HYBRID THREATS FROM THE PERSPECTIVE OF STUDENTS AT SELECTED UNIVERSITIES IN SLOVAKIA: RESEARCH ON PERCEPTION OF FREQUENCY

Hybridné hrozby z pohľadu študentov vybraných vysokých škôl na Slovensku: Výskum vnímania frekvencie

Antonín KORAUŠ, Miroslav GOMBÁR

ABSTRAKT

Cieľom tejto štúdie je práve hlbšie porozumieť vnímaniu frekvencie výskytu hybridných hrozieb vysokoškolskými študentmi. V tomto príspevku analyzujeme vnímanie definovaných hybridných hrozieb, medzi ktoré patria: Kybernetická bezpečnosť, Energetická a priemyselná bezpečnosť, Strategická komunikácia, Vplyv cudzích mocností, Organizovaný zločin a strategická korupcia, Extrémizmus a Environmentálna bezpečnosť, ich závažnosti na *Likertovej škále* s 5 úrovňami od 1 – nezávažná po 5 – veľmi závažná. Na základe týchto zistení môžeme vyvodiť relevantné závery a odvodenia, ktoré môžu prispieť k zlepšeniu preventívnych opatrení a edukačných aktivít zameraných na ochranu žiakov pred hybridnými hrozbami.

Kľúčové slová: Hybridné hrozby. Vnímanie. Vysokoškolskí študenti.

ABSTRACT

The aim of this study is precisely to gain a deeper understanding of the perception of the frequency of occurrence of hybrid threats by university students. In this submitted article, we analyze the perception of defined hybrid threats, which include: Cybersecurity, Energy and Industrial Security, Strategic Communication, Influence of Foreign Powers, Organized Crime and Strategic Corruption, Extremism, and Environmental Security, in terms of their severity on a Likert scale with 5 levels from 1 - not severe to 5 - highly severe. Based on these findings, we can draw relevant conclusions and derivations that can contribute to the improvement of preventive measures and educational activities aimed at protecting students from hybrid threats.

Key words: Hybrid threats. Perception. University students.

INTRODUCTION

The ongoing digital era brings with it technological advancement, numerous advantages, but also new security challenges. The increased use of digital technologies deepens dependence on the online environment. These aspects create opportunities for various forms of threats that spread among users. One of these threats is the phenomenon of hybrid threats, which combine physical and cyber elements with the aim of disrupting, damaging, or manipulating target entities.

In the context of the application of hybrid threats, it is crucial to focus on university students who are active users of digital technologies. The connectivity of these technologies to the internet poses a high potential vulnerability of university students to hybrid threats. Therefore, it is necessary to explore the perception of the frequency of occurrence of hybrid threats by university students and their level of awareness of hybrid threats. It's not only about their perception but also whether they consider hybrid threats to be a common occurrence or something rare and exceptional. Additionally, their experiences in this area and how it manifest in their awareness of security and protection are important.

The main goal of the study is to investigate the attitude of students from selected universities towards the perception of the frequency of occurrence of hybrid threats and gain a better understanding of students' opinions and their attitudes towards security in the digital environment. Such insights will help draw relevant conclusions and implications that can contribute to improving educational activities for students focusing on hybrid threats. This study is based on a quantitative survey among the population of university students, providing a broad and representative view of the perception of the frequency of occurrence of hybrid threats by students from selected universities.

Perception of the frequency of occurrence of hybrid threats from the perspective of university students can be influenced by several factors, such as awareness, experience, media communication, security measures, personal risk perception, and more. It's important to realize that the perception of the frequency of occurrence of hybrid threats can vary significantly among university students, taking into account individual factors and experiences.

1 Theoretical background

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 Mihalčová, et al. (2023).

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. This is because 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 & Carlucci (2023). Securing and defending a state against hybrid attacks is too complex to be divided into strict categories, which is why 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 et al. 2023).

Yanakiev (2019) summarises the achievements of the international conference titled “Interagency and International Cooperation in Countering Hybrid Threats.” The articles in this volume cover a broad range of issues related to NATO, EU and national experiences in the research and practical activities in 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 needs for implementing systemic measures at the state level, it is important 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. (2021), 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 policy-making by evaluating existing policies and organizing the formulation of new ones. Based on the conceptual framework of Giannopoulos et al. (2021), the tools of state and non-state actors in hybrid threats for influencing, destabilizing, and disrupting the performance of public administration include foreign direct investment, support for social unrest, manipulation of 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, destabilizing, and disrupting the performance of public administration Korauš et al. (2022).

Dataset 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 et al. (2021).

2 Research objectives, methods, and results

The basic variables describing the division of the research sample (N=652) include the respondent's gender, age, study format, and the type of university they are attending (economic or police). The research was conducted using an author-designed questionnaire from March 2023 to May 2023. The author's questionnaire analyzes various aspects of the current phenomenon of hybrid threats. A more detailed analysis of the research sample is presented in Table 1.

Table 1: Description of the research sample

Summary Table for all Multiple Response Items (Data) Totals/ percentages based on number of respondents					
N=652 Gender	Age R	Study Format S	Type of University Economic	Type of University Police	Row Totals
Male	Less than 25 years old	full-time study	52	72	124
		external study format	8	18	26
	Total		60	90	150
	26 - 35 years old	full-time study	4	4	8
		external study format	12	44	56
	Total		16	48	64
	36 - 45 years old	full-time study	0	0	0
		external study format	0	34	34
	Total		0	34	34
	More than 45 years old	full-time study	0	0	0
		external study format	0	4	4
	Total		0	4	4
Female	Less than 25 years old	full-time study	88	128	216
		external study format	60	16	76
	Total		148	144	292
	26 - 35 years old	full-time study	0	2	2
		external study format	36	22	58
	Total		36	24	60
	36 – 45 years old	full-time study	0	2	2
		external study format	16	14	30
	Total		16	16	32
	More than 45 years old	full-time study	0	0	0
		external study format	12	4	16
	Total		12	4	16

Source: Author's own processing

The second demographic item of the research tool, defined as the respondent's age, has, based on the conducted analysis, a relationship with Cybersecurity (p=0.032), Strategic Communication (p=0.004), and Environmental Security (p=0.007). Another demographic item of the research tool, which is the study format, has a significant relationship with Energy and Industrial Security (p=0.021) and Organized Crime and Strategic Corruption (p=0.001). Finally, the last demographic item of the research tool is associated with Energy and Industrial Security (p=0.019). We will attempt to further analyse these statistically significant relationships mentioned above in the following text.

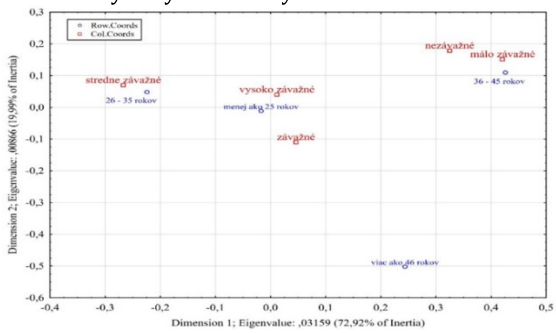
In the first significant relationship mentioned, regarding the severity of Cybersecurity and the respondent's age, we can conclude that 38.462 % of all respondents consider this hybrid threat as serious, and 29.808% consider it highly severe. 22.115 % of the respondents attribute moderate severity to cybersecurity, while only 2.885 % of respondents find it not serious, and 6.731 % consider it slightly serious.

Regarding the age distribution of respondents who perceive cybersecurity as a highly severe hybrid threat, 30.372 % of respondents under the age of 25, 28.282 % of respondents aged 26-35, 31.034 % of respondents aged 36-45, and 21.429 % of respondents older than 45 selected this option. It is noteworthy that the last age group chose to consider it a serious risk up to 64.286 %. The other age groups evaluated cybersecurity as a serious threat fairly evenly: 38.682 % of respondents under 25, 34.343 % of respondents aged 26-35, and 37.931% of respondents aged 36-45.

For those who find Cybersecurity moderately severe, 22.060 % are under 25, 31.313 % are aged 26-35, 10.345 % are aged 36-45, and 7.143 % are older than 45. As for those who consider it slightly serious, 5.731% are under 25, 5.050 % are aged 26-

35, 15.517 % are aged 36-45, and 7.143 % are older than 45. Finally, for those who find it not serious, 3.152 % are under 25, 1.010 % are aged 26-35, 5.172 % are aged 36-45, and none of the respondents are older than 45. We present a correspondence map as a final visualization of the relationship between the perception of the severity of Cybersecurity and the age of the respondent in Figure 1.

Figure 1: Correspondence map of the relationship between the respondent's age and the perception of the severity of cybersecurity

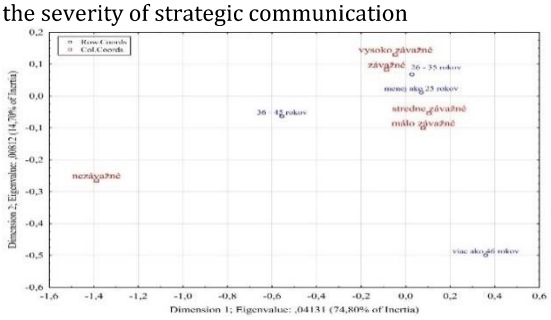


Source: Author's own processing

In summary, the analysis of the relationship between the respondent's age and their perception of the severity of Cybersecurity reveals that respondents under the age of 25 primarily perceive this risk as highly severe and severe, respondents aged 26-35 see this risk as moderately severe, and respondents aged 36-45 perceive it as slightly severe or not severe. As the age of the respondents increases, the perception of the severity of cybersecurity decreases.

The second significant relationship according to Table 2 is the relationship between the respondent's age and the hybrid threat defined as Strategic Communication (p=0.004). In total, 41.538 % of all respondents attribute a moderate level of severity to this hybrid threat, 29.423 % perceive it as severe, and 13.269 % consider it highly severe. On the other hand, 14.038 % consider this hybrid threat slightly severe, and only 1.731 % consider it not severe. The age structure of those who perceive Strategic Communication as moderately severe as a hybrid threat shows that 41.834 % of respondents under the age of 25, 43.434 % of respondents aged between 26-35, 31.034 % of respondents aged 36-45, and 64.286 % of respondents older than 45 have chosen this option. When choosing to perceive the examined hybrid threat as severe, 27.794 % of respondents under 25, 34.343 % of respondents aged between 26-35, 34.483 % of respondents aged 36-45, and 14.286 % of respondents older than 45 chose this option. Strategic Communication was considered highly severe by 14.237 % of respondents under 25, 11.111 % of respondents aged between 26-35, 13.793 % of respondents aged 36-45, and none of the respondents older than 45. We present a correspondence map as a final visualization of the relationship between the perception of the severity of Strategic Communication and the age of the respondent in Figure 2.

Figure 2: Correspondence map of the relationship between the respondent's age and the perception of the severity of strategic communication



Source: Author's own processing

The result of the correspondence analysis reveals that respondents under the age of 25 perceive Strategic Communication as moderately and slightly serious, while respondents aged 26-35 consider this hybrid threat as serious and highly serious. On the other hand, respondents older than 35 do not have a clear opinion about the severity level of this hybrid threat.

The third significant relationship (Table 2) is the relationship between the respondent's age and the perception of the severity of Environmental Security (p=0.007). In total, 4.230 % of respondents labeled this hybrid threat as not serious, 10.385 % as slightly serious, 31.154 % as moderately serious, 30.192 % as serious, and 24.038 % as highly serious. In terms of age structure, for the option of considering Environmental Security as "not serious," 4.585 % of respondents under the age of 25, 1.010 % of respondents aged 26-35, 8.621 % of respondents aged 36-45, and none of the respondents older than 45 chose this option.

It is interesting to note the attitude of respondents older than 45 when defining Environmental Security as slightly serious, with 35.714 % of them choosing this option. A more detailed breakdown of the age structure for each response is provided in Table 2.

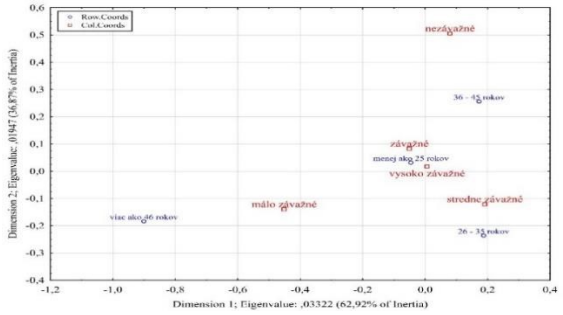
Table 2: Age structure of the perception of the severity level of environmental security as a hybrid threat

Age R	Not serious	Slightly serious	Moderately serious	Serious	Very serious	Total
Less than 25 years old	4,584527	11,17479	32,09169	27,79370	24,35530	100,00
26 - 35 years old	1,010101	8,08081	25,25253	42,42424	23,23232	100,00
36 - 45 years old	8,620690	3,44828	34,48276	29,31034	24,13793	100,00
More than 46 years old	0,000000	35,71429	35,71429	7,14286	21,42857	100,00

Source: Author's own processing

From the graphical representation of the analyzed relationship between the perception of the severity level of Environmental Security in relation to the age of the respondent (Figure 3), respondents under the age of 25 perceive Environmental Security as serious or highly serious. Respondents aged 26-35 prefer the option "moderately serious," respondents aged 36-45 view it as not serious, and finally, respondents older than 45 perceive it as slightly serious.

Figure 3: Correspondence map of the relationship between the respondent's age and the perception of the severity of environmental security

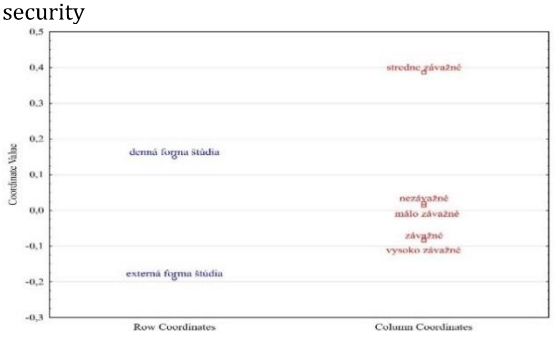


Source: Author's own processing

The fourth significant relationship (Table 2) is the relationship between the respondent's study form and the perception of the severity of Energy and Industrial Security (p=0.005) as a hybrid threat. Overall, respondents perceive energy and industrial security as follows: not serious (2.692 % of respondents), slightly serious (8.462 %), moderately serious (15.577 %), serious (39.231 %), and highly serious (34.038 %).

There is a relatively balanced perception of the lack of seriousness of the analyzed hybrid threat among students in the daytime (2.739 %) and external study forms (2.632%), as well as when defining energy and industrial security as slightly serious risk (8.562 % for daytime students and 8.333% for external students). However, a significant difference between daytime and external students is observed in perceiving energy and industrial security as moderately serious hybrid threats. While 20.890 % of daytime students chose this option, only 8.772 % of external students did. As a serious threat, energy and industrial security is perceived by 36.301 % of daytime students and 42.984 % of external students, and finally, as a highly serious threat, it is perceived by 31.509 % of daytime students and 37.281 % of external students.

Figure 4: Correspondence map of the relationship between the respondent's study form and the perception of the severity of energy and industrial security



Source: Author's own processing

From the results of the correspondence analysis in the form of a correspondence map (Figure 4), it is evident that external study students primarily lean towards the option of being severe and highly severe, while full-time study students lean towards moderately severe. Overall, it can be said that the perception of this threat is critical regardless of the study form, and respondents are aware that reducing energy and industrial security is a very important aspect of endangering the Slovak Republic.

The fifth statistically significant relationship (Table 2) is the relationship

between the respondent's study form and the perception of the severity of Strategic Communication (p=0.021). In summary, Strategic Communication is perceived as not serious by 1.731 % of respondents, slightly serious by 14.038 % of respondents, moderately serious by 29.423 % of respondents, serious by 29.423 % of respondents, and highly serious by 13.269 % of all respondents. Strategic communication is perceived as highly serious by 13.356 % of full-time students and 13.158 % of external students. As a serious threat, 26.027 % of full-time students and 33.772 % of external students perceive the analyzed hybrid threat. Further differences in the perception of the severity of Strategic Communication as a hybrid threat from the perspective of the respondents' study form are listed in Table 3.

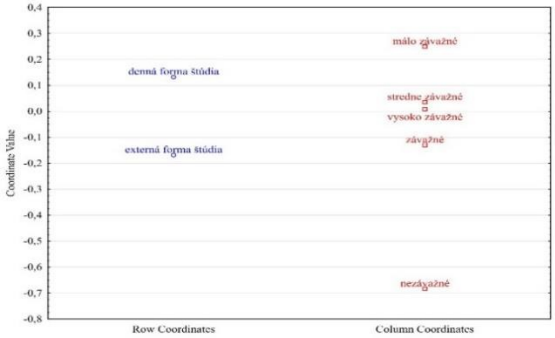
Table 3: Perception of the degree of seriousness of strategic communication as a hybrid threat in relation to the respondent's form of study

Study Format S	Not serious	Slightly serious	Moderately serious	Serious	Very serious	Total
full-time study	0,68493	17,1232	42,80822	26,0274	13,3561	100,0
external study format	3,07017	10,08772	39,91228	33,77193	13,1578	100,0

Source: Author's own processing

From the results of the correspondence analysis in the form of the correspondence map (Figure 5), it is evident that students in external study programs primarily tend to consider Strategic Communication as severe or highly severe, as well as moderately severe. In contrast, full-time students lean more towards perceiving it as slightly severe. Overall, it can be concluded that the perception of this threat is viewed as critical among students in external study programs, with this group of respondents recognizing the significance of Strategic Communication as a vital aspect of the security of the Slovak Republic.

Figure 1 Correspondence map of the relationship between the respondent's form of study and the perception of the importance of strategic communication



Source: Author's own processing

The second-to-last significant relationship (Table 2) is the relationship between the respondent's study program format and the perception of the severity level of Organized Crime and Strategic Corruption as a hybrid threat (p=0.001). Overall, 42.308 % of all respondents perceive Organized Crime and Strategic Corruption as highly severe hybrid threats. 15.385 % perceive them as severe, 32.885 % as moderately severe, 5.385 % as slightly severe, and 4.038 % as non-severe hybrid threats. Further differences in the perception of the severity level of the hybrid threat Organized Crime and Strategic Corruption between respondents in full-time and part-time study programs are detailed in Table 4.

Table 4 Perceptions of the degree of seriousness of organized crime and strategic corruption as a hybrid threat in relation to the respondent's form of study

Study Format	Not serious	Slightly serious	Moderately serious	Serious	Very serious	Total
full-time study	3,082192	6,506849	26,71233	19,17808	44,52055	100,00
external study format	5,263158	3,947368	40,78947	10,52632	39,47368	100,00

Source: Author's own processing

The last analyzed significant relationship according to Table 2 is the relationship between the university where the respondent studies and the perception of the severity level of Energetic and Industrial Security (p=0.019). Overall, 34.039 % of respondents perceive it as highly severe hybrid threats, 39.231 % as severe, 15.577 % as moderately severe, 8.462 % as slightly severe, and 2.692 % as non-severe hybrid threats. More detailed differences in the perception of the severity level of the hybrid threat Energetic and Industrial Security between respondents studying at economic

and police universities are provided in Table 5.

Table 5 Perceptions of the degree of seriousness of energy and industrial security as a hybrid threat in relation to the type of university

Type of University	Not serious	Slightly serious	Moderately serious	Serious	Very serious	Total
economic	2,5641	8,333333	8,97436	48,71795	31,41026	100,00
police	2,74723	8,516484	18,40659	35,16484	35,16484	100,00

Source: Author's own processing

Conclusion

In conclusion, it is necessary to expand the research sample to include other groups of the population in order to gain a more comprehensive overview of the perception of various hybrid threats. It would be interesting to observe differences in terms of the level of education attained, occupation in the private, public, or state sectors, place of residence in terms of the size of the town or city, or self-governing region. The perception of the severity of hybrid threats is a complex issue influenced by many variables. Understanding this problem creates an opportunity to properly target activities aimed at reducing their risk.

An important factor in relation to the security and protection of students in the digital environment is the perception of the frequency of occurrence of hybrid threats by students. In the context of the results presented in the study conducted at selected universities, information was gathered from students regarding their perception of hybrid threats and their impact on their security awareness.

Given the relatively low level of awareness in the examined area, it was found that it is crucial to increase awareness and provide educational programs focused on hybrid threats for university students. Establishing collaboration between higher education institutions, security organizations, and students can help improve awareness of these threats and enhance security in the digital environment.

The perception of the frequency of occurrence of hybrid threats is a dynamic area that changes with technological advancements and new threats. For these reasons, it is necessary to continuously monitor this development and adapt security measures and educational activities to the current situation.

Bibliography

ARCOS, Ruben, GERTRUDIX, Manuel, and Cristina ARRIBAS, et al., 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. [online]. [cit. 2023-07-29]. Available at: https://open-research-europe.ec.europa.eu/articles/2-8

BIRKEMO, G. A. 2013. *Questioning Norwegian societal security efforts—Police-military cooperation in national crisis management [Research application submitted to NFR]. Forsvarets Forskningsinstitutt (FFI).* [online]. [cit. 2023-07-29]. Available at: https://prosjektbanken.forskningsradet.no/prject/FORISS/233724?Kilde=FORISS&distribution=Ar&chart=bar&calcType=funding&Sprak=no&sortBy=date&sortOrder=desc&resultCount=30&offset=60&TemaEmne.2=Forsvar+og+sikkerhet

GIANNOPOULOS, Antonios, PIHA, Lamprini and SKOURTIS, Gorge, 2021. Destination branding and co-creation: a service ecosystem perspective. In: *Journal of Product & Brand Management* [online]. Vol. 30 No. 1, pp. 148-166 [cit. 2023-07-29]. ISSN 1061-0421. Available at: https://doi.org/10.1108/JPBM-08-2019-2504

KETTL, F., Donald, 2020. *Politics of the Administrative Process 8th Edition, Kindle Edition.* Maryland: CQ Press. ISBN 978-1544374345.

KORAUŠ, Antonín, KURILOVSKÁ, Lucia a Stanislav ŠIŠULÁK, 2022. *Increasing the competencies and awareness of public administration workers in the context of current hybrid threats* [online]. [cit. 2023-07-29]. ISBN 978-80-245-2466-5. Available from: https://relik.vse.cz/2022/download/pdf/651-Koraus-Antonin-paper.pdf

MATTINGSDAL, Jostein, ESPEVIK, Roer, JOHNSEN and HYSTAD, Sigurd, 2023. Exploring Why Police and Military Commanders Do What They Do: An Empirical Analysis of Decision-Making in Hybrid Warfare. In: *Armed Forces & Society* [online]. [cit. 2023-07-29]. ISSN 1556-0848
Available from: https://doi.org/10.1177/0095327X23116071.

MIHALČOVÁ, Bohuslava, KORAUŠ, Antonín, ŠIŠULÁK, Stanislav, GALLO, Peter, LUKÁČ, Jozef, 2023. The risks of misusing social networks in the context of hybrid threat. In: *Entrepreneurship and Sustainability* [online] Vol. 10, n. 4, p. 357-371 [cit. 2023-07-29]. ISSN 2345-0282.
Available from: http://doi.org/10.9770/jesi.2023.10.4(22)

MUMFORD, Andrew and Pascal CARLUCCI, 2023. Hybrid warfare: The continuation of ambiguity by other means. In: *European Journal of International Security* [online]. Vol. 8, n. 2, p. 192-206 [cit. 2023-07-29]. ISSN 2057-5637.
Available from: https:://doi.org/10.1017/eis.2022.19.

YANAKIEV, Jankislav, 2018. Promoting interagency and international cooperation in countering hybrid threats. IN: *Information & Security* [online]. Vol. 39, n. 1, p. 5–8. ISSN 1314-2119 [cit. 2023-07-29].
Available from: https://doi.org/10.11610/isij.3900

Affiliation
This article contains the results of research that is part of the 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.*

Author's contact information:
prof. Ing. Antonín Korauš, PhD., LL.M., MBA
Akadémia Policajného zboru v Bratislave,
Sklabinská 1, 835 17 Bratislava 35,
Slovak Republic
E-mail: antonin.koraus@akademiapz.sk
doc. Ing. Miroslav Gombár, PhD.
Fakulta manažmentu, ekonomiky
a obchodu,
Prešovská univerzita v Prešove,
Konštantínova 16, Prešov.
E-mail: miroslav.gombar@unipo.sk