillar for understanding hybrid threats. For illustrative purposes, allow us to display hybrid threat domains through Figure 2.

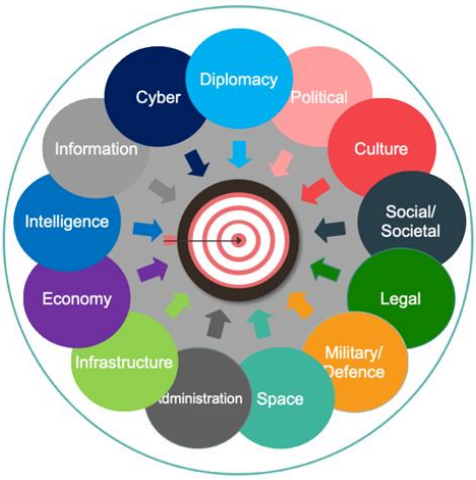

Figure 2. Domains of hybrid threats.

Source: Schmid (2019).

Hybrid threat domains are key areas of the state targeted by individual tools of hybrid threats. Constructive and conceptual knowledge of these domains is important while also recognising the essence of the tool's impact on a specific domain and the possibility of affecting the functioning of the state after an attack. Accepting the suggestions of experts who will consider the need for a clear definition of essential domains that hybrid threats can endanger is justified. Only if such domains are known will it be possible to secure them and thus maintain the security of all objects.

Not every tool and activity directed at a specific domain is a hybrid threat; however, not all activities within the domain are important, even for a hybrid threat actor. For our study, we chose the domain of law within specific domains for a more specific definition. We chose this domain intending to highlight clear elements that may be at risk from hybrid threats in the context of the law.

In the current understanding of what constitutes the legal domain, it can be stated that this is a collection of legal regulations, actions, processes and institutions, including their normative and physical manifestations, which are or can be used to achieve legal or extra-legal effects in the context of the hybrid threat campaign. Within the legal domain, the hybrid threat actor has the opportunity to choose from a wide range of legal provisions to support the campaign against hybrid threats, including the use of legal boundaries and loopholes, which, of course, facilitate

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

his activity and provide him with space and opportunity for use, but also the misuse of national law of the relevant country to obtain its benefit and success (Savolainen et al. 2019).

The action of hybrid threat actors in the legal domain causes conflicts, which subsequently appear in society. These conflicts disrupt the state's proper functioning and affect individuals, institutions, and the legal authorities responsible for maintaining and protecting security. Such conflicts also have an interpersonal nature and can lead to a severe disruption of social relations, which currently fall under the legal category of criminal offences (Šišulák 2020). These existed in the distant past, too. Still, for a society, regardless of the period it is found in, binding rules of behaviour that are not violated and that no one tries to attack or abuse for their benefit – creating disinformation and the like – were and still are necessary for its functioning. Thus, attacking the legal domain is a suitable method for an actor to attack yet another domain because the use of legal possibilities makes it easier to access the social or cultural domain.

We note that it is important to know the following facts for the theoretical and applied dimensions of presenting our research results. The legal field can also be differentiated into national and international law, and it is thus important to state that these areas of law can be used very inappropriately for political purposes. Compared with other domains, the legal domain mainly depends on the actor's perception of the aim. We emphasise that legislation – the law – is a significantly intensive tool because it can convey a moral basis, which can then be used for other negative, harmful activities (Sweijs, Zilincik, Bekkers and Meessen 2021).

The legal domains were discussed in more detail with respondents during the guided interviews. The influence of hybrid threats on the legal domain fundamentally affects them and their views, whether the topics are headed towards the fact that the legal level in the Slovak Republic needs to deal with specific boundaries, which can be a suitable space for the actors of hybrid threats. They also pointed to specifics that may influence the state's security – hoaxes, slippery slope arguments, doxing – but at the same time, they, as members of the Police Force, are restricted and cannot act without violating another legal provision. In support of their opinions, we state that it is also necessary to direct the adjustment of the legal framework in our country so that we can effectively prevent and expediently eliminate the impact of hybrid threats on the legal domain in the Slovak Republic.

Phases of hybrid threats

The last pillar we will focus on is the individual phases of hybrid threats, and we will also do so through an illustrative example, Figure 3.

Figure 3: The concept of hybrid threats.

Source: Cullen et al. (2021).

In the preparation phase, the final goal of a hybrid threat actor is to have his target voluntarily make damaging decisions and take incorrect actions. Suppose the actor comes to the stage where there will be a escalation plan

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)
towards a military conflict. In that case, the actor will attempt to infiltrate the given state's internal environment, including by strategic manipulation. In this phase, the patience of the actor is important (Cullen 2021). The essence of this first phase is that the actor prepares and creates a suitable environment for his subsequent successful action. The actor's activities in this phase are challenging to detect because his intentions could be more explicit. The primary aim of these activities is to compel the state, i.e. the target of hybrid action, to start making negative, even damaging decisions in line with the actor's interests. The activity in the preparatory phase can be characterised as actions aimed at facilitating change in the organisation or a specific environment (Oyserman and Lee 2008).

Based on discussions with experts from practice, we can state that revealing the actor's activity during this phase is vital; therefore, we must find effective tools to help us do this. If such an actor is revealed during this preparatory phase, it can be anticipated that his activity will be minimised afterwards. An effective tool, for example, is the targeted protection of the safety of individuals, companies, organisations and all elements that may be an actor's target and, thus, hybrid threats. Based on the above, the task is to systematically monitor, assess, analyse and respond to activities that have the potential to polarise society, introduce uncertainty and thus undermine the legitimacy, credibility and ability of state institutions to act as well as the democratic constitutional order, ultimately hurting the security interests of the Slovak Republic.

The destabilisation phase is when the actor intensifies his activity, for example, in a campaign – carrying out several operations. In this phase, the actor aims to obtain the most information possible to threaten his target as effectively as possible. The actor's activity here is increasingly apparent, but the actor does not admit to this agility. A problem that practice also identifies lies in the fact that the target state being threatened by the actor does not have sufficient evidence to prove the action of the hybrid threat actor reliably. During this phase, it is difficult to detect when the actor changes the mode of his activity (Schmid 2017).

Aside from those mentioned above, the destabilisation phase uses various grey zones between traditionally considered separate areas, but in today's security environment, they are, in fact, closely connected and intertwined. This is, for example, the boundary between external and internal security, the perception regarding friend and enemy, the interface relating to legislation, the virtual and the real world and the understanding of peace and war. It then follows that this phase affects several domains – legal, military, social, political, economic, cyber and public administration. The basic difference between the preparatory and the destabilisation phases is mainly in connection with the response to the actor's activity in a specific domain.

Experts pointed out to us the fact that during this phase, a systematic response to an actor's activity is inappropriate because the actor is acting with the aim of long-term strategic interest. Therefore, it is necessary to ensure through gradual, purposeful action the constructive elimination of the actor's influence on the boundaries of individual domains and their vulnerable components because if the actor does not reach the desired state, his activity either returns to the preparatory phase or initiates the escalation of his activity. This depends on importance, the strategic objective, the response, and other opportunities.

The pressure phase – hybrid war. In this phase, the actor goes beyond the scope of furtiveness with his activities. In this case, the sharp end of the escalation spectrum of hybrid threat activities is already occurring, and the key element is the use of force to achieve one's purpose; thus, the nature and character of the entire conflict turn into war. In this phase, the actor uses a combination of covert and open military operations, which are accompanied by other tools, such as information operations or cyber attacks (Wither 2016).

In this phase, the nature of the actor's activities changes to an act of force through which he forces the enemy to do his will (Clausewitz 1976). Hybrid warfare is specific in combining several hybrid threats; it combines cyber attacks, terrorism and insurgency in a series of assaults using information and communication technologies.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

Hybrid warfare is not a new phenomenon; its presence in modern war operations, such as those in Ukraine and Russia, is a challenge, especially for the security conditions in Europe (Asmoro, Marsetio, and Putro 2022).

The third research question we formulated aimed to clarify the four specific pillars that should be known to understand the concept of hybrid threats. In the previous sections, we summarised theoretical knowledge and knowledge from experts from practice and members of the Police Force, who also offered us suggestions, opinions and justified facts related to actors, domains, tools and phases of hybrid threats. We appreciate that experts from practice provided us with specific deficiencies they perceive in practice and pointed out specifics related to guaranteeing security.

How is it possible to effectively build the awareness of students of the Police Academy in Bratislava – future members of the Police Force – regarding the issue of hybrid threats? Is it necessary to ensure international cooperation in building purposeful education within the security forces following the danger of hybrid threats?

An essential component of the research was also the possibility of effectively building the awareness of students of the Police Academy in Bratislava – future members of the Police Force – about the issue of hybrid threats. The most effective method for building awareness is targeted academic research and then translating its results into pedagogical practice within specific, individual subjects, such as priority, criminal law, investigation, informatics, criminology and security management. Even within the framework of our research, the issue is gradually being transformed into the teaching process, and students are becoming familiar with the specifics associated with the subject.

Our guided interviews revealed that the students value such an initiative and ask about specifics they could also encounter in practice. It can be seen that they are aware of the importance of this issue and realise that to ensure the security of our country, it is necessary to detect all the potential threats at the national and international levels.

In association with the above, the research also aimed to ensure international cooperation in building purposeful education in the security forces concerning the danger of hybrid threats. This substantial part of the research reflected the essential need for international cooperation with universities in other countries so that education reflects both national and global needs in the context of effectively combatting hybrid threats. What is stated is justified by differentiated experiences and possibilities of individual higher education institutions abroad, which allow us to recast specific, verified experiences into our teaching process.

4. Conclusions

From the knowledge we acquired when processing the presented study, we conclude that building and maintaining the security of the Slovak Republic within the Police Force through knowledge of hybrid threats is exceedingly important. Relevant practical information provided by respondents during guided interviews can be seen as part of the research, and a correlation can be found between them on the theoretical and scientific levels. This is an effective prerequisite for limiting the spread of hybrid threats and their associated dangers in our country.

From the point of view of the main goal – identifying the four pillars that must be understood in connection with the concept of hybrid threats and a specific focus on the Police Force or members of the Police Force and experts from practice, from the National Security Office – the main goal was fulfilled on the scientific, professional and practical sides through research questions that were discussed with four categories of respondents. Partial reactions are contained in the text of this paper and in chapter 4 – Research results and topics for discussion.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

In the case of building an effective approach among members of the Police Force and public administration employees concerning the perception of possible threats and hybrid threats, it can also be assumed that building and maintaining security in the Slovak Republic will be at a significantly higher level. Relevant objects – members of the Police Force and public administration employees – will perceive the risks of hybrid threats and work with information that will be verified, which is a vital basis for identifying the phenomenon of hybrid threats.

In the given context, we want to highlight with these findings the importance of the methodology for realising the knowledge of risks from hybrid threats (Hullová and Fidler 2022). In a broader sense of the word, knowledge methodologies are schemes of approaches and programmes verified by practice and theory in achieving a set goal. In the narrower sense of the term, we label respecting the delegated competencies in the purposeful design of procedures that lay the foundations for its effective and efficient implementation as the *methodology of criminal-police knowledge* (Lisoň and Vaško 2018).

The knowledge presented herein contributes to the research and development of building security and the elimination of hybrid threats at the national and international levels because hybrid expansion in the information space is also spreading, and there is no reason to believe that hybrid threats are decreasing or disappearing (Tkachuk et al. 2021). Hybrid aggression is part of our society and endangers the security of democracies.

Carrying out the research and the national project, in the framework of which this study is presented, will significantly improve the preparedness of public administration authorities and members of the Police Force at the central and regional levels to detect, analyse and implement targeted measures against hybrid threats (Korauš, Kurilovská and Šišulák 2022). Building up human resources and technical capacities and implementing educational and communication activities will significantly increase our country's resilience to various forms of hybrid threats in the relevant domains. A targeted audit of vulnerability and subsequent proposals to amend and supplement regulatory frameworks will fill in system weaknesses against hybrid activity and support the fight against hybrid threats.

Our *de lege ferenda* suggestions based on the knowledge we acquired when conducting this research are with certainty the following: Creating a methodology for Police Force members that would help them identify the risks of hybrid threats; a change in legislation that would make it possible to punish selected manifestations of hybrid threats; a more effective system of information on the phenomenon of hybrid threats; and the expansion of research opportunities in this area.

The ambition of the presented study is to contribute to the scholarly debate, which is of great importance within the given issue and requires precision and clarity of all attributes related to it. Empirical research has demonstrated the need for continuous comprehensive knowledge of the risks of hybrid threats. In connection with the issue of hybrid threats, it is essential to emphasise the need for a constant flow of transformations in the development dynamics of this specific phenomenon. The transfer of knowledge in the mentioned system needs to take place such that one output in the form of knowledge is at the same time input to another, leading to new knowledge. The emergence, quantitative and qualitative change of the information nature of the risks of hybrid threats – their origin, growth, partial paralysis, and complete deactivation – form a solid chain in the environment and time (Hullová and Fidler 2022). These facts must be accepted by all interested parties, including members of the Police Force, who, in line with the competencies delegated by the law, take part in identifying hybrid threats and their danger, but, of course, also in reducing their occurrence.

References

Act No. 173/1993 Coll. on the Police Force, as amended. https://www.epi.sk/zz/1993-171

Arcos, R., Gertrudix, M., Arribas, C., & Cardarilli, M. (2021). Dataset. Responses to digital disinformation as part of hybrid threats: an evidence-based analysis on the effects of disinformation and the effectiveness of fact-checking/debunking (Version 1) [Data set]. Zenodo. https://doi.org/10.12688/openreseurope.14088.1

Arcos, R., & Smith, H. (2021). Digital Communication and Hybrid Threats, *Revista Icono 14-Revista Cientifica De Comunicacion Y Tecnologias*, 19(1), 1-14. http://www.doi.org/10.7195/ri14.v19i1.1662

Asmoro, N., Marsetio, S. Z., & Putro, R. W. (2022). Hybrid Threats To Transformation The Doctrine Of Military Campaign Based On Historical Perspective To Achieve Comprehensively National Security. *Journal of Positive School Psychology*, 6(8), 955-968. https://journalppw.com/index.php/jpsp/article/view/9830/6421

Balcaen, P., Du Bois, C., & Buts, C. (2022). A Game-theoretic Analysis of Hybrid Threats. *Defence and Peace Economics*, 33(1), 26-41. http://www.doi.org/10.1080/10242694.2021.1875289

Bazarkina, D. (2021). Evolution of Approaches to Countering Hybrid Threats in the European Union's Strategic Planning. *Contemporary Europe-Sovremennaya Evropa*, 6, 133-143. http://www.doi.org/10.15211/soveurope62021133143

Bazarkina, D. (2022). Countermeasures for Hybrid Threats: The Experience of the European Union and Its Member States. *Her. Russ. Acad. Sci*. 92 (Suppl 4), S315–S320 (2022). https://doi.org/10.1134/S1019331622100033

Birkemo, G.A. (2013). Questioning Norwegian societal security efforts—Police-military cooperation in national crisis management [Research application submitted to NFR]. Forsvarets Forskningsinstitutt (FFI). https://journals.sagepub.com/doi/full/10.1177/0095327X231160711

Bratko, A., Zaharchuk, D., & Zolka, V. (2021). Hybrid warfare – a threat to the national security of the state. *Revista De Estudios En Seguridad Internacional-Res*., 7(1), 147-160. https://doi.org/10.18847/1.13.1

Buzalka, J. (2012). Teória bezpečnostných rizík [The Theory of Security Risks]. Bratislava: Akadémia PZ v Bratislave, 2012. 167 p. [print]. ISBN 978-80-8054-547-5.

Clausewitz, C. (1976). On War (Edited and Translated by Michael Howard, Peter Paret). Princeton: Princeton University Press. [print].

Cullen, P. et al. (2021). The Landscape of Hybrid Threats: A Conceptual Model (Public Version), 58 p. http://www.doi.org/10.2760/44985.

Čentéš, J., & Šanta, J. (2018). Qualitative aspects of Criminal Code of the Slovak Republic and reasons for its amendment. In: Studia Prawnoustrojowe [print]: *Journal of the Faculty of Law and Administration at UWM in Olsztyn*, 41, 79-96. ISSN 1644-0412. https://www.ceeol.com/search/article-detail?id=786268

Čentéš, J., & Vojtuš, F. (2020). Efektívnosť práva a prístupy k jej skúmaniu [The Effectiveness of the Law and Approaches to Its Study]. In Čentéš, J. (ed.) et al.: „Efektívnosť prípravného konania – jej skúmanie, výzvy a perspektívy" [Effectiveness of preliminary proceedings – its investigation, challenges and perspectives], Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020, p. 28-41. ISBN 978-80-7160-577-5. https://www.akademiapz.sk/sites/default/files/OIT/Aktuality/2021/2021-1-12-Zborni__k-z-medzina__rodnej-vedeckej-konferencie-APVV_01.pdf

Drelich-Skulska, B., & Domiter, M. (2020). Security in the Science of International Relations and Economic Security. A Contribution to the Discussion. *Transformations in Business & Economics*, Vol. 19, No 2A (50A), pp.551-564.

Filipec, O. (2022). Multilevel analysis of the 2021 Poland-Belarus Border Crisis in the Contextof Hybrid Threats. *Central European Journal of Politics*, 8(1), 1-18. https://doi.org/10.24132/cejop_2022_1

Glänzel, W., & Thijs, B. (2017). Using hybrid methods and 'core documents' for the representation of clusters and topics: the astronomy dataset. *Scientometrics* 111, 1071-1087. https://doi.org/10.1007/s11192-017-2301-6

Hullová, M. (2020). Východiskové štádium procesov odhaľovania a objasňovania mravnostných trestných činov. [The starting stage of the processes of revealing and clarifying moral crimes] In: Fenomén bezpečnosti, bezpečnostní věda a výzkum a bezpečnostní aplikace : Sborník vědeckých prací Fakulty právních a správních studií Vysoké školy finanční a správní, a.s. Praha [The phenomenon of security, security science and research and security applications: Collection of scientific works of the Faculty of Legal and Administrative Studies of

the University of Finance and Administration, a.s., Prague]. Prague: Vysoká škola finanční a správní, 2018. ISBN 978-80-7408-165-1. s. 391-405. https://www.vsfs.cz/prilohy/konference/sbornik_final_ed.pdf

Hullová, M., & Fidler, Ľ. (2022). Riziká z realizácie hybridných hrozieb [Risks from the realization of hybrid threats]. In Medelský, J., Laca, N. 2022. Dezinformácie a právo (úlohy a postavenie bezpečnostných zložiek). Zborník príspevkov [Disinformation and law (the roles and position of security forces). Collection of contributions]. Bratislava. Akadémia Policajného zboru v Bratislave. s. 43-54. [print]. ISBN 978-80-8054-964-0

Chambers, J. (2016). Countering Gray-zone Hybrid Threats:. Modern War Institute at West Point, 59 p. https://web.archive.org/web/20180410104356id_/https://mwi.usma.edu/wp-content/uploads/2016/10/Countering-Gray-Zone-Hybrid-Threats.pdf
Giannopoulos, G.M., Theocharidou, G., Theodoridis, and Gattinesi, P. (2018). D eveloping Vulnerability and Detection Indicators for Hybrid Threats. JRC Technical Report, JRC109791

Koncepcia bezpečnostného systému Slovenskej republiky [The Conception of the Security System of the Slovak Republic], 2023. https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2022/636

Korauš, A., Kurilovská, L., & Šišulák, S. (2022). Increasing the Competences and Awareness of Public Administration and Police Officers in the Context of Current Hybrid Threats. In RELIK 2022 [elektronický dokument]: conference proceedings / zost. Jitka Langhamrová, zost. Jana Vrabcová. - Prague: Prague University of Economics and Business, 2022, p. 379-388. ISBN 978-80-245-2466-5. https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf.

Kurilovská, L. (2013). Základné zásady trestného konania: Účel a základná limitácia [Basic principles of criminal procedure: Purpose and basic limitations]. Šamorín: HEURÉKA, 141 p. [print]. ISBN 978-80-89122-91-2

Lisoň M., & Vaško, A. (2018). Teória kriminálno-policajného poznania [The Theory of Criminal-Police Knowledge]. Bratislava: Wolters Kluwer, 2018, 389 s. [print]. ISBN 978-80-8168-838-6

Mattingsdal, J., Espevik, R., Johnsen, B. H., & Hystad, S. (2023). Exploring Why Police and Military Commanders Do What They Do: An Empirical Analysis of Decision-Making in Hybrid Warfare. *Armed Forces & Society*, https://doi.org/10.1177/0095327X23116071

Mazaraki, A., Kalyuzhna, N., & Sarkisian, L. (2021). Multiplicative Effects of Hybrid Threats. *Baltic Journal Economic Studies*, 7(4). 136-144. https://doi.org/10.30525/2256-0742/2021-7-4-136-144

Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, 8(2), 192-206. https://doi.org/10.1017/eis.2022.19

Oyserman, D., & Lee, S.W.S. (2008). Does Culture Influence What and How We Think? Effects of Priming Individualism and Collectivism. *Psychological Bulletin*, 134(2), 311-42. https://doi.org/10.1037/0033-2909.134.2.311

Sanz-Caballero, S. (2023). The concepts and laws applicable to hybrid threats, with a special focus on Europe. *Humanit Soc Sci Commun* 10, 360, https://doi.org/10.1057/s41599-023-01864-y.

Savolainen, J., Gill, T., Schatz, V., Ojala, L., Jakstas, T., Kleemola-Juntunen, P., Lohela, T. (Ed.), & Schatz, V. (Ed.). (2019). Handbook on maritime hybrid threats: 10 Scenarios and Legal Scans . Hybrid CoE. Hybrid CoE Working papers https://www.hybridcoe.fi/wp-content/uploads/2019/11/NEW_Handbook-on-maritimethreats_RGB.pdf

Schmid, J. (2017). Hybride Kriegführung in Vietnam – Strategie Und Das Center of Gravity Der Entscheidung. *Zeitschrift Für Außen- Und Sicherheitspolitik*, 10(3), 373-90. https://doi.org/10.1007/s12399-017-0659-4.

Schmid, J. (2019). Hybrid warfare – a very short introduction. COI S&D Concept Paper. Helsinki, May 2019, 15 pages. [print]. ISBN: 978-952-7282-20-5.

Szabová, E., & Vrtíková, K. (2022). Efektívnosť prípravného konania v otázkach previazaných s osobou spolupracujúceho obvineného [Effectiveness of preliminary proceedings in matters related to the person of the cooperating accused]. In Čentéš, J., Kurilovská, L. et al. (eds.), 2022. EFEKTÍVNOSŤ PRÍPRAVNÉHO KONANIA – súčasný stav a výzvy pro futuro. Zborník príspevkov z konferencie, Bratislavské právnické fórum 2022 [THE EFFECTIVENESS OF PREPARATORY PROCEDURE – the current state and challenges for the future. Collection of contributions from the conference, Bratislava Legal Forum 2022]. Bratislava: Wolters Kluwer SR, p. 22 – 46. ISBN 978-80-571-0546-6. https://www.flaw.uniba.sk/fileadmin/praf/Veda/Zborniky/Zbornik_prispevkov_Efektivnost_pripravneho_konania_KTPKK.pdf#page=22.

Sweijs, T., Zilincik, S., Bekkers, F., & Meessen, R. (2021). A framework for cross-domain strategies against hybrid threats. Hague Centre for Strategic Studies. HCSS Security, 53 p. https://euhybnet.eu/wp-content/uploads/2021/06/Framework-for-Cross-Domain-Strategies-against-Hybrid-Threats.pdf.

Šišulák, S. (2020). Kritéria efektívnosti prípravného konania [Criteria for effectiveness of preliminary proceedings]. In ČENTÉŠ, J. (ed.) et al.: „Efektívnosť prípravného konania – jej skúmanie, výzvy a perspektívy" [Effectiveness of pretrial proceedings – its investigation, challenges and perspectives], Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta, 2020, p. 127-137. ISBN 978-80-7160-577-5. https://www.akademiapz.sk/sites/default/files/OIT/Aktuality/2021/2021-1-12-Zborni__k-z-medzina__rodnej-vedeckej-konferencie-APVV_01.pdf.

Tkachuk, I. V., Shynkarenko, R. S., Tokovenko, O. S., Svorak, S. D., & Lavoryk, A. V. (2021). Hybrid Threats and the Transformation of the State Political Institute: A Neo-Institutional Approach. *Ad Altajournal of Interdisciplinary Research*, 11(1), 29-33. Special Issue 16. ISSN: 1804-7890. https://www.magnanimitas.cz/ADALTA/110116/papers/A_05.pdf.

Van Raemdonck, N., & Meyer, T. (2022). Why Disinformation is Here to Stay. A Socio-technical Analysis of Disinformation as a Hybrid Threat. In L. Lonardo (Ed.), Addressing Hybrid Threats: European Law and Policies Edward Elgar. https://researchportal.vub.be/en/publications/why-disinformation-is-here-to-stay-a-socio-technical-analysis-of-

Wadjdi, A. F., Tambayong, J., & Sianturi, E. M. (2023). Enhancing national defense capabilities through collaborative programs: insights and policy recommendations for Indonesia. *Insights into Regional Development*, 5(3), 10-23. https://doi.org/10.9770/IRD.2023.5.3(1)

Walker, Ch., & Ludwig, J. (2017). The Meaning of Sharp Power: How Authoritarian States Project Influence. *Foreign Affairs*. http://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power

Wither, J. K. (2016). Making Sense of Hybrid Warfare. *Connections*, 15(2), 73-87. https://doi.org/10.11610/Connections.15.2.06

Yanakiev, Y. (2019). Promoting Interagency and International Cooperation in Countering Hybrid Threats. *Information & Security: An International Journal*. https://doi.org/10.11610/isij.3900

Funding: The contribution was created as a result of the project: Research of educational concepts in the field of hybrid threats within selected EU countries with the subsequent elaboration of the education concept for SR conditions project code in ITMS 2014+: 314011CDW7.

Data Availability Statement: More information and data can be obtained from the authors on a resonable request

Author Contributions: The authors contributed equally, they have read and agreed to the published version of the manuscript. All authors have read and agreed to the published version of the manuscript.

ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2023 Volume 11 Number 1 (September)
http://doi.org/10.9770/jesi.2023.11.1(14)

Prof. Dipl. Eng.. Antonín KORAUŠ, PhD., LL.M., MBA, Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia.
ORCID ID: https://orcid.org/0000-0003-2384-9106.

Assistant Prof. JUDr. Patrícia KRÁSNÍ, PhD., LL.M., Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia.
ORCID ID: https://orcid.org/0000-0003-0079-9652.

Assoc. Prof. Dipl. Eng. Stanislav ŠIŠULÁK, PhD., MBA, Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava, Slovakia.
ORCID ID: https://orcid.org/0000-0003-4727-9582.

Dipl. Eng. Stanislava VESELOVSKÁ, PhD., Pan-European University in Bratislava, Faculty of Economics and Entrepreneurship, Tematinská 10, 851 05 Bratislava, Slovakia.
ORCID ID: https://orcid.org/0009-0005-5616-018X