INCREASING THE COMPETENCES AND AWARENESS OF PUBLIC ADMINISTRATION AND POLICE OFFICERS IN THE CONTEXT OF CURRENT HYBRID THREATS

Antonín Korauš - Lucia Kurilovská - Stanislav Šišulák

Abstract

The increase in hybrid threats that jeopardize the foundations of a democratic rule of law poses one of the most serious risks to state security. One of the significant sources of hybrid threats in society is the deliberate and long-term spreading of propaganda, disinformation, and deceptive information, especially in the internet environment, which creates a breeding ground for the rise of anti-systemic, anti-democratic political attitudes, which often turn into violent crimes.

Security management at both central and regional levels is currently lacking in identifying and addressing hybrid threats and their manifestations, and in most public institutions — local government and regional self-government — this activity is a marginal and ignored area of security. Complex understanding of the issue is a high-quality prerequisite for the elimination of hybrid threats throughout society. For this reason, it is necessary to develop uniform methodological procedures and proposals for adequate, effective tools to address and counter the negative manifestations of these threats, for the public administration and police personnel, and provide them with an adequate professional form of education in this field not only for the purpose of informing, but also for the purpose of raising awareness of hybrid threats. These reasons have led to the creation of a project under the Operational Programme "Effective Public Administration" aimed at increasing Slovakia's resilience to hybrid threats by strengthening public administration capacities.

Keywords: hybrid threats, public administration, education, raising awareness

JEL Code: F 52, H 56, J 45

Introduction

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. 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 unprecedented scales. Political warfare, active measures, and communication-led covert actions and 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 team 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 specificities 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, the authors created and presented the novel model of hybrid threats in hybrid warfare as a combination of multiple conventional and unconventional tools of warfare. The 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 of 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, a team of authors (Balcaen et al. 2022) pioneered the study of this changing security paradigm from a defence 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 with 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 its 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, the authors investigate actions for cybersecurity and cyber defence in the conditions of an 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 in 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 behaviour, rules, and morals. The factual data were collected and analysed for the period of 1988 – 2020 and covered several 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 at al. 2021).

1. Research of educational concepts in the field of hybrid threats within selected EU countries followed by the development of a concept of education for the conditions of the Slovak Republic

The project will coordinate the educational activities of students and cadets of the Academy of Police Force in Bratislava, members of the Police Force of the Slovak Republic and employees of public administration active in detecting and preventing the manifestations of hybrid threats.

The aim of the research part of the project is mainly to identify uniform and unambiguous practices in the field of identification, countering, and prevention of hybrid threats through research that shall focus in particular on the analysis, synthesis and comparison of expertise in the subject of hybrid threats at national and international level. The feasibility of the research is directly dependent on the input information, documents and data provided by other partners within their analytical capacities, tools, and existing international cooperation.

The research part will consist mainly of a search, analysis and synthesis of relevant professional documents, on the basis of which, using the comparative method, the expertise obtained from the project partners will be compared with the knowledge obtained by the research activities of the research team of the Academy of the Police Force in Bratislava in order to define the needs for ensuring an effective fight against hybrid threats in the Slovak Republic. The research will also focus on the analysis of current legislation on the issue of hybrid threats in the Slovak Republic. Subsequently, the research part will continue with an analysis and comparison of the available information allowing for a more consistent insight into the problem and its understanding in the context of mutual relations. This section, applying the historical method, will also examine previous perspectives on dealing with the issue, as well as examine and analyse specific cases using the causal analysis in this area. Next, the research methodology will continue based on the primary information; through the analysis and synthesis of knowledge, the experts will focus on the stated objectives, the output of which will be the methodologies and education at the Academy of Police Force in Bratislava. This phase, thanks to various explorative methods, is expected to provide a deep insight into both theoretical as well as practical problems that arise in this area. Scientific synthesis will also be used, which, based on the previous phase, will enable to put together the acquired theoretical and practical findings into a new system of knowledge on the examined issue. This new knowledge will be presented to the participants of the study and will also be presented at a conference and in the created methodologies. The degree of originality of education is directly determined by the societal developments that have emerged in the recent years and where the urgent need to raise awareness of the risks posed by hybrid threats is visible. The paradox of the present time is that the "online generation" is growing up without the awareness and knowledge of the possible pitfalls of hybrid threats.

The output of the research part will include:

- Research of educational concepts in the field of hybrid threats within selected EU countries, followed by the development of the concept of education for the conditions of the Slovak Republic.
- Adaptation of thematic plans and information sheets within the mandatory subjects — in particular: Cybersecurity, Information Management, Strategic Management and Crisis Management
- A training programme in the system of lifelong learning for the needs of the Police Force and public administration.

1.1. Inclusion of hybrid threats into the curricula of the Academy of the Police Force

The aim of the education of about 400 full-time and part-time students of the Academy of Police Force in Bratislava will be to develop and improve the professional competencies in the field of hybrid threats during 2 semesters of pilot education in the selected compulsory subjects, namely: Cybersecurity, Information Management, Strategic Management and Crisis Management.

The educational activity focused mainly on the issue of hybrid threats, their manifestations and dangers will include intercultural education, work with prejudices and topics related to hybrid threats. The education aims to inform the students about hybrid threats and the Academy of the Police Force in Bratislava will proceed to the adaptation of thematic plans and information sheets within the selected mandatory subjects.

1.2. Training programme in the lifelong learning system

The training activity will focus mainly on the issue of hybrid threats in the work of police officers and public administration employees. In particular, the aim of the training is to develop and improve professional competences in the field of hybrid threats. The target groups of the training are mainly selected police officers and public administration staff. The aim of the individual parts of the training is to inform police officers and public administration employees about hybrid threats, their manifestations, and dangers. The topics of the education will concern prevention and tackling different forms of hybrid threats. The training programme in the lifelong learning system will be an accredited training programme covering approximately 1,800 police officers and public administration employees, of which 1,080 will be trained face-to-face and 720 online. Upon successful completion of the lifelong learning programme, the trainees will receive a certificate of completion of the training.

Conclusion

The implementation of the national project will significantly improve the readiness of public authorities at both central and regional levels to detect, analyse and adopt targeted measures against hybrid threats. Building human resources, technical capacities and implementing educational and communication activities will significantly increase the resilience of key actors to different forms of hybrid threats in the relevant domains. A vulnerability audit and subsequent proposals to amend regulatory frameworks will fill systemic vulnerabilities against a hybrid activity. At the same time, Slovakia's resilience to hybrid threats will be increased through the implementation of a comprehensive set of measures involving optimising of processes in public administration entities, increasing educational capacities, acquiring new competences and skills by public authorities through a system of professional training.

The introduction of evidence-based approaches to decision-making processes in the form of regular analytical materials will increase the quality and impact of the decisions taken and allow for the evaluation of their effectiveness.

By completing the building of strategic communication capacities of the key departments, the central government bodies will:

- be able to communicate their public policies and measures, and build citizens' trust in the state and its institutions much more effectively
- increase and enhance the quality of human capital — thanks to the introduction of online and face-to-face training
- improve the quality of management decisions based on a better knowledge base
- have consolidated information across different entities of central government bodies
- achieve a more efficient use and sharing of resources by streamlining cooperation between the sectors concerned.

The COVID-19 crisis has also highlighted how social inequalities and uncertainty lead to vulnerabilities in security. This increases the potential of more sophisticated and hybrid attacks by state and non-state actors which exploit the vulnerability through a combination of cyber-attacks, damage to critical infrastructure, disinformation campaigns and radicalisation of political language.

A low level of awareness and knowledge of hybrid threats, their forms, actors and processes among the public administration and police staff requires a fundamental and comprehensive solution in the form of a robust educational programme. A modern educational program based on modules and adapted to the specific needs of the target group in the form of e-learning as well as personal interactive trainings can significantly increase not only the level of awareness but also the readiness of public administration and police personnel to identify individual components of hybrid threats and choose an adequate response.

Simulations are one of the most effective ways to test the strengths and weaknesses of the structures and processes of individual components of the security system in response to hybrid threats. To this end, the educational project counts on the development and subsequent implementation of simulations of scenarios of different types of hybrid threats in the form of an exercise involving the central and regional levels of public administration entities and the police. Their aim will be to test the ability to identify the attributes of hybrid threats, choose an appropriate approach and adjust the response to the evolving environment.

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 the above-mentioned hyper politicization. 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.

Acknowledgment

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.

References

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