

ZVYŠOVANIE KOMPETENCIÍ A POVEDOMIA PRACOVNÍKOV VEREJNEJ SPRAVY V KONTEXTE AKTUÁLNYCH HYBRIDNÝCH HROZIEB

JEL Code: JEL Code, JEL Code, JEL Code (2 – 3)

Introduction (Times New Roman, 14 pt., bold)

Text of introduction (Times New Roman, 12 pt. , alignment in block, spacing 1,5) xxxxxxxx

1 Title of chapter (Times New Roman, 14 pt., bold)

Hybrid Threats is a concept that has entered to many states' official documents and security strategies. Both the EU and NATO have taken serious measures to counter hybrid threats related activity. The authors (Arcos and Smith 2021) in this special paper on hybrid threats aim to improve the understanding of the general professional public on how hybrid threat actors use and can potentially use the information environment to target democratic societies and decision-making processes at different levels. purposes. Information and communication technologies have brought remarkable advances in the ways we obtain information and build awareness on the world and its events and interact with the others, but at the same time, these developments create opportunities for conducting information and influence operations with a hostile intent at an unprecedented scales. Political warfare, active measures, and communication-led covert actions operations are not new, and propaganda has been used throughout the history in conflict and war like situations. However, today our digital communication environment and the communication tools that we employ for legitimate purposes are also being employed by hostile authoritarian actors and/or their proxies at a scale that has interfered in our democratic processes like elections, to erode trust in our institutions, polarize and divide our societies in unhealthy ways and sow animosities between states and international partner countries. Since human beings make decisions based on their representations about the world and the information available through interpersonal symbolic interactions and through the different media, information can be deliberately utilized for a malign activity to produce cognitive, affective and behavioural effects.

The research of the collective of authors (Mazaraki et.al 2021) is based on the results of a scientific study that proved that the transformation of modern interstate conflicts takes place in the direction of their acquisition of hybridization features, if it is understood as a process of using various coercive means, predominantly of a non-military nature. The authors argue that an urgent task in the context of countering hybrid threats is to assess the likelihood of multiplier effects from the implementation of their combinations. The military, economic and information spheres have been identified as key dimensions of hybrid confrontation. The specificity of hybrid threats in the economic sphere are those that would allow the initiating aggression to disguise its participation in the conflict and the target country to obtain critical resources for the development of its economic system. The nature of synergistic and cumulative effects is considered and their interpretation in the context of hybrid warfare is presented. The respective effects are defined as multiplicative, i.e. those that have a multiplying effect, providing accumulation (accumulation) and synergy (amplification) from

the implementation of threats in different areas of hybrid confrontation. The evaluation of the probability of the multiplying effect of various hybrid threats focuses on the fight against those combinations of threats, which can have a significant impact on the political and economic system of the state of hybrid aggression.

The authors (Steingartner and Galinec 2021) dealt with the design of the model of hybrid threats and cyber deception platform and solution for cyber threat detection. National networks face a broad range of cyber threats. It includes advanced and persistent peril that can evade commercially available detection tools and defeat generic security measures. Cyber attacks are becoming more intense and complex as they reflect an increasing level of sophistication, e. g. by advanced persistent threat (APT) activity. This environment of menace is of a global nature when transcending geographic boundaries and characterized by the emerging development of offensive cyber capabilities that are an inherent part of conflicts. Deception methods and techniques are being successfully employed by attackers to breach networks and remain undetected in the physical and in the virtual worlds. However, in the world of cyber security, deception as a tactic and element of a more robust defensive strategy has been still largely underexploited. The broad concepts of deception within cyber security were introduced decades ago. Still, these were technological solutions focused on providing technical capabilities to distract, mislead or misdirect the attacker. Only recently has the focus shifted on to how to shape the attackers' sense-making of what is happening as they illegitimately explore networks. In this way, Cyber Deception nowadays provides an opportunity to scare, deter, and retaliate against those that violate organizations' systems. In connection with the foregoing authors created and presented the novel model of hybrid threats in hybrid warfare as a combination of multiple conventional and unconventional tools of warfare. Authors investigated the cyber deception platform and industrial model and solution for threat detection using deception-based methods.

For decades, the concept of deterrence and the fear for nuclear confrontation withheld large powers from waging aggression against each other. Recent technological developments and the growing interconnectedness however allowed some states to find ways to challenge the West by using so called 'hybrid threats'. This way of waging war entails the synchronized use of a broad spectrum of instruments that are well-designed to stay below the thresholds of detection, attribution and retaliation. Combining these (relatively cheap) threats with conventional military hard power confronts the liberal democracies with a difficult choice in terms of defence budget allocation. Whereas arms race stability in the conventional and nuclear domain leads to a peaceful stalemate, this article demonstrates that adding hybrid threats to the spectrum of state power projection leads to a gradual shift of the power balance. While hybrid threats have been extensively studied within the international relations literature, the collective of authors (Balcaen et al. 2022) pioneered the study of this changing security paradigm from a defense economic perspective.

The "rules of war" themselves have changed significantly. Nonmilitary options have come to play a greater role in achieving political and strategic goals and, in some situations, are greatly superior to the power of weapons. The role of mobile joint forces operating in an integrated

reconnaissance and information environment is rising through the use of new opportunities now available to control and logistic systems. The European Union (EU) and its Member States continue to face serious and acute threats, which are increasingly taking non-conventional forms, such as radicalization leading to terrorist attacks, chemical attacks, cyber-attacks or disinformation campaigns. All these actions have one thing in common - they seek to destabilize and endanger society and undermine core values. In connection with the foregoing authors (Galinec et al. 2019) created and presented the novel model of hybrid threats. Furthermore, within the same model authors investigate actions for cybersecurity and cyber defence in conditions of increasing challenge of cyber-attacks and the limited capabilities to respond to this threat describing the process of creation and performance of EU Cyber Rapid Response Teams (CRRTs) and Mutual Assistance in Cyber Security, introducing novel approach to cybersecurity and cyber defence at the EU level.

Hybrid expansion on the information space is spreading, there is no reason to believe, say the authors Tkachuk et al. 2021 that hybrid threats are declining. Hybrid aggression is growing, threatening the political security of democracies. The article reviews hybrid influences and threats. The study focuses on the most influential player - the Russian Federation, which poses one of the greatest hybrid threats to states, ignoring the generally accepted civilizational norms of behavior, rules and morals. The factual data were collected and analyzed for the period of 1988-2020 and covered a number of hybrid threats, methods of distribution, methods of implementation, social media used and proven facts. The study focused on the most influential hybrid threats, including propaganda, cyber attacks, hybrid wars and discrediting government agencies.

In the context of hybrid warfare, an urgent question arises as to the adequacy of responding to its challenges. Ukraine, the EU countries and NATO are facing new threats, which require democracies to make changes in military and political activities, to find new forms and methods of ensuring national security. Hybrid warfare as a form of undeclared war is conducted with the integrated use of military and nonmilitary instruments (economic, political, informational and psychological, etc.), which fundamentally changes the nature of military struggle. Thus, the change in the nature of the current armed conflict and the hybrid aggression of the Russian Federation against Ukraine have created an impetus to accelerate transformations and structural changes in the security and defence sector of Ukraine but also EU countries (Bratko et al. 2021).

Summary

Zvýšenie odolnosti Slovenska voči pôsobeniu hybridných hrozieb pomocou realizácie komplexného súboru opatrení zahŕňajúcich optimalizáciu procesov v subjektoch verejnej správy, zvýšením vzdelávacích kapacít, získaním nových kompetencií a zručností subjektami verejnej správy prostredníctvom odborného systému vzdelávania.

Kríza spôsobená ochorením COVID-19 takisto zdôraznila to, ako sociálne rozdiely a neistota vedú k bezpečnostnej zraniteľnosti. Zväčšuje to potenciál rafinovanejších a hybridných útokov zo strany štátnych a neštátnych subjektov, ktoré využívajú zraniteľnosť pomocou kombinácie kybernetických útokov, poškodzovania kritickej infraštruktúry, dezinformačných kampaní a radikalizácie politického jazyka.

Nízka miera informovanosti a znalostí o problematike hybridných hrozieb, ich foriem, aktérov a procesov v radoch pracovníkov verejnej správy si vyžaduje zásadné a komplexné riešenie vo forme robustného vzdelávacieho programu. Moderný vzdelávací program postavený na moduloch a prispôsobený špecifickým potrebám danej cieľovej skupiny vo forme e-learningu ako aj fyzických interaktívnych tréningov môže zásadne zvýšiť nielen mieru povedomia ale aj pripravenosti pracovníkov verejnej správy identifikovať jednotlivé zložky hybridných hrozieb a zvoliť adekvátnu reakciu.

Jedným z najefektívnejších spôsobov akým otestovať silné a slabé miesta štruktúr a procesov jednotlivých zložiek bezpečnostného systému pri reakcii na hybridné hrozby sú simulácie. Za týmto účelom project vzdelávania počíta s vypracovaním a následnou realizáciou simulácií scenárov rôznych druhov hybridných hrozieb vo forme cvičenia so zapojením centrálnej i regionálnej úrovne subjektov verejnej správy. Ich cieľom bude otestovať schopnosť identifikovať atribúty hybridnej hrozby, zvoliť vhodný prístup a prispôbovať reakciu vývoju prostredia.

A summary of the issue of hybrid threats is provided by research (Bazarkina 2021), where the aim was to identify the main components of the EU approach to countering hybrid threats. To achieve this goal, research questions were posed: 1) How does the theory of hybrid warfare define hybrid threats, what are its strengths and weaknesses? 2) How is the approach to combating hybrid threats regulated in the EU? 3) What changes are taking place in this approach under the influence of trends in recent years, including the crisis caused by the coronavirus pandemic? The author concludes that the "open architecture" of the hybrid war theory, the wide possibilities of interpreting the definition of hybrid threats allow us to improve practical measures and theoretical approaches to security problems. However, as economic competition and political contradictions under geopolitical rivalry deepen, the approach to countering hybrid threats is hyper politicized, being used to justify sanctions pressure, strengthening military blocs or massive psychological campaigns against a political adversary. The EU tries to develop and improve a systemic approach to ensuring security in the context of the growth of hybrid threats. However, this approach is increasingly deformed under the influence of above-mentioned hyperpoliticization. This is especially evident in the EU's attitude towards Russia and China, which are constantly accused of creating hybrid threats. The excessive use of the rhetoric of the hybrid war theory in the EU discourse jeopardizes the security of Europe.

Conclusion (Times New Roman, 14 pt., bold)

Acknowledgment (Times New Roman, 14 pt., bold)

If any

References (Times New Roman, 14 pt., bold)

Pleas, use 10 – 15 references. All citations in the text and all references must meet APA styles (American Psychological Association – more information <http://www.apastyle.org/>)!

Please, use automatic citation maker for citation and references: [automatic APA citation maker](http://citationmachine.net/index2.php?reqstyleid=2&newstyle=2&stylebox=2).(<http://citationmachine.net/index2.php?reqstyleid=2&newstyle=2&stylebox=2>)

- Avery, R. J., Bryant, W. K., Mathios, A., Kang, H., & Bell, D. (2006). Electronic course evaluations: Does an online delivery system influence student evaluations? *The Journal of Economic Education*, 37(1), 21–37. <https://doi.org/10.3200/JECE.37.1.21-37>
- Berk, R. A. (2012). Top 20 strategies to increase the online response rates of student rating scales. *International Journal of Technology in Teaching and Learning*, 8(2), 98–107.
- Arcos, R.; Smith, H. (2021) Digital Communication and Hybrid Threats, REVISTA ICONO 14-REVISTA CIENTIFICA DE COMUNICACION Y TECNOLOGIAS, Volume 19, Issue 1, Page 1-14. DOI 10.7195/ri14.v19i1.1662
- Balcaen, P.; Du Bois, C.; Buts, C.: (2022) A Game-theoretic Analysis of Hybrid Threats. DEFENCE AND PEACE ECONOMICS. Volume 33. Issue 1. Page 26-41. DOI 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. Issue 6. Page 133-143. DOI 10.15211/soveurope62021133143
- Bratko, A.; Zaharchuk, D.; Zolka, V. (2021) Hybrid warfare - a threat to the national security of the state. REVISTA DE ESTUDIOS EN SEGURIDAD INTERNACIONAL-RESI. Volume 7. Issue 1. Page 147-160. DOI 10.18847/1.13.10
- Galinec, D.; Steingartner, W.; Zebic, V.: (2019) Cyber Rapid Response Team: An Option within Hybrid Threats. Book Group Author: IEEE 15TH INTERNATIONAL SCIENTIFIC CONFERENCE ON INFORMATICS. Page 43-49. Poprad, SLOVAKIA. NOV 20-22, 2019
- Mazaraki, A.; Kalyuzhna, N.; Sarkisian, L.: (2021) MULTIPLICATIVE EFFECTS OF HYBRID THREATS. BALTIC JOURNAL ECONOMIC STUDIES. Volume 7. Issue 4. Page 136-144. DOI 10.30525/2256-0742/2021-7-4-136-144
- Steingartner, W.; Galinec, D.: (2021) Cyber Threats and Cyber Deception in Hybrid Warfare Volume 18. Issue 3. Page 25-45. ACTA POLYTECHNICA HUNGARICA. ISSN: 1785-8860
- 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 ALTA-JOURNAL OF INTERDISCIPLINARY RESEARCH. Volume 11. Issue 1. Page 29-33. Special Issue 16. ISSN: 1804-7890

Contact

Antonín Korauš

Academy of the Police Force in Bratislava

Sklabinská 1, 835 17 Bratislava 35

Mail: antonin.koraus@akademiapz.sk

Lucia Kurilovská

Faculty of Law, The Comenius University in Bratislava,

Šafárikovo nám. 6. 818 06 Bratislava

Mail: lucia.kurilovska@flaw.uniba.sk

Stanislav Šišulák

Academy of the Police Force in Bratislava

Sklabinská 1, 835 17 Bratislava 35

Mail: stanislav.sisulak@akademiapz.sk