DOI: https://doi.org/10.52651/vr.j.2023.3

VOJENSKÉ REFLEXIE

AOS military science journal AOS

VOLUME XVIII.
ISSUE 3/2023

AKADÉMIA OZBROJENÝCH SÍL
GENERÁLA MILANA RASTISLAVA ŠTEFÁNIKA

Armed Forces Academy
of Gen. Milan Rastislav Štefánik

VOJENSKÉ REFLEXIE

MILITARY SCIENCE JOURNAL

VOLUME XVIII.
ISSUE 3/2023

Journal is indexed in ERIHPLUS, DOAJ

ISSN 1336-9202

Editorial Board address
Akadémia ozbrojených síl generála Milana Rastislava Štefánika
Demänová 393, 031 01 Liptovský Mikuláš
tel. +421 960 423524, +421 960 422620
e-mail redakcie / e-mail board: lubomir.belan@aos.sk; ivan.majchut@aos.sk

The peer-reviewed journal Vojenské reflexie was established in 2006 and is issued by the Armed Forces Academy, which is a state military university with a long history of **scientific research in the field of security, defence and the military**. At present, the academy cooperates with partners from military and civilian universities and other renowned specialized institutions from the Slovak Republic as well as from abroad.

The journal Vojenské reflexie is intended for contributors and readers from the security community, members of the armed forces, academic teachers, students and other readers interested in the following:

- **security and strategic studies,**
- **operational art and tactics,**
- **economy and management of defence resources,**
- **socialstudies and humanities,**
- **political science and international affairs,**
- **military technologies and technological studies,**
- **military and police theory and practice,**
- **lifelong and career education.**

Opinions and attitudes presented in the articles do not necessarily have to be in accordance with the opinion of the editor and the editorial board of the journal. They are the sole responsibility of their authors. The journal does not charge article processing or any other charges.

The articles are published in Slovak, Czech and English language. The articles are peer-reviewed. The journal Vojenské reflexie is published in electronic format on its website: vr.aos.sk :

- Twice a year in Slovak and Czech language, always in June and December

- Once a year in English, always in December.

Vojenské reflexie is a journal with open access, which means that the whole content is available for the readers or institutions for free. The readers may read, download, copy, distribute, print or refer to the texts of the articles or use them for any purpose without the consent of the authors or editor. The readers may copy, distribute and refer to the articles when citing the source.

Regarding the peer-reviewed articles and other published texts, **Vojenské reflexie** uses the Creative Commons - Attribution 4.0. license. By submitting the article the author agrees with the use of CC BY 4.0 license. The author grants the journal the right to first publication of the work. Copyrights are granted to the authors. Thus, the authors are granted the right to publish their work on their website, on academic social sites or to raise its profile in other ways.

Reviewers

Prof. Klára S. KECSKEMÉTHY, CSc.,

Faculty of Military Science and Officer Training,
Budapest, Hungary

Dr.h. c. Prof. Eng. Pavel NEČAS, PhD., MBA,

Matej Bel University, Banská Bystrica,
Banská Bystrica

Assoc. Prof. Eng. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.

Academy of Police Force,
Bratislava

Prof. Eng. Vojtech JURČÁK, CSc.,
Prof. Eng. Boris ĎURKECH, CSc.,
Assoc. Prof. Eng. Ivan MAJCHÚT, PhD.,
PhDr. Mária MARTINSKÁ, PhD.,
PhDr. Soňa ŠROBÁROVÁ, PhD., MBA,
Eng. Daniel BREZINA, PhD.

AFA of General M. R. Štefánik,
Liptovský Mikuláš

CONTENTS

DOI: https://doi.org/10.52651/vr.a.2023.3.07-20
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2023, Number 3, Page 07-20

CHALLENGES FACED BY LAW ENFORCEMENT IN THE 21ST CENTURY, WITH A SPECIAL FOCUS ON SPECIFIC ISSUES OF HYBRID THREATS – SECURITY "OF A THOUSAND FACES"

Péter CIELESZKY

ARTICLE HISTORY

Submitted: *17. 02. 2023*

Accepted: *06. 12. 2023*

Published: *31. 12. 2023*

ABSTRACT

In this paper, I explore the challenges facing policing in the 21st century through a multifaceted approach to security. Herein, the idea of security is seen as being filled with the evolutionary determination of humans, which is expressed in the concept of security as it applies to the individual, the need to establish an internal order of social coexistence at the level of human communities, and the relations between certain community formations, i.e. states, as well as international relations. I will show how the creation of security today is becoming an increasingly complex issue, while ancient algorithms and instincts drive the psychological mechanisms that underpin this perception. The real challenge today is how to mitigate the security deficits referred to in this study so that their impacts legitimise everyday relations and satisfy our basic evolutionary needs.

KEYWORDS

security, order, evolutionary psychology, globalization, legitimacy

INTRODUCTION

In the autumn of 2019, I was leafing through a book. A colleague of mine called it just a "blue book" in which experts, professionals and young researchers wrote about the security challenges of the 21st century (Finszter and Sabjanics, 2017). If one browses through the table of contents, they will find some 43 studies, arranged thematically in chapters, on the importance of security, the security challenges of strategic forecasts and interdisciplinary responses that embrace the topic. The volume covers – without claiming to be exhaustive – approaches to security from a military, law enforcement, economic, health care, international, national security, energy and environmental security, water security, etc. aspect.

This diversity and thematic variety reminded me of the bustling atmosphere of a whirling cavalcade at a market fair. These works are characterised by different approaches and varying degrees of focus, each of which, in its own way, provides a wealth of valuable information for those interested in the topic. This horizon is almost unfathomable. It is as if the individual pieces of a large puzzle were being outlined, some of them touching, some of them so far apart from each other that only the imagination can fill the gap that opens up. Some of its details are now fully worked out to the extremes, while other areas are just beginning to attract scientific interest. Variations on a theme, searching for possible nodes of security's rich manifestations of network-like entanglements. The complexity of the problem area requires not only effective research in the sub-areas, but also a systemic approach to them to ensure effective action to address the challenges. This is partly indicated by the editors' recommendation.

"The [...] processes of the past decades have brought to the surface threats and problems that have changed the understanding of the topic of security, differentiated needs have emerged, new areas and issues have surfaced; thus a complex, systemic overview of security challenges has become extremely timely." (Finszter and Sabjanics, 2017, p. 7)

In this dissertation, I have tried to take a multi-faceted, non-exhaustive but thought-provoking approach to security in order to draw the reader's attention also to the necessity of a systemic approach, as formulated by the editors, in addition to the timeliness thereof.

As the methodology for research of the topic an overview and critical processing of the most obvious literature sources was offered. Military, security and law enforcement science are obviously fundamental field for the investigation of the indicated issue in the title. I also considered it worthwhile to place the conceptual changes of security in a broader social science, more specifically a political and state science economics (evolutionary), psychology, cultural anthropology and history of ideas context. It not only proves its nature, but also the diversity of humanity's scientific interest in this phenomenon and the concept that seeks to capture.

1 ON THE CONCEPT OF SECURITY AND ITS EVOLUTIONARY APPROACH

There is no consensus in the literature on the conceptual definition of security (Balogh, 2013), but the different approaches provide a valuable opportunity to examine the subject of research from multiple perspectives, even encyclopaedically, to display the limits of the validity of each approach (Gärtner, 2007). In addition to this diversity, the changes in the meaning of the term are not random, and sometimes their direction can be precisely defined. Today, for example, *"the classical notion of security is reactive and territorial, while the modern notion of security is of functional and preventive nature."* (Gazdag and Remek, 2018, p. 29)

The question is, of course, what is considered variable and what is invariant. My premise is that the fundamental change is not in the original content of the concept, but in the set of circumstances and acts by which security can be guaranteed. These latter circumstances are covered by the concept of protection, which can be considered as a fundamental component of security (Gazdag and Remek, 2018). Rather, I see the fact of

diversity manifested in the conceptual framework of security as a reflection of our world as an increasingly complex system. A world in which our needs remain largely unchanged, but are expressed through an increasing number of referrals, and in which creating the conditions to meet them requires ever greater effort, ever more complex organisation and ever more resources. The system for guaranteeing security has therefore become almost incomprehensibly complex. The concept, if I see it as an expression of an idea, has retained its original source and its meaning remains unchanged.

In researching this immutability, I myself first associated it with a content derivable from the etymology of the word, which denotes a state free from disturbing circumstances ("sine cura"). Furthermore, I assume that an environment protected from such conditions is in some way orderly and has value – and therefore must be protected. If I am to explore the cause of this immutability, then I should continue with the concepts of order and value, and explore the layers of their meaning. In the present case, I am content to assume the immutability of our need for a value-based order, and not to let the striking variety of forms of its historical expressions (the diversity of civilisations and cultures) deceive me and distract me from the immutability of its causes.

In my earlier study, I argued (Cieleszky, 2021) that behind the determination of systemic thinking lies an evolutionary need inspired by a priori necessity spanning across historical ages. Its manifestations are expressed in, or can be traced back to, acts of self-preservation, species-preservation and subsistence. I have summarised this idea as the idea of order, and found that its manifestations are expressed through increasingly complex social (and other) relations, in an orderly manner, representing value.

In his approach to evolutionary psychology, Tamás Bereczkei argues that the psychological mechanisms of human behaviour are universal and species-specific because of their evolutionary origins. However, it is not the manifest manifestations of behaviour (cultural variability) that are invariant, but the psychological programmes that ultimately genetically present in all human beings, and which relate in particular to interpersonal relationships (Bereczkei, 2008). However, these interpersonal relations can only be interpreted in the case of a group of a limited number of individuals (Csányi Vilmos, 2016, chap. 5.1), and given that *"our species has spent more than 99% of its evolutionary history in a hunter-gatherer mode of existence [...] and its psychological mechanisms have been selected as a result of the effects of this environment"* (Bereczkei, 2008, p. 27), there is essentially no evolutionary-level adaptive explanation for an autonomous entity interpretation of interpersonal relations in modern societies other than the aforementioned one.

So when I approach the need for security, I see it as a condition of existence that can be interpreted in the conceptual circle of the idea of order and that is supported by a legitimate value system that can be traced back to it, the framework of which is provided by the early human social formation, the group, but which today, due to our way of being, which creates increasingly complex social formations, can only be realised through increasingly complex systems. However, the fact that this is the case creates a constant need for legitimacy, given that our psychological mechanisms are not optimised for our current mode of existence. Mathematical equations write by using Equation.

2 OUR EVERYDAY SECURITY IN THE SHADOW OF GLOBALISATION

The above-mentioned cultural variability can undoubtedly be a source of invaluable experience, as the more complex the ways in which human communities have been organised into formations and the more complex the representation of reality as a consensus-based construct (Balogh, 2013) has become, the more diversified the examination of the issue of security has become. The sectoral approach to security associated with Barry Buzan and his co-authors (Buzan et al., 1997) has thus been invaluable in helping to carry out investigations that reach beyond the previous frameworks of security interpretations. One of the aims of sectoral delimitation is to make the subject of research accessible and knowable, by highlighting a part from the whole. However, the examination and exploration of the functioning of each sub-area must be carried out in a way that maintains their compatibility by the functioning of their original complex environment, i.e. our perceived reality. After all, the point is to understand the complex environmental operation that guarantees security for the reference objects in the given age and under the circumstances. Sectoral delimitation – or any delimitation – is therefore a technical act, although its concrete implementation is created precisely by the possibility of partial independence of the examined areas. Understanding how complex systems work would otherwise be beyond the reach of scientific thinking.

Taking into account practical aspects, it is also worth reflecting on the delimitation of the concept of security inherent in everyday thinking. In this sense, a distinction can be made between concepts of security applicable to international relations that are, with regard to the individual, social in nature (1), community-determined in the field of social coexistence(2), affecting relations between states(3) (Gazdag and Tálas, 2008). The latter is usually considered as part of the interdisciplinary field of security studies, which emerged after the Second World War, and is separate from international studies, while the former are the focus of interest of other disciplines (Gazdag and Remek, 2018).

The social perception of security is essentially based on the presence or absence of conditions that are relevant to the individual (health, public benefits, job and life security, etc.) and is our most direct relationship with physical reality, our physical environment and our associated needs. For a long time in the process of becoming human, the dominant force of this was the only content that could be hidden in the concept of security – a dominant force that was certainly encoded for a long time by the conservative nature of evolution (Csányi Vilmos, 2016). This is probably precisely the source of the idea we are looking for, and its determinants are being explored by human ethology, which is researching the biological basis and sources of human behaviour today, especially through the current results of the scientific approach of evolutionary psychology, which I have referred to above.

The community-determined perception already targets individuals as members of the (nowadays, state-forming) basic population that make up the community by ensuring the internal order (Gazdag and Tálas, 2008) of social coexistence. This is also the explicit field of investigation of the “young” science of law enforcement, since law enforcement in the narrow sense of the term – in the context of the modern state – is an administrative activity whose social function is to avert the dangers arising from unlawful human behaviour – in possession of the monopoly on legitimate physical violence (Finszter, 2018).

Importantly, the study of the psychological mechanisms that determine interpersonal relations is an essential element of any research that seeks to understand the functioning of the members of the basic population that make up the community and of the community itself, given the fact of evolutionary adaptation referred to in the previous chapter and their impact on the perception of security. There are convincing arguments that the sometimes dysfunctional functioning of modern societies, the identification of certain social problems as individual pathologies, are precisely the consequence of an unnatural modern social existence. In one of his lectures, Péter Popper refers to the fact that it is no wonder that people protect themselves and the people around them from the influence of social pathology by forming small communities by sticking together. It is hard not to wonder how ancient algorithms and instincts drive these psychological mechanisms, and how this affects modern man's idea of security and his needs in this regard (Popper, 2021). In this respect, therefore, if we listen to the explanation of evolutionary psychology, we must work to strengthen the elements of security that are involved in these mechanisms.

In the case of international relations between states, it is important to draw attention to some of the key changes that are contributing to the evolution of our perceptions of security in the broader sense, but also to the evolution of social and community-determined perceptions of security. The role of the reference object – the state or the nation-state – which plays a decisive role in guaranteeing security is constantly changing. With the emergence of modern states and the establishment of their relative sovereignty, the general acceptance of international law and Westphalian sovereignty, among the interpretations of sovereignty classified by Stephen D. Krasner (Varga, 2015), has created the foundation for international relations between states, undoubtedly in a system dominated by anarchy in international relations. However, what is also known as the Westphalian system – which has replaced a much more unpredictable mechanism – has been disrupted, and some speculate even broken up, by the impact of globalisation. *"Many people believe that the change in the world is driven by the struggle of civilisations. According to Ulrich Beck, this is a mistake. The reality is that the borders of nation-states are disintegrating, and the world today is characterised by a race between different cultures to gain and hold power."* (Irk, 2012, p. 25–26)

Béla Pokol argues that the *"increasing power of the global international order over individual sovereign states in many ways makes the value of sovereignty more formal in terms of the autonomy of individual states"* (Pokol, 2014, p. 1), and then argues that *"[...] the determination of sovereign states by global powers has increased enormously, and the exploitation of the opportunities arising from their sovereignty [...] is blocked by the international treaties that institutionalise the global international order."* (Pokol, 2014, p. 6)

3 MADE IN AMERICA

Hearing the ideas referred to, it is difficult to abstract from an American example. In his farewell address on 17 January 1961, President Eisenhower warned of *"the institutionalised system of cooperation among political, business, military and scientific elite groups which has become established since World War II, which has brought the processes of*

production under its control in such a way that society is unable to control them." (Eisenhower, 1961)

Andrew Mullen pointed out in this context – in this case, of course, following the example of the US – that the defence industry is supporting this with intensive media propaganda (Mullen, 2010). Then, in a paper published in Critical Sociology (Rothe and Collins, 2018, p. 16), the researchers come to the dilemma of the captured state and *"show that behind the military-industrial dependence of developed economies lies a spectacular cycle of power legitimation that in the US is reinforced and accepted by the masses, embedded in a nationalist-national security ideology."* (Cieleszky, 2021, p. 22). The military-industrial dependence can certainly be replaced by the notion of consumption dependence, and the globalised world will be equally adaptable to this approach.

Finally, a 2014 study by two Princeton professors concludes the American story by stating that *"when the interests of the average voter and the economic elite do not coincide, final policy decisions are very highly correlated (0.78 correlation) with the economic elite's position and very rarely correlated (0.05 correlation) with the average voter's position."* (Gilens and Page, 2014, p. 571). This raises problems of legitimacy of power, which, together with the decline of America's leadership role and the devaluation of the values it represents (Kagan, 2015), promises a difficult future.

The example clearly shows how certain effects of globalisation and the pressure-exerting role of the economic elite in the area of security connect secured living spaces of a social nature for the individual, which are community-defined in the area of social coexistence and which can be applied to international relations affecting the relations between individual states, for example in terms of the United States.

4 GLOBALISATION AND SECURITY DEFICITS

In a broader context, economist Dani Rodrik has taken a quite unique perspective on the possibility of democratic value choices within the nation-state framework to be fulfilled in the global structure – providing a crucial framework for understanding security. His theory of the trilemma (Rodrik, 2021) is that the three poles of choice are goals driven by nation-state interests, democratic political goals, and goals towards the realisation of a connection to the globalised world economy through deep economic integration (Cieleszky, 2021). But, in his view, only two objectives can be more fully realised simultaneously, with the consequence, in my view, of creating a deficit in every election, which we can safely call a security deficit.

In the choice of nation-state interests and economic integration, a democratic recession that favours the strengthening of authoritarian states; in the case of economic integration and the development of a democratic political system, a loss of identity leading to the emergence of parallel societies; and, when the democratic framework and the interests of the nation-state are unfolding, the backwardness resulting from the lack of integration, which leads to lower levels of well-being and thus existential security.

It is clear that security is compromised in all three choices. In the case of the first one, in particular, by openly or more covertly restricting the fundamental rights of persons.

In the second case, due to the uncontrollability of the internal order of social coexistence – manifested, for example, in the deterioration of the public security situation. And in the third case, because of the fall in living standards and the known consequences thereof.

Finally, let us quote the European Commission's reflection on the EU's strategy for the Security Union, which states: *"Security is not only the basis for personal safety, it also protects fundamental rights and provides the foundation for confidence and dynamism in our economy, our society and our democracy."* (Európai Bizottság, 2020, p. 1). The strategy has thus explicitly expressed the intertwining concerning the secure areas of international relations affecting the social relations of the individual, community-determined state relations and the relations between individual states, which I have described in more detail in this chapter.

Therefore, if we start from an ordinary approach to security, we can also take a short route – through the impact of globalisation – to the recognition of the multifaceted and complex threats to security, and to the identification of security deficits. In the present case, these are manifested in the loss of freedom, loss of identity or existential threat. A further study could aim to compare the effects of these deficits with the perceptions affected by the referenced psychological mechanisms.

5 SECURITY FROM A LAW ENFORCEMENT PERSPECTIVE

As Zoltán Balla puts it, *"the word 'security' is the term that most closely captures the essence of law enforcement"* (Balla, 2017, p. 19), and it is no coincidence that *"the scientific study and analysis of security is dealt with by military science and the emerging field of law enforcement science."* (Balla, 2017, p. 19). It seems clear, therefore, that there are aspects of the establishment of security (in the narrow sense of the term) that relate to the law enforcement field – just as it is true that *"from the aspect of military science, it is the military elements of security that must be sought"* (Dr. Vida, 2013, p. 104). In a sense, this formulation can serve as a starting point, but it certainly needs to be nuanced, for several reasons.

There is no doubt that within the state as a reference object, the boundaries that used to separate the issues of external and internal security seem to be disappearing, blurring and in some instances dissolving (Finszter, 2018). At the same time, as I have argued before, globalisation permeates almost every aspect of life, with the world economy as its driving force – which, according to some, is the perspective from which globalisation itself can be most readily discussed (Irk, 2012). The fact of the changes indicated has implications for the law enforcement-focused approach to security (Balla, 2017) and the military elements of national defence management.

However, this is only a seemingly obvious situation. It is well known that law enforcement administration was born out of national defence administration, and the creation of the modern state provided the interpretative framework for the transformation of these disciplines into professions. *"The rise to professional status of these two types of emergency response has been accompanied by the fact that the two service activities moved*

away from each other. Being a nation-state has made the qualitative difference between internal and external threats clear." (Finszter, 2018, p. 25)

However, with the distortion of the Westphalian system – one element of which is clearly the impact of globalisation – these internal-external boundaries have again become blurred, as have the boundaries between the two administrative areas. In international politics, we need only think of the failures of the military peacekeeping operations of the Cold War period, which led to the complexity of the new types of interventions and the expansion of their conflict resolution tools from 1988 onwards (Gazdag and Remek, 2018). And in the case of individual states, numerous twentieth-century examples have shown that *"the preferred solution to unbridled arbitrariness is to operate the army as police and the police as an army."* (Finszter, 2018, p. 25). So the delimitation was not easy, even after all this time.

In addition, it can be observed that the national defence and the once separate and autonomous law enforcement administration tended to emphasise their priority in the creation of security, often over any other – i.e. sectoral – actors, if they were even noticed at all. However, liberal and critical approaches to security theory have pointed out that there is no single or exclusive custodian of security today. The interest of society as a whole, in the broadest, cosmopolitan sense of the word. In his "skeptical criminology"(Irk, 2012), Ferenc Irk explains that the twentieth century has opened up a complex of challenges that have redrawn the conditions of existence of human communities and ushered in the era of the world risk society (Finszter, 2018).

The conclusions can be taken even further. Because, while there is no single custodian for the creation of security, it is also true that today, without the concerted action of all the custodians, real security is unthinkable. And this can only be realised through value-based thinking. This is why I have emphasised in the basic premises that, among the invariant elements included in the conceptualisation of security, it is worth starting the research with the examination of the concepts of order and value.

6 ON THE ISSUE OF LEGITIMACY

The previous traditional view was that the only threat to international security was military aggression between states (Albrecht, 2006). Today, this view has been refined and is seen as one of the sources of danger, however broadly we interpret the concept of military aggression. This is due to several reasons. However, Ferenc Irk's comment on globalisation can be seen as a precursor to the problem, as he believes that globalisation should primarily no longer be understood in a geographical or physical sense, but as *"a specific set of functional, political and value dimensions"* (Irk, 2012, p. 24). This also touches on the question of the social legitimacy of power, since *"if [...] in all existential questions concerning the future, governments are no longer capable of more than merely pointing to the objective constraints of the transnational economy as overwhelming, any politics will be reduced to a charade of inertia and the democratic state will lose its legitimacy. And globalisation is becoming a trap for democracy."* (Hans-Peter and Schumann, 1998, p. 20). The process outlined is having the effect of significantly weakening the legitimate framework for security,

including its community and institutional aspects, and reducing the range of instruments available to it.

The challenge of modern law enforcement thus goes hand in hand with the change in the social legitimation of power, which is inextricably linked to globalisation. Therefore, one of the future's key questions, as regards the law enforcement aspects of security (as part of civil administration), is, on the one hand, how to integrate the communities involved in the creation of security, taking into account their sectoral characteristics, and, on the other hand, how to organise, as an organisational form, the framework of its institutional functioning, as the resources of a system based on the sovereignty of individual states are necessarily exhausted by globalisation. On the latter question, the manifest manifestations of integrationist theories (EU) are as much in evidence among the solutions as the possibilities of extending global governance (a global network of international institutions, regimes, NGOs, states and other entities) in the absence of global government (Balogh, 2013).

7 ON DEMOCRATIC VALUES

It is easy to see that *"the growing dependence of domestic policies on the international environment is placing increasing demands on the adaptive capacity of states."* (Remek, 2017, pp. 134–135). However, I also think it is important to note that this has to be done in a reconfiguring legitimation context, where there is a significant change in the social relationship to power. One of the determining factors is that challenges, which may appear in the future in parallel, sometimes amplifying each other, have different effects on the lives of human communities and community formations at different levels of conditioning, and even more so on the predictability of the consequences. And the fact that this is the case is a major determinant of the chances of achieving global security.

It is of course difficult to measure the conditioning of the mindset of individual communities, but it is certain that our livelihoods and needs are guaranteed at a higher level in democratic systems. Also worthy of mention is Michael W. Doyle's keynote from the 1980s, known as the theory of democratic peace. The essence of his idea (Doyle, 1983a, 1983b), as expressed in two of his studies, is that practice shows that countries with democratic regimes do not, or much less frequently, engage in wars with each other than those with authoritarian regimes. This idea goes all the way back to the philosophy of Immanuel Kant (Rácz, 2018), but Doyle did not have to wait centuries for its impact. The export of democracy has become the official ideology of the USA (Rácz, 2018). Regardless of its known downsides, there is no doubt that the part of the world that embraces democratic values seems to have become more peaceful at the same time. In this context, it is worth drawing attention to three things.

Several studies have recently addressed the question of what proportion of the world's population lives in democratic or what can be considered democratic conditions. According to one study, the proportion of the population living in democracies as a percentage of the total population has remained stable since 2005 at around 52-55%, which represents a democratic surplus of 55% in terms of the number of individual countries (Our

Word in Data, 2021). Other research is slightly more moderate, with an estimate of 48.4% for the total population and 45.5% for countries (Demokracy Index 2019, 2021).

Stanford University professor Larry J. Diamond points out in a study that the dynamic of the spread of democratic values has been replaced by decades of stagnation around the world – which he calls a democratic recession. It also points to the fact that between 2010 and 2014, 25 countries experienced a so-called democratic regression, sometimes with an authoritarian character, affecting the internal legitimacy of these regimes (Diamond, 2015).

According to the Bennett Institute's 2020 report, it is clear that distrust and dissatisfaction with the democratic process is evident in both developing and developed democracies and has been monotonically increasing for almost two decades (the share of the population affected has increased by 9.7% in just over two decades, from 47.9% to 57.5%).

In the light of the above, one of the most important dilemmas is how to create a political, social and economic environment that provides supportive conditions for the development of a democratic system on the globe, while ensuring that democratic states trapped by globalisation can retain their sovereignty by prioritising a legitimate entity that is acceptable to all participants. Both problems are significant in their own right, and without a solution, a framework for security cannot be established either. More precisely, security in the traditional sense (security of a given territory) can be guaranteed, but only for a time, according to historical experience. However, higher levels of integration are unthinkable, and without it, there is no chance of addressing the challenges effectively.

CONCLUSION

My interpretation is that our need to create security comes from an a priori source. Its framework is determined by the group size characteristic of primates, and its content is saturated with psychological mechanisms that have evolved through evolutionary adaptation. In our increasingly complex social relations, our insistence on systematic thinking stems from and can be traced back to the unchanging need for a value-based order. I have called this claim the idea of order, which, as an expression of these determinations at the level of thought, can be considered a construction standing on the pedestal of current reality.

However, in the diversity of civilisations and cultures, the original patterns of the source that appears as the idea of order are rarely clearly visible. The more complex the conditions of existence that delimit the daily lives of human communities, the more transversal the relationship between the need and the act aimed at satisfying it becomes, and the greater the resource requirements for achieving security within a given framework will be. The fact of this causes a legitimation problem, the impact of which is amplified by globalization, the typical mode of operation of the world organised according to system-level and network-like patterns.

Democracy, which can be considered the optimised mode of operation of the developed world, is in a legitimacy crisis. Democratic countries, as well as communities with other arrangements and different levels of conditioning, at different stages of development,

have become responsible for the emergence of challenges that are far greater than those that humanity is globally prepared to overcome. While previously there was no global threat of anthropogenic origin, today not only has a new form of these challenges emerged, but one of them – climate change – has emerged, the consequences of which are partly irreversible and can only be tackled by calculating a certain realistic loss that can be planned.

In short, we can easily lose our ability to take back control over the area of the future that we were able to shape earlier and make corrections. The individual actions and capabilities of countries are not enough, and international organisations are not effective enough. And while there is certainly a reserve in the system of cooperation, it is difficult to say at this stage to what extent the level of global capacity to act can be meaningfully raised by mobilising these reserves.

It is therefore worth reflecting on how to go beyond the boundaries that limit our traditional solutions, which today are at the level of real policy. Or, more precisely, in addition to real policy responses, such as improving the quality and effectiveness of multilateral cooperation, innovative solutions must be sought to develop the right level of global capacity to act.

In my view, therefore, these are the circumstances that will have a decisive impact on the challenges of law enforcement in the 21st century.

REFERENCES

ALBRECHT, H.-J. 2006. A biztonságkoncepció átalakulása és ennek következményei az európai bel- és jogpolitikára. [The transformation of the security concept and its implications for European home affairs and justice policy]. In *Belügyi Szemle.* [Internal Affairs Review]. Vol. 54, No. 2, 2006. pp. 3–26.

BALLA, Z. 2017. *A rendészet alapjai és egyes ágazatai*. [The basics of law enforcement and specific sectors thereof]. Budapest: Dialóg Campus Kiadó, 2017. 95 p. ISBN 978-615-5764-59-2.

BALOGH, I. 2013. Biztonságelméletek. [Theories of Security]. In *Nemzet és Biztonság.* [Nation and Security]. Vol. 6, No. 3-4, 2013. pp. 36–56. ISSN: 2559-8651.

BAYLIS, J. – SMITH, S. – OWENS, P. 2020. *The Globalization of World Politics: An Introduction to International Relations.* Oxford: Oxford University Press, 2020. 617 p. ISBN 978-0-19-882554-8.

BERECZKEI, T. 2008. *Evolúciós pszichológia.* [Evolutionary Psychology]. Budapest: Osiris Kiadó, 2008. 542 p. ISBN 978-963-276-006-3.

BESENYEI, L. 2017. Exponenciálisan gyorsuló idő - exponenciálisan növekvő biztonsági kockázat. Világmodell-szemléletű kitekintés a 21. század biztonsági kihívásaira. [Exponentially accelerating time – exponentially increasing security risk]. A global model approach to the security challenges of the 21st century]. In *Biztonsági kihívások a 21. században*. [Security Challenges in the 21st Century]. Budapest: Dialóg Campus Kiadó, 2017. pp. 523–543. ISBN 978-615-5680-50-2.

BÍRÓ, G. 2003. *Bevezetés a nemzetközi politikai viszonyok tanulmányozásába.* [An introduction to the study of international political relations]. Budapest: Osiris Kiadó, 2003. 396 p. ISBN 963-389-331-3.

BUZAN, B. – WEAVER, O. – DE WILDE, J. 1998. *The new framework for analysis.* London: Lynne Rienner Publishers, 1998. 239 p. ISBN 1-55587-784-2.

CIELESZKY P. 2021. A rend eszméje 2. [The idea of order 2]. In *V. Turizmus és Biztonság Nemzetközi Tudományos Konferencia Tanulmánykötet.* [V. Tourism and Security International Scientific Conference Volume of Studies and Essays]. Nagykanizsa: Pannon Egyetem, 2021. pp. 18–30. ISBN 978-963-396-172-8.

DIAMOND, L. 2015. Facing Up to the Democratic Recession. In *Journal of Democracy.* Vol. 26, No. 1. 2015. pp. 141–155. Available at: <https://doi.org/10.1353/jod.2015.0009> Accessed: 2023. 01. 22.

DOYLE, M.W. 1983a. Kant, Liberal Legacies, and Foreign Affairs. In *Philosophy&Public Affairs*. Vol. 12, No. 3, 1983. pp. 205–235. Available at: <https://www.jstor.org/stable/2265298> Accessed: 2023. 01. 22.

DOYLE, M.W. 1983b. Kant, Liberal Legacies, and Foreign Affairs 2. In *Philosophy&Public Affairs*. Vol. 12, No. 4, 1983. pp. 323–353. Available at: <https://www.jstor.org/stable/2265377?refreqid=excelsior%3A97d4cc9ec87790df97d11788e0ff90be> Accessed: 2023. 01. 22.

EISENHOWER, D.D. 1961. *Eisenhower Farewell Address "Military Industrial Complex".* [online]. In Youtube. 2016. Available at: https://www.youtube.com/watch?v=OyBNmecVtdU Accessed: 2023. 01. 22.

European Commission. *2020. EU security union strategy.* [Official Website] Available at: <https://eur-lex.europa.eu/HU/legal-content/summary/eu-security-union-strategy.html> Accessed: 2023. 01. 22.

FINSZTER, G. 2018. *Rendészettan.* [Law Enforcement Studies]. Budapest: Dialóg Campus Kiadó, 2018. 495 p. ISBN 978-615-5845-94-9.

FINSZTER, G. – SABJANICS, I. 2017. *Biztonsági kihívások a 21. században.* [Security Challenges in the 21st Century]. Budapest: Dialóg Campus Kiadó, 2017. 838 p. ISBN 978-615-5680-50-2.

GÄRTNER, H. 2007. *Nemzetközi biztonság.* [International Security]. Budapest: Zrínyi, 2007. 229 p. ISBN 978-963-327-443-9.

GAZDAG, F. – REMEK, É. 2018. *A biztonsági tanulmányok alapjai.* [Basics of security studies]. Budapest: Dialóg Campus Kiadó, 2018. 282 p. ISBN 978-615-5845-87-1.

GAZDAG, F. – TÁLAS, P. 2008. A biztonság fogalmának határairól. [On the limits of the concept of security]. In *Nemzet és Biztonság.* [Nation and Security]. Vol. 1. No. 1, 2008. pp. 3–9.

GILENS, M. – PAGE, B.I. 2014. Testing Theories of American Politics: Elites, Interest Groups, and Average Citizens. In *Perspectives on Politics*. Vol. 12, No. 1, 2014. pp. 564–581. Available at: https://doi.org/10.1017/S1537592714001595 Accessed: 2023. 01. 22.

HANS-*Peter – M.,* SCHUMANN*, H. 1998. A globalizáció csapdája.* [The Global Trap]. Budapest: Perfekt Kiadó, 1998. 352 p. ISBN 963-394-313-2.

IMMANUEL, K. 2019. *Az örök béke.* [Perpetual peace]. Budapest: Helikon Kiadó, 2019. 78 p. ISBN 978-963-479-298-7.

IRK, F. 2012. *Kétkedő kriminológia - A rizikótársadalom kriminálszociológiája.* [Skeptical criminology - Criminal sociology of the risk society]. Miskolc: Bíbor Kiadó, 2012. 438 p. ISBN 978-963-9988-37-8.

KAGAN, R. 2015. *Made in America.* Budapest: Antall József Tudásközpont, 2015. 168 p. ISBN 978-615-5559-00-6.

KRASNER, S.D. 1999. *Sovereignty: Organized Hypocrisy*. Princeton: Princeton University Press, 1999. 280 p. ISBN 978-0-691-00711-3.

MULLEN, A. 2010. Twenty years on: the second-order prediction of the Herman-Chomsky Propaganda Model. In *Media, Culture & Society*. Vol. 32, No. 4, 2010. pp. 673–690. Available at: <https://doi.org/10.1177/0163443710367714> Accessed: 2023. 01. 22.

NOVÁKY, E. – S. GUBIK, A. 2017. A bizonytalanság kezelése a jövőkutatásban. [Managing uncertainty in futures research]. In *Biztonsági kihívások a 21. században*. [Security Challenges in the 21st Century]. Budapest: Dialóg Campus Kiadó, 2017. pp. 497–523. ISBN 978-615-5680-50-2.

Our Word in Data. 2021. *Numbers of autocracies and democracies* [online] Available at: <https://ourworldindata.org/grapher/numbers-of-autocracies-and-democracies> Accessed: 2023. 01. 22.

POKOL, B. 2014. Globális uralmi rend és állami szuverenitás. [Global governance order and state sovereignty]. [online]. Budapest: Magyar Tudományos Akadémia, 2014. 31 p. ISSN: 2064-4515. Available at:<http://real.mtak.hu/121166/1/2014_13_Pokol.pdf > Accessed: 2023. 01. 22.

POPPER, P. 2021. *Hogyan válasszunk magunknak sorsot?* [online]. Available at: <https://www.facebook.com/nyitottakademia/photos/a.179542955401946/3727354283954111/> Accessed: 2023. 01. 22.

PUZZANGHERA, J. 2014. 85 richest people own as much as bottom half of population, report says. [online]. In *Los Angeles Times.* Available at: <https://www.latimes.com/business/la-fi-mo-oxfam-world-economic-forum-income-inequality-20140120-story.html> Accessed: 2023. 01. 22.

RÁCZ, G. 2018. A demokratikus béke elmélete. [The theory of democratic peace]. In *Nemzet és Biztonság – Biztonságpolitikai Szemle.* [Security Policy Review]. Vol. 11, No. 3, 2018. pp. 127–133. ISSN: 2559-8651.

REMEK, É. 2017. Az EBESZ I. Világrend, biztonság, nemzetközi szervezetek, elméletek. [OSCE I World order, security, international organizations, theories]. In *Hadtudományi Szemle.* [Military Science Review]. Vol. X, No. 2. 2017. pp. 126–142. Available at: http://archiv.uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2017/2017_2/17_2_bp_remek_1.pdf Accessed: 2023. 01. 22.

RODRIK, D. 2021. *The inescapable trilemma of the world economy.* [online]. Available at: <https://rodrik.typepad.com/dani_rodriks_weblog/2007/06/the-inescapable.html> Accessed: 2023. 01. 22.

ROTHE, D.L. – COLLINS, V.E. 2018. Consent and Consumption of Spectacle Power and Violence. In *Critical Sociology*. Vol. 44, No. 1, 2018. pp. 15–28. Available at: <https://doi.org/10.1177/0896920515621119> Accessed: 2023. 01. 22.

SZENES, Z. 2013. Akadémiai viták a hadtudomány struktúrájáról. [Academic debates on the structure of military science]. In *Hadtudomány.* [Military Science]. Vol. XXIII, No. 3-4, 2013. pp. 59–66. ISSN: 1215-4121.

The Economist Group. 2021. *Democracy Index 2019 (Annual Report)*. [online]. Available at: <https://www.eiu.com/topic/democracy-index/> Accessed: 2023. 01. 22.

VARGA, G. 2015. A szuverenitás különböző megközelítései és jelentéstartalma. [Different approaches to sovereignty and its meaning]. In *Nemzet és Biztonság.* [Nation and Security]. Vol. 8, No. 1, 2015. pp. 30-38.

VIDA, Cs. 2013. A biztonság és a biztonságpolitika katonai elemei. [Military elements of security and security policy]. In *Nemzetbiztonsági Szemle.* [National Security Review]. Vol. I., No. 1. 2013. pp. 87–105. Available at: <https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/10197> Accessed: 2023. 01. 22.

Péter CIELESZKY, PhD Student

https://orcid.org/0000-0001-7755-3410

University of Public Service

H-1083 Budapest, Ludovika tér 2.

+36 20 466 53 87

cieleszky.peter@uni-nke.hu

DOI: https://doi.org/10.52651/vr.a.2023.3.21-37
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2023, Number 3, Page 21-37

INFORMATION AND MISINFORMATION IN TERMS OF THEIR IMPACT ON THE YOUNG GENERATION

Petr JEDINÁK, Iva BORSKÁ

ARTICLE HISTORY

Submitted: 05. 09. 2023
Accepted: 06. 12. 2023
Published: 31. 12. 2023

ABSTRACT

The paper deals with the form of information, specifically misinformation, on our young generation. It describes how misinformation affects their attitudes and behavior in everyday life. The article highlights the role of information in today's world.
The paper presents the results of the research, the target group of which was the studying young generation over 19 years old. Data collection took place in 2022 using the method of questioning the survey with subsequent statistical evaluation. The main goal of this research is to find out the abilities of this target group in the area of verifying the truth of information. The research was aimed at obtaining an answer to the question of how the young generation orients itself in the media environment. An important part of the research was the determination of respondents' attitudes towards misinformation and their behavior when dealing with misinformation. Statistical analysis was performed using adequate mathematical and statistical procedures.

KEYWORDS

Disinformation, propaganda, misinformation, research.

INTRODUCTION

The increase in disinformation goes hand in hand with the increase in information. But how does today's young generation perceive misinformation? In the contribution, we present some research that we carried out in 2022. In our research, we focused on the analysis of the attitudes of the young generation towards disinformation, their knowledge and skills in working with disinformation, we were interested in the perception of education in the field of media literacy, as well as the attitudes of the young generation to the free dissemination of information.

1 INFORMATION AND DISINFORMATION

The amount and easy availability of information in today's society brings positives in the form of its efficient and quick use. On the other hand, the amount of available information makes it difficult to quickly navigate through the amount of information, the need for a quick search for relevant, valid and up-to-date information increases and thus limits the possibilities of its optimal use. This causes different approaches/reactions of people to information (Mleziva 2004, p. 12):

- with an overall reduced interest in information, caused precisely by its excessive amount and easy availability,
- with a general mistrust of information or, conversely, uncritical acceptance of information that is in line with the individual's opinions,
- with searching and receiving interesting or even sensational information, despite its low degree of probability
- not distinguishing the importance, function and meaning of individual information (Mleziva 2004, p. 12).

Consequently, there is a need to distinguish between true information and false information. The so-called quality information, i.e. information that expresses the actual verifiable state of affairs, is considered to be true information (Kuchaříková, 2019, p.16). Quality information can be described by the following attributes (Mleziva, 2004, p. 42-43):

- Validity – i.e. the degree of agreement in which the given information describes the fact to which it relates.
- Communicability – i.e. the potential of verbal description of reality, includes
  - *clarity,*
  - *accuracy of expression,*
  - *clarity,*
  - *logic*
  - *clarity with regard to the potential recipient.*
- Effectiveness – i.e. scope with respect to the purpose it is desired to achieve. An insufficient range reduces the informational value of the message, an excessive range reduces clarity.
- Timeliness – i.e. timeliness at the time of presenting the information premature presentation of information may lead to incompleteness and inaccuracy of the information, delayed communication of information can make the presented information unattractive (loss of its interest, i.e. its out-of-dateness, or falsity.
- Correctness – i.e. truthfulness, objectivity, agreement with reality.
- Verifiability of truth and validity.

Disinformation is defined as "*false, deceptive, false information that aims to influence the judgment and opinion of an individual, several persons or the entire society.*" Nutil (2018. p. 18). Disinformation is intentionally created information that is spread in connection with influencing public opinion. Disinformation is intentionally created information that is spread in connection with influencing public opinion(Wardle, 2017, online).

Misinformation refers to the dissemination of false information without intentional impact on the recipient (Wardle, 2017, online). The difference between disinformation and misinformation is that disinformation is false information spread intentionally, misinformation is false information spread without knowing that it is a lie. This is also confirmed by Definition of misinformation by the Ministry of the Interior of the Czech Republic: "*Misinformation is incorrect or misleading information that is neither systematically nor intentionally disseminated with the aim of influencing decision-making or the opinions of those who receive it*." (Ministry of the Interior of the Czech Republic, online).

The Ministry of the Interior of the Czech Republic points out the danger of disinformation in that "*disinformation content does not undermine the authority of, for example, one specific politician or political party, but often causes mistrust towards the media as such, towards the political system or democracy itself. Moreover, they inspire apathy, as they spread the idea that "nothing can be trusted" and "nothing can be done about it", because everything is in the hands of the all-powerful gray eminences*." (Ministry of the Interior of the Czech Republic, online).

Information, misinformation, disinformation belong to key concepts in media literacy education. Media literacy can be considered as "*one of the conditions for the successful socialization of an individual, which has a double form*". These are the components (Jirák, 2002, p. 72):

- acquiring knowledge that is important for obtaining the so-called critical distance - it is a defense against the effects of the media, which are not desirable, obtaining knowledge that will lead to maximum use of the potential of information received from the media.
- Media literacy has two dimensions (Jirák, 2002, p. 72):
- Knowledgeable - what an individual should master in order to be considered media literate (e.g. the role of the media in the social context, media history, etc.)
- Skilled - focused on the ability to analyze received messages (e.g. verifying information, evaluating credibility, comparing with other received messages).

Relatively well-known research focused on the field of disinformation in the Czech Republic includes the 2019 Survey of Public Opinion on the Issue of Disinformation conducted by the Center for Public Opinion Research of the Institute of Sociology of the Academy of Sciences of the Czech Republic for the Ministry of the Interior of the Czech Republic.

Another research study focused on the spread of misinformation is News in the Digital Age 2020, produced by the Independent Journalism Foundation with research agency Nielsen Atmosphere.

2 RESEARCH

The aim of the conducted research was to map the perception of disinformation among the young generation in the Czech Republic, in terms of attitudes towards disinformation, knowledge and skills in working with disinformation, in terms of the perception of education in the field of media literacy and in terms of attitudes towards the free dissemination of information. Questionnaire methods were used to collect data.

2.1 Research methodology

Research object: Disinformation.
Research subject: Perception of disinformation by the young generation.
Respondents: Men and women living in the Czech Republic aged between 20 and 34.
Research method: Questionnaire investigation, with subsequent mathematical-statistical evaluation.

2.2 Questionnaire

Based on a qualitative analysis of the professional literature, a non-standardized (original) questionnaire was designed. The questionnaire was created in a printed form, which was compiled and published through the university computer network. The questionnaire consisted of a total of 35 questions, 30 of which were closed.

The questionnaire was composed in three parts. The first part contained the identification features of the respondents (gender, age, number of years of experience). The second part of the questionnaire was made up of a table showing the way to fill in the questionnaire (four-point Likert scale; the respondent is required to express the degree of agreement or disagreement with various statements relating to a certain attitude. The answers are summarized in a defined manner and the result is proportional to the individual's knowledge of the reflected topic.

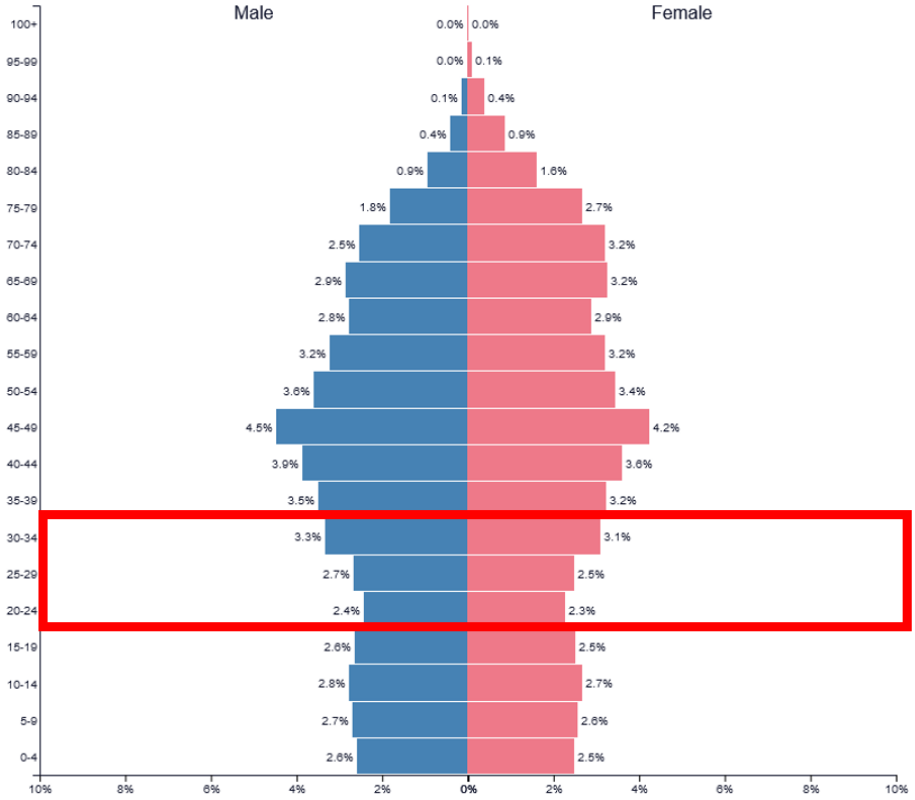
The third part of the questionnaire form represented the investigative part of the questionnaire investigation. The investigative part consisted of questions (statements) of the research investigation focused on correct knowledge of information security (the respondent expressed the degree of agreement or disagreement with the given statement).

2.3 Preliminary research (piloting)

Before the research itself, a small pilot probe was carried out, the purpose of which was to verify the comprehensibility of the questionnaire and to verify the statements for the part measuring the respondents' attitudes. As part of the pre-research, answers were obtained from 37 men and 24 women. The developed questionnaire was corrected in terms of validity (reformulation of some unclear questions, omission of questions in which all respondents only declared an agreeing or disagreeing position, etc.). Each participant's total score was calculated and each test item was subsequently correlated with this total score. Items that showed a low correlation were discarded from the test questions. The remaining questions were subsequently administered to the respondents as part of the research survey.

2.4 Respondents

In terms of methodology, a quota selection of respondents was used in terms of gender and age structure. The selection of respondents was based on public (Graph 1) data from the address (URL1, 2023). According to these available statistics, the population is divided by gender, with the indicated age categories after 5 years. For this reason, the population of the age range of 20-34 years was considered to be the young generation.



Graph 1 Population structure of the Czech Republic
Source: (URL, 2023)

2.5 Collection, processing and control of data

During the data collection of this period itself, 826 questionnaires were received. Subsequent computer processing resulted in the rejection of 63 questionnaires (7.7% of the total number of questionnaires received) due to incomplete completion. We therefore used a total of 763 questionnaires for statistical processing.

All questionnaires were subsequently recoded into the MS Excel 2010 program so that their statistical analysis was possible. A data matrix was created, which was imported into the Statistica v.10 software environment and subsequently analyzed in this environment. Adequate mathematical and statistical procedures, which are the content of this software environment, were used for data processing.

2.6 Achieved results

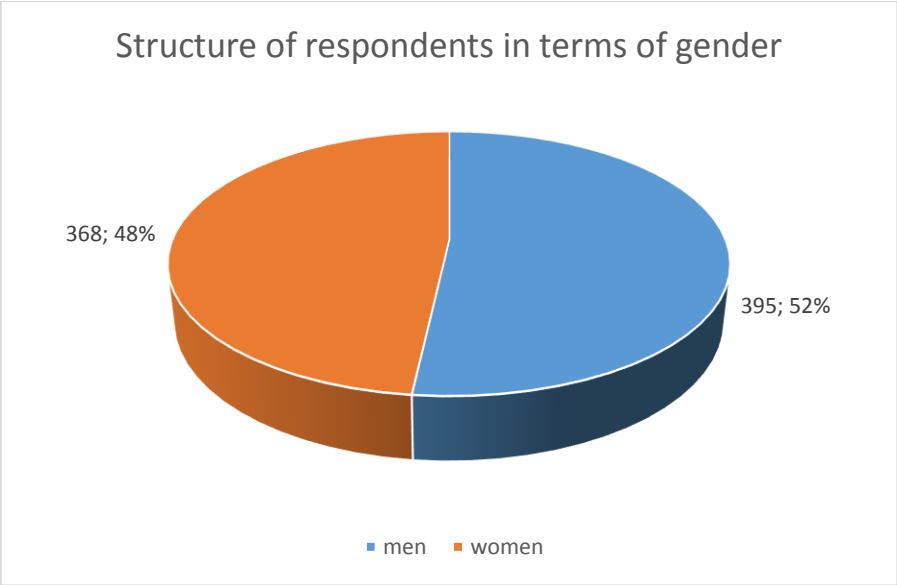
The representation of respondents in terms of age is shown in Graph 2 below, the basic statistical data of respondents is presented in Table 1.

Table 1 Basic statistical data of respondents

Age	
Mean	27,34600262
Stasndard error	0,170454788
Median	28
Modus	25
standard deviation	4,708379656
Sample variance	22,16883899
Kurtosis	-1,328109328
Skewness	-0,113884782
Range	14
Minimum	20
Maximum	34
Count	763

Source: own research

Out of the total sample of 763 respondents, men predominate, numbering 395 (52%) over women numbering 368 (48%). The structure of respondents in terms of age is shown in Graph 2.



Graph 2 Structure of respondents in terms of gender

Source: own research

In terms of gender, the group of women can be described using the following parameters (Table 2):

Table 2 Basic statistical data of women

Age	
Mean	27,18206522
Stasndard error	0,247017538
Median	26
Modus	25
standard deviation	4,738617979
Sample variance	22,45450036
Kurtosis	-1,400853629
Skewness	-0,014272466
Range	14
Minimum	20
Maximum	34
Count	368

Source: own research

In terms of gender, the group of men can be described using the following parameters (Table 3):

Table 3 Basic statistical data of men

Age	
Mean	27,49873418
Stasndard error	0,235520062
Median	28
Modus	34
standard deviation	4,680868657
Sample variance	21,91053139
Kurtosis	-1,23966204
Skewness	-0,20849438
Range	14
Minimum	20
Maximum	34
Count	395

Source: own research

The statistical analysis of the data was processed in categories:

- Attitudes towards misinformation
- Knowledge and skills in working with disinformation
- Media literacy education
- Attitudes towards the free dissemination of information

Attitudes towards disinformation were tested using five closed-ended questions that were assigned a value using the assigned scale. Subsequently, a summary value was determined from the obtained data, to which statistical tests were applied.

A research question was set for testing:

RQ1: Do attitudes toward disinformation differ by gender?

Research question RQ1 was tested using the working hypothesis (H01), with an alternative hypothesis (HA1) linked to it:

H01: *Attitudes towards disinformation do not differ depending on the gender of the respondents.*

HA1: *Attitudes towards disinformation differ by gender.*

In the collected research sample, the assumptions of the use of statistical methods were verified, especially normality (Table 4) and homoscedasticity (Table 5). In the case of multivariate random samples, the assumption that the data come from a multivariate normal distribution plays a major role. Testing for multivariate normality is a rather complicated task (Meloun, Militký, 2012, p. 49).

Table 4 Results of normality testing (own research)

Testing for normality (attitudes towards disinformation)			
Kolmogorov-Smirnov K-S test	d = 0,12051	p < 0,1	Normality **rejected**
Shapiro-Wilk´s W-test	w = 0,96787	p = 0,0000	Normality **rejected**

Source: own research

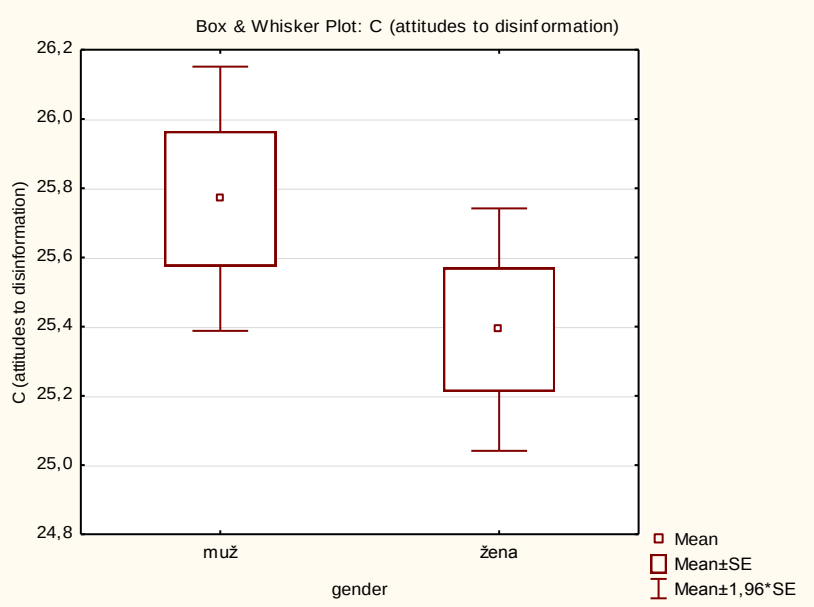
Table 5 Results of homoscedasticity testing (own research)

Testing for homoscedasticity (attitudes towards disinformation)			
F = 2,064773	p = 0,00000	gender	homoscedasticity **rejected**

Source: own research

Considering the received testing results, it can be stated that the conditions for the use of parametric mathematical-statistical methods are not met, therefore non-parametric tests were used in the data analysis. The Mann–Whitney U test was used to test the significance of two independent means.

For research question RQ1 (difference in perception of misinformation attitudes depending on gender), we depicted a box diagram in Graph 3.



Graph 3 Attitudes of men (left) and women (right) to misinformation

Source: own research

As can be seen from the graph (Graph 3), men incorporate working with disinformation into their lives more than women. To verify the statistical significance of this difference, we used the Mann-Whitney U test (Table 6).

Table 6 Results of testing differences depending on gender (own research)

Attitudes towards disinformation				
	U	Z	p	
attitudes towards disinformation	69883,5	0,919091	0,358	Hypothesis H01 **accepted**

Source: own research

From the received results, we state that at the 5 percent level of significance we accept the working hypothesis H01, i.e. there is no statistically significant difference in the attitudes of men and women towards disinformation.

Subsequently, we proceeded to test knowledge and skills in working with disinformation. This category was surveyed using 7 closed questions that were assigned a value using an assigned scale. Subsequently, a summary value was determined from the obtained data, to which statistical tests were applied.

A research question was set for testing:

RQ2: Do knowledge and skills in dealing with disinformation differ by gender?

The research question RQ2 was tested using the working hypothesis (H02), and an alternative hypothesis (HA2) is linked to it:

H02: *Knowledge and skills in dealing with disinformation do not differ depending on gender.*

HA2: *Knowledge and skills in dealing with disinformation differ by gender.*

In the collected research sample, the assumptions of the use of statistical methods were verified - normality (Table 7) and homoscedasticity (Table 8).

Table 7 Results of normality testing (own research)

Testing for normality (Knowledge and skills in working with disinformation)			
Kolmogorov-Smirnov K-S test	d = 0,11298	p < 0,1	Normality **rejected**
Shapiro-Wilk´s W-test	w = 0,97533	p = 0,0000	Normality **rejected**

Source: own research

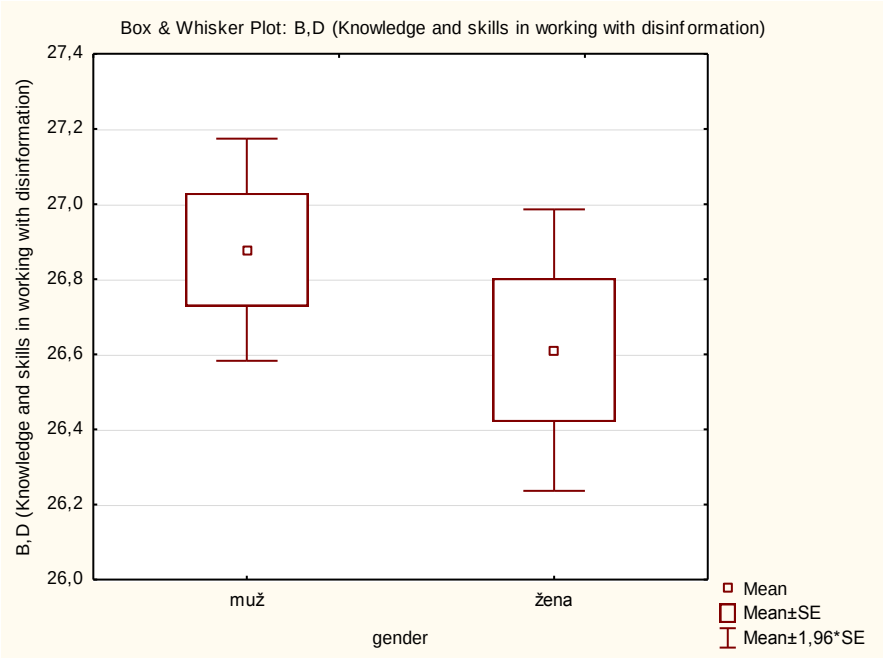
Table 8 Results of homoscedasticity testing (own research)

Testing for homoscedasticity (Knowledge and skills in working with disinformation)			
F = 2,214692	p = 0,00000	gender	homoscedasticity **rejected**

Source: own research

Considering the received testing results, it can be stated that the conditions for the use of parametric mathematical-statistical methods are not met, therefore non-parametric tests were used in the data analysis. The Mann–Whitney U test was used to test the significance of two independent means.

For research question RQ2 (difference in perception of knowledge and skills in dealing with disinformation depending on gender), we depicted a box diagram in Graph 4.



Graph 4 Knowledge and skills of men (left) and women (right) when working with disinformation

Source: own research

As can be seen from the graph (Graph 4), men achieve higher knowledge and skills when working with misinformation. To verify the statistical significance of this difference, we used the Mann-Whitney U test (Table 9).

Table 9 Results of testing differences depending on gender (own research)

Knowledge and skills in working with disinformation				
	U	Z	p	
Knowledge and skills in working with disinformation	68061,5	1,518013	0,129012	Hypothesis H02 **accepted**

Source: own research

From the received results, we state that at the 5 percent level of significance we accept the working hypothesis H01, i.e. there is no statistically significant difference in the assessment of knowledge and skills in working with disinformation depending on gender.

Media literacy education was tested using five closed-ended questions that were assigned a value using an assigned scale. Subsequently, a summary value was determined from the obtained data, to which statistical tests were applied.

A research question was set for testing

RQ3: Do attitudes toward media literacy education differ by gender?

Research question RQ3 was tested using the working hypothesis (H03), with an alternative hypothesis (HA3) linked to it:

H03: *attitudes towards media literacy education do not differ depending on the gender of the respondents.*

HA3: *respondents' attitudes towards media literacy education are different depending on gender.*

In the collected research sample, the assumptions of the use of statistical methods were verified - normality (Table 10) and homoscedasticity (Table 11).

Table 10 Results of normality testing (own research)

Testing for normality (attitudes towards media literacy education)			
Kolmogorov-Smirnov K-S test	d = 0,13259	p < 0,1	Normality **rejected**
Shapiro-Wilk´s W-test	w = 0,96405	p = 0,0000	Normality **rejected**

Source: own research

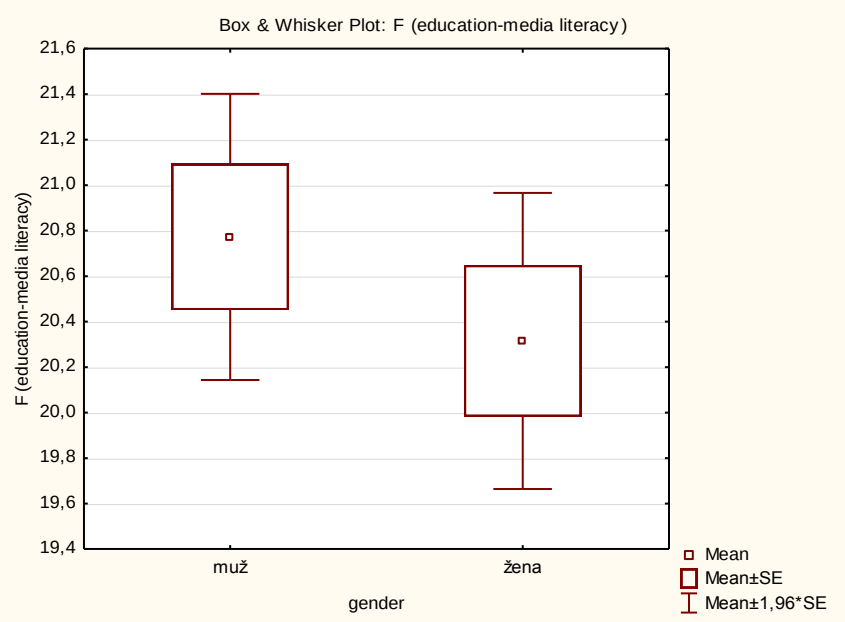
Table 11 Results of homoscedasticity testing (own research)

Testing for homoscedasticity (attitudes towards media literacy education)			
F = 1,464762	p = 0,00000	gender	homoscedasticity **rejected**

Source: own research

Considering the received testing results, it can be stated that the conditions for the use of parametric mathematical-statistical methods are not met, therefore non-parametric tests were used in the data analysis. The Mann–Whitney U test was used to test the significance of two independent means.

For research question RQ3 (difference in the perception of attitudes towards media literacy education depending on gender), we depicted a box diagram in Graph 5.



Graph 5 Evaluation of the education of men (left) and women (right) in the area of media literacy

Source: own research

As can be seen from the graph (Graph 5), men evaluate education in the field of media literacy better than women. To verify the statistical significance of this difference, we used the Mann-Whitney U test (Table 12).

Table 12 Results of testing differences depending on gender (own research)

attitudes towards media literacy education				
	U	Z	p	
attitudes towards media literacy education	69862	0,926159	0,354364	Hypothesis H03 **accepted**

Source: own research

From the received results, we state that at the 5 percent level of significance we accept the working hypothesis H01, i.e. there is no statistically significant difference in attitudes towards education in the field of media literacy depending on gender.

Attitudes towards the free dissemination of information were tested using four closed questions, which were assigned a value using an assigned scale. Subsequently, a summary value was determined from the obtained data, to which statistical tests were applied.

A research question was set for testing

RQ4: Do Attitudes to the free dissemination of information differ by gender?

Research question RQ4 was tested using the working hypothesis (H04), with an alternative hypothesis (HA4) linked to it:

H04: *Attitudes towards the free dissemination of information do not differ depending on the gender of the respondents.*

HA4: *Attitudes towards the free dissemination of information differ by gender.*

In the collected research sample, the assumptions of the use of statistical methods were verified - normality (Table 13) and homoscedasticity (Table 14).

Table 13 Results of normality testing (own research)

Testing for normality (Attitudes towards the free dissemination of information)			
Kolmogorov-Smirnov K-S test	d = 0,11420	p < 0,1	Normality **rejected**
Shapiro-Wilk´s W-test	w = 0,96097	p = 0,0000	Normality **rejected**

Source: own research

Table 14 Results of homoscedasticity testing (own research)

Testing for homoscedasticity (Attitudes towards the free dissemination of information)			
F = 1,464762	p = 0,00000	gender	homoscedasticity **rejected**

Source: own research

Considering the received testing results, it can be stated that the conditions for the use of parametric mathematical-statistical methods are not met, therefore non-parametric tests were used in the data analysis. The Mann–Whitney U test was used to test the significance of two independent means.

For research question RQ4 (difference in the perception of attitudes towards the free dissemination of information depending on gender), we depicted a box diagram in Graph 6.

Graph 6 Evaluation of the attitudes of men (left) and women (right) towards the free dissemination of information

Source: own research

As can be seen from the graph (Graph 6), men prefer greater freedom and openness to the dissemination of information than women. To verify the statistical significance of this difference, we used the Mann-Whitney U test (Table 15).

Table 15 Results of testing differences depending on gender (own research)

Attitudes towards the free dissemination of information				
	U	Z	p	
Attitudes towards the free dissemination of information	62543,50	3,331870	0,000863	Hypothesis H04 **rejected**

Source: own research

From the received results, we state that at the 5 percent level of significance we reject the working hypothesis H0 about the agreement of attitudes towards the free dissemination of information, depending on gender, and accept the alternative hypothesis HA4 - men prefer greater freedom and openness to the dissemination of information than women, statistically significantly (at the 5 percent level of significance).

CONCLUSION

In their contribution, the authors focused on the problem of how young people approach misinformation. We were interested in their attitudes and behavior towards various information in everyday life. The goal was to find out if they can distinguish what disinformation is, and how they deal with it. To obtain the documents, we carried out our own research at the Police Academy of the Czech Republic in Prague.

The respondents were students of combined and face-to-face teaching in bachelor's and master's study programs. Students of the combined form were professionally included in the security forces of the Czech Republic and also officials working in the state and public administration. Of the 826 completed questionnaires received, we subsequently had to discard 63 questionnaires due to incompleteness. For the evaluation, we worked with data from 763 respondents. The representation of men and women was almost equal, 395 women and 368 men.

In the paper, we present the results of four research questions (RQ1 – RQ4) and the hypotheses established for them. We further advanced the results for discussion, within the framework of information subjects taught at the Police Academy of the Czech Republic in Prague. Students were also allowed to work on this topic in their bachelor's and diploma theses in the future. They have the opportunity to use the data obtained from this research, or to follow up and expand on it.

The conclusion can be drawn from the conducted research that today's youth can distinguish information from misinformation. Differences in perception of misinformation between men and women noted. Recommendations from the conducted research: With regard to the constant increase of misinformation in the public space, it is necessary to offer various forms of educational activities in the field of media literacy and to further monitor the perception of misinformation on the young generation in order to establish trends in this area.

REFERENCES

Definice dezinformací a propagandy. Ministerstvo vnitra České republiky. [online]. 2019 [cit. 2023-10-05]. Dostupné na internetu z: http://www.mvcr.cz/cthh/clanek/definice-dezinformaci-a-propagandy.aspx.

JIRAK, J. 2002. Základní půdorys mediální gramotnosti. In Hrachovcova, M. – Staněk, A. (eds.). Občanská výchova v globalizující se společnosti. Olomouc: Univerzita Palackého, s. 71 – 77.

KUCHAŘÍKOVÁ, M. 2019. Percepce a produkce pravdivých a nepravdivých informací v prostředí internetu jako součást mediální výchovy Diplomová práce. Olomouc: Univerzita Palackého v Olomouci, s.15.

MELOUN, M. – MILITKÝ, J. 2012. Interaktivní statistická analýza dat. Praha: Karolinum, 960 s. ISBN 9788024621739.

MLEZIVA, E. 2004. Diktatura informací: jak s námi informace manipulují. Plzeň: Aleš Čeněk, ISBN 80-86898-12-1.

NUTIL, P. 2018. Média, lži a příliš rychlý mozek: průvodce postpravdivým světem. Praha: Grada. ISBN 978-80-271-0716-2.

Populace. [online]. 2019 [cit. 2023-10-05]. Dostupné na internetu z: https://www.populationpyramid.net/czech-republic/2023/.

WARDLE, Claire. Fake news. It's complicated. First Draft [online]. 2017 [cit. 2023-10-05]. Dostupné z: https://firstdraftnews.org/fake-news-complicated/.

Tisková zpráva: Češi a dezinformace. [online]. 2021 [cit. 2023-10-05]. Dostupné z: https://www.nfnz.cz/aktuality/tiskova-zprava-cesi-a-dezinformace/.

Výzkum veřejného mínění k problematice dezinformací. [online]. 2019 [cit. 2023-10-05]. Dostupné z: https://www.mvcr.cz/chh/clanek/vyzkum-verejneho-mineni-k-problematice-dezinformaci.aspx.

PhDr. Petr Jedinák, Ph.D., MBA
Police Academy of the Czech Republic in Prague
Faculty of Security Management
Department of Management and Informatics
Lhotecká 559/7
143 01 Praha 4 Czech republic
Tel: +420 974 828 216
e-mail: jedinak@polac.cz

PhDr. Iva Borská, CSc.
Police Academy of the Czech Republic in Prague
Faculty of Security Management
Department of Management and Informatics
Lhotecká 559/7
143 01 Praha 4 Czech republic
Tel: +420 974 828 243
e-mail: iborska@polac.cz

DOI: https://doi.org/10.52651/vr.a.2023.3.38-58
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2023, Number 3, Page 38-58

ON DISINFORMATION AND PROPAGANDA IN THE CONTEXT OF THE SPREAD OF HYBRID THREATS

Radoslav IVANČÍK

ARTICLE HISTORY

Submitted: *12. 09. 2023*
Accepted: *06. 12. 2023*
Published: *31. 12. 2023*

ABSTRACT

Disinformation, propaganda, and hybrid threats are topics that, especially since Russia's annexation of Crimea in 2014 and even more so since last year's military invasion of Ukraine by Russian troops, resonate not only in professional but also in societal debates. Disinformation is one of the primary tools of propaganda and information warfare, and thus also the spread of hybrid threats through the press, television, radio, but especially through the Internet and social networks. For this reason, the author in the article, within the framework of interdisciplinary scientific research, using relevant scientific methods, with the aim of deepening the academic discourse in the subject area, deals with disinformation, propaganda and hybrid threats, pointing out that it is extremely important on the part of transnational organizations, democratic states and their competent institutions, including security forces, on the one hand, to take effective and efficient measures aimed at reducing the possibilities of their spread, and on the other hand, to support prevention and education in the field of media literacy and working with information.

KEYWORDS

Disinformation, propaganda, hybrid threats, information war

INTRODUCTION

Disinformation, propaganda, and hybrid threats are topics that, especially since Russia's annexation of Crimea in 2014 and even more so since last year's military invasion of Ukraine by Russian troops, resonate not only in professional but also in societal debates. Considering the current developments in the global and regional security environment and the security situation near and far around the borders of the European Union, and therefore also the borders of the Slovak Republic, it does not even look like these topics should disappear from the public discourse in the near future. On the contrary, their intensity increases in connection with new cases and events that reveal Russian interference in the

sovereign affairs of foreign states, especially North American and European democratic states. Typical examples of Russian interference are attempts to influence public discourses and moods in Western societies through disinformation campaigns conducted through the press, television, but especially through the Internet and social networks, especially in the run-up to important parliamentary or presidential elections. This was the case, for example, during the vote on the United Kingdom's exit or stay in the European Union in 2016, the American presidential elections in the same year and also in 2021, the French presidential elections in 2017 and 2022, the European Parliament elections in 2019 or the German parliamentary elections in 2021. Although the real impact of Russian disinformation campaigns on the final results of the referendum, or presidential and parliamentary elections is difficult to measure, it is indisputable that they had some influence on the decisions of the voters of the affected countries. And they still have, as the Russian Federation, through the spread of hybrid threats, tries to disrupt and negatively influence the functioning of democratic states, polarize individual societies, sow chaos among people, arouse insecurity and question democratic values, freedoms, and principles. Disinformation, propaganda, and hybrid threats are currently topics that need to be thoroughly investigated due to several negative aspects that are demonstrably not only on democratic societies. That is also why the author in the article, in the framework of interdisciplinary scientific research, using relevant scientific methods (especially analytical-synthetic method, content, critical and qualitative analysis, document study method, knowledge generalization method and others), with the aim of deepening the academic discourse in the subject area, and based on the works of renowned domestic (Kelemen, 2015, Hofreiter, 2019; Jurčák, 2016, 2018; Kazanský, Nečas, 2021) and foreign (Hoffman, 2007, 2009, Piwowarski, 2017; Snyder, 2018; Stoker, Whiteside, 2020; Darnton, 2020; Qualter 2020) authors deals with disinformation, propaganda and hybrid threats.

1 DEFINITION OF KEY TERMS

Given the fact that the issue of disinformation, propaganda and hybrid threats is today the subject not only of professional but also of numerous social discussions, in which many times there is a wrong definition, understanding or differentiation of individual terms, in the interest of the successful implementation of scientific research and the achievement of set research goals, it is necessary precise definition of basic terms. In the following subsections, individual key concepts will therefore be defined in a structure from the most general (broadest) term to the most specific, i.e., from hybrid war and hybrid threats, through information war to propaganda and disinformation.

1.1 Hybrid warfare and hybrid threats

"Hybrid war" is nowadays - mainly in connection with political, security or military topics, such as the ongoing conflict in Ukraine - a relatively often used term, whose clear and generally acceptable meaning or even real applicability in the scientific environment is not

fully agreed. In the public space, this term began to appear more often since 2014, primarily in connection with the Russian annexation of Crimea and the widespread support for the activities of paramilitary separatist groups in Ukraine. The very history of the term goes back several years and is connected with the work of Frank Hoffman. He sees the concept of hybrid warfare as *"a fusion of standard and non-standard tactics used to achieve military objectives within an armed conflict"* (Hoffman, 2007, p. 7). At the same time, according to him, *"hybrid war represents more than just a conflict between states and other armed groups. It is an application of different forms of conflict that distinguish hybrid threats or hybrid conflicts. This is especially true since hybrid wars can be led both by states and by various non-state actors"* (Hoffman, 2009, p. 35).

Hybrid war can also be understood as *"a wide spectrum of hostile activities in which the role of the military component is rather small, because political, informational, economic and psychological influence becomes the main means of conducting the battle. Such methods help to achieve significant results: territorial, political, and economic losses of the enemy, chaos, and disruption of the system of exercising state power and weakening of society's morale"* (Manko - Mikhieiev, 2018, p. 13). It can also be characterized as *"a set of lethal and non-lethal means that a state or non-state actor uses to assert its interests against the will of another actor. At the same time, hybrid war combines several ways of conducting the battle: classic military operations, operations in cyberspace or cyber-attacks, espionage, spreading false information with the aim of influencing the enemy's public opinion, etc."* (Danyk et al., 2017, p. 6)

Another of the definitions says that "hybrid war is an armed conflict led by a combination of non-military and military means with the aim of their synergistic effect to force the adversary to take such steps that it would not take on its own. At least one side of the conflict is the state. The main role in achieving the goals of the hybrid war is played by non-military means in the form of information and psychological operations, propaganda, economic sanctions, embargoes, criminal activities, terrorist activities and other subversive activities of a similar nature, which are conducted against the entire society, especially against its political structures, bodies state administration and self-government, the economy of the state, the morale of the population and the armed forces" (Kříž et al., 2015, p. 8).

Hybrid warfare is also defined as *"war led with the simultaneous, flexible, and highly adaptable use of both conventional and unconventional methods. Specific methods and means include the use of non-state actors, insurgent warfare, terrorism, political, economic information, and legal tools, but also the deployment of advanced weapon systems and operations in cyberspace"* (Řehka, 2017, p. 23). The merit of this concept is the absence of a clear line between war and a state of peace because many of these tools are commonly used by states to influence other actors, while armed violence, as one of the defining features of war, may not be present at all, or with a very limited intensity, in some phases. Among the key features of this concept is also a certain time limitlessness (in contrast to conventional war,

which can mostly be precisely defined in time) and the fact that informational and cyber effects on the enemy's population play a fundamental role (Řehka, 2017, p. 24).

Overall, it can be concluded that in the case of hybrid war, it is a way of conducting a modern armed conflict, which does not start with a shot and certainly not with a declaration of war, of which the attacked society does not initially know, does not even suspect or admit that it has been attacked and is in war. It includes a dynamic combination of military and non-military (political, diplomatic, economic, technical/technological, humanitarian, sabotage, terrorist, criminal, etc.) activities carried out by state and non-state actors, regular and irregular formations, using lethal and non-lethal means, disinformation, propaganda, sanctions and other tools, regular and irregular methods of combat and in the implementation of information, cyber and psychological operations.

As already indicated in the introduction of this sub-chapter, the concept of hybrid warfare has also met with criticism and is accepted somewhat ambivalently within the professional security community. It is criticized, on the one hand, that there is no clear and precise definition of the concept and that everyone imagines something different under it, and, on the other hand, that there is extensive overuse of it, especially in the last few years, which can lead to a certain emptying and unusability of the concept in professional, but also the political context (Reichborn-Kjennerud and Cullen 2016; Stoker and Whiteside, 2020). A harsher criticism questions the essence and meaning of the existence of the concept of hybrid war based on the premise that there has been some kind of fundamental change in the nature and character of war. According to Green (2020), the political nature and character of war has not fundamentally changed since the time of Clausewitz and his concept of war, and non-kinetic components in the form of cyber and information warfare are not new methods of war existing in themselves, but rather an extension of existing ways of waging war.

In any case, the effort to define the concept and the scientific discussion regarding the issue of hybrid war is extremely important from the point of view of scientific research despite the above-mentioned criticism of this concept. However, it should be perceived on a more general level as a reflection of a certain change in point of view or a change in the previous thinking about the possibilities of conducting a modern war. From the point of view of fulfilling the goals of this study, an essential factor is the increase in the use and importance of the role of disinformation within information, cyber and psychological operations implemented by state or non-state actors in order to influence the adversary in order to achieve their own goals.

Therefore, it seems more appropriate to use the concept of "hybrid threats", although even in this case - despite the growing interest in recent years and the developing academic and professional discussion about hybrid threats - there is no common unified and generally accepted definition of this category of threats. For that reason, it is possible to meet their multiple definitions. From the perspective of international organizations, NATO (2023) defines hybrid threats as *"a combination of military and non-military actions, as well as covert and overt means, including disinformation, cyber-attacks, economic pressure, the deployment of*

irregular armed groups and the use of conventional forces." Hybrid methods are used to blurring the lines between war and peace and seek to sow doubt in the minds of the target population. Their goal is to destabilize and undermine societies.

The European Union uses a broader definition according to which: *"Hybrid threats combine conventional and unconventional, military and non-military activities that can be used in a coordinated way by state or non-state actors to achieve specific political goals. Hybrid campaigns are multidimensional, combining coercive and subversive measures using conventional also unconventional tools and tactics. They are designed to be difficult to detect or attribute. These threats target critical vulnerabilities and seek to create confusion that would prevent quick and effective decision-making."* (EU, 2018) Hybrid threats can range from cyber-attacks on critical information systems, through the disruption of critical services such as energy supplies or financial services, to undermining public trust in government institutions or deepening social differences (EU, 2018).

The European Centre of Excellence for Countering Hybrid Threats characterizes hybrid threats as *"coordinated and synchronized action that deliberately targets the systemic vulnerability of democratic states and institutions through a wide range of means, for example activities that use detection and attribution thresholds, as well as various interfaces (war - peace, internal - external security, local - state and national - international), as well as activities aimed at influencing various forms of decision-making at the local (regional), state or institutional level and designed to support and/or fulfil the agent's strategic goals and at the same time they undermined and/or damaged the objective"* (Hybrid CoE, 2023). Experts from the Hague Centre for Strategic Studies characterize hybrid threats very simply as *"a spectrum of undesirable activities from violent to non-violent implemented in both the military and civilian spheres"* (HCSS, 2022).

In addition to the above-mentioned definitions, one can come across other definitions from several authors in the professional literature, which are, however, more or less identical. In general, it can therefore be concluded that hybrid threats represent a combination or set of various coercive and subversive activities using conventional and unconventional methods (diplomatic, economic, military, technological, subversive, criminal, terrorist, and others), which can be carried out by various state and non-state actors in a coordinated manner use to achieve specific goals without formally declaring war on the adversary.

1.2 Information warfare

"Information war" represents a concept that is very closely related to the dynamic development of human civilization, especially the general information and technological revolution and the unprecedented rapid development in the field of modern information and communication technologies, which, naturally, also manifested itself in the military sphere and influenced the way of conducting modern wars. Information warfare itself is essentially a general term covering several types of warfare that have certain common characteristics.

Probably the most essential of these features is (as the name implies) the emphasis placed on information, which in this type of conflict is taken as a key element necessary to achieve victory. Different authors explain the term information war in different ways, and therefore, similar to the previous terms, also in the case of information war, it is possible to find several different, more or less accurate definitions in the professional literature. However, there is no universal, unified, and generally accepted and used definition of the term information warfare.

The most general and probably the simplest definition understands information warfare as *"waging war in an information environment"* (Řehka, 2017, p. 63). Another definition refers to information warfare as *"the struggle for control over the information activities of the adversary and the effort to protect one's own"* (Bayer, 2006, p. 39). Another, more complex definition says that: *"Information warfare represents a wide range of activities, the tool or goal of which is information and information technology. These activities include, for example, the dissemination of disinformation, psychological operations, and cyber-attacks – disrupting and penetrating communication networks in order to obtain strategic information. These activities can take place even in times of peace without having to prevent any conflict at all. The main goal of information warfare is not to weaken the adversary from the outside, but to weaken, disorient and destabilize him from the inside"* (Darnton, 2006, p. 142).

The North Atlantic Treaty Organization (2020) considers information warfare as *"an operation conducted to gain an informational advantage over an adversary. It consists in controlling one's own space, protecting access to one's own information, and at the same time obtaining and using information of the adversary, destroying its information systems and disrupting information flows"*. Burns (1999) defines information warfare as *"a set of techniques involving the collection, transmission, protection, denial, disruption and degradation of information by which an actor maintains an advantage over an adversary"*. Kubeša (2013, p. 162) characterizes it as *"acting on the adversary at the strategic, operational and tactical level through information means to achieve a specific goal, continuously - in times of peace and war"*.

At a higher level of abstraction, information warfare is understood as ideological influencing of the adversary, while a wide range of tools are used for this purpose, such as disinformation, propaganda, but also diplomacy or military coercion, etc. Information and knowledge have always been important in war, but the rapid increase in the amount of information and the mass spread of modern information and communication technologies have completely changed the operational environment in which modern warfare is conducted. Therefore, it is important to identify the domains in the information environment in which information operations and information warfare can take place. Specifically, it is a physical domain (infrastructure and people), an information domain (the content of the notification) and a specific domain represented by cyberspace. It is the use of cyberspace for

waging war and conducting information operations that is crucial from the point of view of information warfare (Řehka, 2017, p. 63)

Information warfare can take a variety of forms and use a variety of different tools, from purely military to civilian. Libicki (1995, p. 7) identifies 7 forms of information warfare: (a) command and control operations, (b) intelligence operations, (c) electronic warfare, (d) psychological warfare, (e) economic-information warfare, (f) hacker warfare and (g) cyber warfare. From this typology, the means of psychological warfare, which he understands as *"the use of information against the human mind"*, are important for the spread of disinformation.

Another important aspect is the fact that the information war has long gone beyond the borders of the military itself. And even more worrying is the fact that these borders are gradually being erased, even under the influence of the rapid development of new technologies. Thus, the traditional understanding of war is no longer sufficient in the understanding of information war, and based on the research results, it can be claimed that both society and individuals are already part of information war (albeit in the vast majority of cases unknowingly). Physical battlefields are increasingly moving into virtual space, while the primary goal is no longer to destroy the real physical infrastructure of the enemy, but to hit, destroy, knock out or at least disrupt the operation and functionality of his information and communication systems and networks, thereby disrupting the operation of his entire society (Ivančík, 2021, p. 150).

In addition to the above-mentioned definitions, also other definitions can be found in the professional literature, but they are more or less similar. In general, therefore, it can be concluded that information warfare represents a wide range of activities, including information, psychological and cyber operations, with the aim of ensuring the protection of own information, information flows and information and communication systems, disrupting (or destroying) the adversary's information and communication systems and networks, penetrate them, obtain and use his information, feed him with false, altered and deceptive information, and weaken, disorient and destabilize him from within.

1.3 Propaganda

In the case of the term "propaganda" - similarly as in the case of the key terms mentioned above - there is also no unified and generally accepted definition. It is one of the fundamental tools of psychological and informational influence not only on the own population, army and armed security forces, but also on the population, army and armed security forces of the enemy. Propaganda was already used in ancient times, but it became key especially during the Second World War and then later during the so-called Cold War. The very perception of the term "propaganda" has also undergone a certain historical development. While propaganda was previously perceived as a purely neutral concept,

nowadays its emotional colouring and perception by the public is strongly negative, which is why today it is used almost exclusively to describe the enemy's information activities. However, every state (not only in a state of war) uses some form of its own propaganda, but in the case of its own information operation, it replaces it with generally more acceptable terms such as strategic communication, information operation, etc.

Several definitions of propaganda can be found in the professional literature. For example, that *"propaganda is a deliberate, systematic effort to shape perception, manipulate cognition, and direct behaviour in order to achieve a response consistent with the propagandist's desired intent"* (Jowett - O'Donnell, 2012, p. 29). Another definition states that *"propaganda is the work of large organizations or groups to win over the public to their specific interests through the massive use of attractive arguments packaged to hide both their persuasive intent and the lack of evidence"* (Sproule, M.J., 1997, p. 51). To complement the definitions, Qualter (2020) states that, to be effective, propaganda must be seen, remembered and understood, and to be so, it must be adapted to the specific needs of the situation and the audience it is aimed at.

Řehka (2017, p. 65) perceives propaganda in the context of modern war as a necessity for success and defines it as *"an effort to influence people so that their thinking and behaviour change in a desired way in favour of the one for whom it is conducted"*. Táborský (2020, p. 21) understands propaganda as *"a deliberate attempt to make people think and behave in a desired way"*. Similarly, according to Kaničárová (2021), *"propaganda means the purposeful dissemination of true or fabricated information in an attempt to elicit a desired reaction in the audience"*. The National Security Analysis Centre explains propaganda as *"an activity that is aimed at spreading a certain idea, emphasizing only its positive aspects and disseminated to convince the audience of its correctness"* (Short Dictionary of Hybrid Threats, 2021).

From the above definitions, it can be concluded that propaganda is a form of communication that tries to influence the thinking or behaviour of the addressee in such a way as to suit the hidden intentions of the propagandist. For this purpose, the propagandist uses various direct or indirect means of communication, which he adapts to his intentions. Propaganda involves the deliberate distortion of facts or the use of half-truths and lies in order to manipulate the thinking and/or behaviour of recipients. However, the reality changed or completely created by the propagandist is always presented as true; the addressee should not know that he is being manipulated. For this reason, propaganda is seen as something negative.

1.4 Disinformation

Disinformation is one of the primary tools of propaganda and information warfare, and thus also the spread of hybrid threats. Although the term "disinformation", especially in connection with terms such as "information" or "hybrid" warfare, has only started to appear in larger numbers in the last few years, it is far from being a tool that was invented today.

Historically, the tactic of spreading deliberately false information in the ranks of the troops and among the enemy's population was already used in ancient times (Bittman 2020, p. 45), but the name and the current form of disinformation originated, as already mentioned, in the Soviet Union, for which - as stated Bittman (2020, p. 50) - *"deception, disinformation and vulgar, reckless lying have become an integral part of the system"*. It was here that the concept of "active measures" was invented, which meant the mass creation, use and dissemination of disinformation and the implementation of secret actions, the aim of which was, among other things, to divide the Western public, influence public opinion and discredit the local political leaders (Bittman 2020, p. 51).

From the point of view of definition - also on the basis of the above information - it is not surprising that, even in the case of disinformation, there is currently no unified and generally accepted definition of it, and therefore we can come across a relatively large number of definitions in the literature, differing primarily in which sectors or areas of the company does disinformation occur, or they apply. Despite their greater or lesser difference, the common feature of all used definitions is the fact that it is a deliberate modification of the provided information with the intention of influencing, deceiving, or misleading the addressees of this information.

According to the Short Dictionary of Hybrid Threats (2021): *"Disinformation is verifiably false, misleading, or manipulatively presented information that is intentionally created, presented, and disseminated with the clear intent to deceive or mislead, cause harm, or secure some gain (for example, political or economic). Disinformation often contains an element that is obviously true, which gives it credibility and can make it more difficult to detect. Disinformation does not include inadvertent reporting errors, satire, and parodies, nor biased reports and comments that are clearly marked as such"*.

In the Encyclopaedia of Sociology, disinformation is defined as *"any distorted, false information, used with the aim of influencing an individual or a certain group of people in a certain desirable way. Most of the time, it is primarily about creating a good or bad impression about a person, event, work, phenomenon, negotiation, etc. in the interest of political, ideological, or even purely private interests. It is often aimed at influencing public opinion, while it may have already been created with such an intention, but it may also arise accidentally or for another purpose, which may not be explicitly disinformation (e.g., when it is caused by taking a certain announcement out of its original context or placing it in other context)"*.

According to the Action Plan for Combating Disinformation, which was prepared jointly by the European Commission and the European External Action Service at the level of the European Union, and which was subsequently adopted by the European Parliament, *"disinformation is demonstrably false or misleading information created, presented and disseminated for the purpose of economic gain or intentionally deceiving the public and can cause public harm"* (European Commission, 2018). The key element, that is emphasized in this context in the document, is intent. The North Atlantic Alliance perceives disinformation as

"the intentional creation and dissemination of false and/or manipulated information with intent lie and/or mislead, with disinformation actors seeking to deepen divisions within and between allied countries and undermine people's trust in elected governments".

In the scientific and professional literature, one can come across several other definitions of the term disinformation, especially from authors who deal with the issue in their research or works. Based on the content analysis of individual works, it can generally be concluded that individual authors generally characterize disinformation as *"false, inaccurate or misleading information that is deliberately disseminated in order to achieve mainly political, economic or other goals"* (Freelon - Wells, 2020; Wardle - Derakhsham, 2017).

From the point of view of the spread of disinformation, the Internet and the emergence of social media gave modern propagandists a very effective tool for spreading disinformation. Information, and therefore also disinformation, can be spread here by absolutely anyone, while their truth, nor the credibility of the spreader, is subjected to more or less no opposition. In addition, disinformation spread in this way reaches the other side of the world practically at the same time and can spread like a global virus. In addition, disinformation is quite often and intentionally created in such a way that this spread is further supported, for example by using various sensational claims or extreme feelings that are intended to evoke in the reader (Shu et al. 2020, p. 4).

2 DISINFORMATION AND PROPAGANDA AS A SECURITY THREAT

The following chapter outlines how disinformation campaigns work and why disinformation and propaganda are among the security threats we have faced in the last few years. Concrete examples of some states and transnational organizations are also briefly presented, in which way they try to fight disinformation and propaganda.

2.1 Basic principles of the functioning of contemporary Russian propaganda

As already outlined in the previous chapter, current Russian propaganda follows the historical "disinformation tradition" of the former Soviet Union. However, in addition to the classic channels of television and radio, it manages to effectively use the current possibilities in the field of cyberspace, primarily through Internet websites and social networks. More intensive Russian disinformation activity can be identified since the beginning of the new millennium, while further intensification of activities by Russia's intelligence services and agencies, influencing public debate and moods in democratic societies by using various "internationalist and civil movements" occurred in 2008.

The year 2008 was crucial for the current form of Russian hybrid action, because it experimentally tried out some methods of conducting hybrid warfare directly in the conflict in Georgia. For example, it carried out information and psychological operations using methods that it later permanently included in its repertoire of hybrid operations. Whether it

was the use of disinformation and the manipulation of facts, the manipulated selection of "eyewitnesses" favourable to the Russian narrative, or, on the contrary, the omission of facts that do not fit into it, but also much more massive action on the Internet as part of the information war (Rogoża – Dubas, 2008, pp. 3-4).

If the conflict in Georgia represented for Russia a kind of laboratory for its hybrid action, then after the well-known events in Ukraine in 2014, related to the Russian annexation of Crimea and the creation of the separatist republics - Donetsk and Luhansk, it is possible to see the finished product and the result of these experiments. In light of this, Snyder (2018, p. 158) states that *"this is a conflict involving the most sophisticated propaganda campaign in history"*.

Paul and Matthews (2016) identify 4 specific features in the character of contemporary Russian propaganda:

- it is high-volume and multi-channel,
- it is fast, continuous, and repetitive,
- is not tied to objective reality,
- is not bound by consistency.

The high volume and multi-channel nature of Russian propaganda lies in the fact that it is created on a large scale and at the same time is broadcast or otherwise distributed through many different channels. At the same time, it is created in various formats (text, video, image, sound) and distributed through all available channels, from classic (television, radio) to new (internet, social networks, discussion forums, chat rooms, disinformation websites) (Paul and Matthews 2016). The so-called troll farms are also used very intensively. The most famous of them is the Internet Research Agency based in St. Petersburg. The direct link of this troll farm to the Russian state is indisputable, since it has the status of a "government object" and is guarded by the Federal Security Service of the Russian Federation, which is the Russian intelligence service whose task is to ensure the internal security of the state. The agency operates 24 hours a day. The main job of the agency's employees, who work in shifts and are paid very well compared to St. Petersburg conditions, is to disrupt and flood discussions on social networks and spread disinformation (Aro, 2019, p. 189-191). Other tools include the use of disinformation websites that spread a pro-Russian narrative, while some authors of these websites are directly financed by Russia, while others, on the contrary, act from their own convictions. In addition to disinformation websites, the broadcasting of the state-funded RT (Russia Today) television, which conveyed the Russian narrative to a foreign-language audience, was also an important pillar until recently.

Speed, continuity, and repeatability are key qualities especially important for today's internet age. Russian propaganda has no regard for facts, which allows it to react flexibly and immediately to the latest events and dictate the direction and way in which the event will be interpreted and discussed. At the same time, it very often reaches for the recycling of old topics and misinformation, depending on how it suits Russia (Paul – Matthews 2016).

The fact that Russian propaganda is not tied to objective reality means that it does not worry too much about the truth of the information it sends to the world. A popular method is the use of at least partially true information, the so-called grains of truth, on which another, but already fully fabricated, story is attached (Paul - Matthews 2016). An important factor in the creation of such a story is also its framing, i.e., influencing the emotional tone of the message using language manipulation and the choice of appropriate words (Táborský, 2019, 42-45). However, Russian propaganda does not avoid completely unmasked lies, as it often uses falsified evidence as a basis for its claims and/or refers to non-existent sources and witnesses of the described events (Paul - Matthews 2016).

Consistency is deliberately not high on the list of Russian propagandists. Different types of media can emphasize different topics, and individual pro-Russian channels can broadcast completely different sounding versions of one and the same topic or message. Even the same channel can change the tone of one piece of information several times, even completely diametrically, which allows propagandists to respond ad hoc to the mood of the audience (Paul - Matthews 2016). It is one of the paradoxes, which somewhat goes against the definitions of propaganda mentioned above, but for Russia it is not only about promoting its own narrative, but also about flooding the information space with different, often contradictory versions of the same story or event.

Therefore, the goal of pro-Russian propaganda is not always to forcefully convince the target audience only of the "own truth" that suits the regime there, but also to flood the information and media space with a considerable amount of different information, which many times completely exclude each other. The result is information chaos, flooding of the infosphere with ballast and information overload of the target audience. The feeling is deliberately evoked about the relative truth of all information and the unattainability, perhaps even non-existence, of objective truth. Russia has already successfully applied this tactic to domestic audiences. In line with this, Snyder (2018, p. 156) states that *"once citizens doubt absolutely everything, it prevents them from looking beyond Russia's borders for alternative models, having a meaningful debate about reform, and trusting themselves enough to advocate for policy change"*. The goal of Russian propaganda is to induce apathy and the feeling that nothing can be changed, and that change is not even worth trying. One of the many dangers of Russian propaganda for liberal-democratic political systems lies precisely in the attempt to create an apathetic person without interest in the surrounding (political) events and disrupt the functioning of civil society in general.

2.2 Disinformation and propaganda as a security threat

Propaganda, the new evolutionary part of which also includes various disinformation campaigns, has always been a threat to the internal security of the state, because its goal was to influence the society of a foreign state actor in its favour. However, while before, from today's point of view, the possibilities of propagandists to spread disinformation were largely

limited to traditional media (television, radio), today they can use a wide range of different new media platforms, with cyberspace and its components (internet, websites, and social networks) playing a key role.

In this case, especially social networks prove to be a very efficient and effective tool (Kuchtová, 2023), enabling the spread of disinformation on a mass scale based on the principles on which they operate. Social networks have more or less replaced journalists and classical media in the role of so-called gatekeepers who selected information and set the agenda for their audience. To a certain extent, this task has been taken over by algorithms that decide what a given user on a given medium will see on their virtual wall. The problematic moment is that no one - except the operators of the given network - knows how the given algorithms work and at the same time, for business reasons, these algorithms serve content that they assume will interest the user in order to keep it on their platform as long as possible and thus produce profit. This contributes to the fact that primarily interesting, bombastic, often shocking content is spread and not true content. This can take various forms, from articles with sensationalism, through clickbait to outright disinformation and conspiracies, and political content created and massively expanded by trolls and anonymous accounts (e.g., in the form of links to articles from disinformation websites) (McKay – Tenove 2021, p. 705).

Of course, disinformation on social networks is not the only component of current Russian propaganda, but it is currently one of the most visible and discussed ways of spreading hybrid threats. Due to their nature and functioning, they create a very suitable environment for the rapid and mass dissemination of disinformation, which can lead to the disruption of the internal security and functioning of democratic states, the undermining of trust in the democratic system, principles, and values, as well as the disruption of overall social cohesion. A great danger also stems from the attempt to influence public debate and discourse with disinformation that uses already existing conflict lines (political, religious, social, ethnic, etc.) in society and can gradually lead to an even greater deepening of these lines and the radicalization of some parts of society. The result of the combination of promoting radicalization and undermining trust in democratic values and principles is then (among other things) an increase in support for anti-system parties. This calculation of negative impacts is not definitive, but it sufficiently demonstrates why disinformation is a serious security threat for contemporary democratic states and institutions, which must be adequately responded to.

2.3 Some institutional responses to the spread of disinformation

Disinformation spread on the Internet and social networks is a phenomenon characterized by great complexity with a tendency to test the limits of liberal democracy. Specifically, it concerns, for example, issues of freedom of speech, the right to privacy, or the regulation of social networks and the content published on them. Also, because these fundamental questions, as inherent parts of liberal democracy (freedom vs. security), are

open, no definitive and unified solution currently exists, but individual (European) countries and transnational institutions understandably react to this threat in different ways.

The year 2014, when the Russian annexation of Crimea and the related disinformation campaign took place, can be considered as the starting point of efforts to securitize[1] disinformation by individual actors. Among other significant moments that reinforced the need for an adequate response are disinformation campaigns in the context of the Brexit referendum in the United Kingdom (2016) or efforts to influence the parliamentary elections in Germany (2017, 2021) and the presidential elections in the USA (2016 and 2020) and in France (2017, 2022). The North Atlantic Alliance began to securitize disinformation in its documents also in 2014, when the word "disinformation" entered its vocabulary. In the same way, the European Union and its member countries began to understand disinformation campaigns as a security threat against which it is necessary to take adequate measures, for example in the form of new legal measures, the creation of new special bodies or institutions to combat disinformation, support for public education in the field of media and digital skills, cooperation with the media and social networks, etc.

For example, in the Baltic countries, which have long been among the leaders in the field of cyber and information security, they are aware of the importance of educating society and consistently pay attention to this activity. An example can be Estonia, where already in 2011, the National Defence and Security Awareness Centre was established, the main objective of which is to raise awareness of security threats in Estonia, among other things, by organizing workshops and issuing publications for young people. As part of primary school education, students complete the subject of national defence, in which, among other things, they also deal with the issue of disinformation (Rosen, 2023). Lithuania also pays attention to the education of the population, primarily in the field of media literacy, which is a mandatory part of the school curriculum in schools. It also builds on the wider cooperation of the governmental and non-governmental sectors, an example of which is the Debunk.eu project aimed at early detection of disinformation, which involves state officials, armed forces, ministries of defence and foreign affairs, journalists, volunteers, researchers, and IT experts (Debunk, 2023). One of the measures is the establishment of the National Centre for Cyber Security in 2015, the purpose of which is to improve the cooperation of state departments and the critical infrastructure sector. There have also been legal measures that, among other things, allow the just-mentioned National Cyber Security Centre to temporarily block servers from which disinformation is spread (Abromaitis, 2022).

As far as transnational organizations are concerned, from the point of view of the Slovak Republic, the activities of the European Union and the North Atlantic Alliance in the fight against disinformation are primarily important. The European Union relies on a combination of several approaches - national and transnational. Already in March 2015, the

[1] Securitization represents a process when a certain already politicized topic (it is the subject of public policy) becomes an existential threat for the given actor, which requires and enables exceptional measures and interventions beyond the scope of the normal political process.

East StratCom Task Force was established, which aims to detect and combat disinformation not only in the EU countries, but also in the countries of the Eastern Partnership (EEAS, 2021). This centre is behind the EUvsDisinfo project, the main purpose of which is to detect and draw attention to disinformation in the countries of the Union (EUvsDisinfo, 2023). In 2017, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) was established in Helsinki, Finland, which complements the aforementioned working group as it is primarily dedicated to the study and countering of hybrid threats. This centre was established as a joint project with NATO and its members are member countries of both the Alliance and the Union. Another element in the fight against hybrid threats is the Rapid Alert System (RAS) (also cooperating with NATO), which should enable the sharing of knowledge and warnings about disinformation campaigns (EEAS, 2019). In addition, the EU tries to involve civil society in these activities (for example, within the cooperation of journalists, fact-checkers, academics, etc.), it also focuses on education (for example, in the form of Media Literacy Week), and the EU also uses its political power to act and cooperate with the technology companies (Facebook, Twitter, etc.).

The North Atlantic Alliance is fighting disinformation in several ways. However, the basic pillar of the alliance approach consists in the creation of two institutions dedicated to the given issue. In 2014, the NATO Strategic Communications Centre of Excellence (StratCom COE) was established, which deals with the field of strategic communication, which also includes research on disinformation and disinformation campaigns. The centre is responsible both for the implementation of educational activities, such as the organization of seminars, conferences, and the publication of various documents, and also for cooperation at the intergovernmental level (StratCom COE, 2023). The second important alliance institution is the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE), which is primarily responsible for cyber security, which at least partially covers the issue of disinformation (CCD COE).

CONCLUSION

There is no doubt about the presence of disinformation and propaganda in public and private physical and cyber space. Several mechanisms and tools with which Russian or other foreign propaganda work to influence democratic processes or spread disinformation are relatively well mapped. The issue of disinformation and propaganda and their dissemination is a very complicated area in which many different topics intersect. Currently, the spread of disinformation and propaganda as part of the spread of hybrid threats, primarily via the Internet and social networks, is an extremely dangerous threat that can have very adverse consequences for individuals, organizations, and the entire society. Unfortunately, the prediction of further development in this area is unfavourable. The Internet and social networks, the use of which will certainly increase in the coming years, connect us to the whole world, provide us with a lot of information, but at the same time make us vulnerable. It is

similar in the case of modern information and communication technologies, systems and means. Their quality, availability and scope of use will also certainly increase, which will bring us a lot of positives, but also negatives in the form of their abuse precisely for the spread of disinformation and propaganda as part of the spread of hybrid threats. As a follow-up to this and at the same time in accordance with the fulfilment of the objectives of the study, it is necessary to point out how important it is for transnational organizations, democratic states and their competent institutions, including the security forces, to take effective and efficient measures aimed at reducing the possibility of the spread of hybrid threats, and simultaneously support prevention and education in the field of media literacy and work with information. Increasing awareness of disinformation, improving the ability to recognize and detect it, as well as eliminating its spread as much as possible would certainly mean fewer opportunities for populism, radicalism, extremism, xenophobia or any influence or division of society precisely on the basis of spreading false, deceptive and misleading information. The engagement of relevant transnational organizations – in the case of the Slovak Republic, primarily the North Atlantic Alliance and the European Union – and the institutions of democratic states in this issue is therefore not only desirable, but even necessary. On the other hand, we must all realize that their possibilities are not infinite, that not everything will be solved for us by the state, the Alliance or the Union, and so it is necessary that we ourselves contribute to suppressing the amount, power and influence of disinformation and propaganda and actors, who spread them.

REFERENCES

ABROMAITIS, Ž. 2022.Lithuania builds new strategy to fight Russian disinformation. In *Lietuvos nacionalinis radijas ir televizija,* 2022. [online] [cit. 01-09-2023]. Dostupné na internete: <https://www.lrt.lt/en/news-in-english/19/1846743/lithuania-builds-new-strategy-to-fight-russian-disinformation>.

ARO, J. 2019. *Putin's Trolls: On the Frontlines of Russia's Information War Against the World*. New York : Ig Publishing, 2018. 327 s. ISBN 978-1-473-55620-1.

BAYER, M. 2006. Strategic Information Warfare: An introduction. In Halpin, E. et al. (eds.): *Cyberwar, Netwar and the Revolution in Military Affairs*. London : Palgrave Macmillan, 2006, s. 32-48. ISBN 978-0-230-62583-9.

BITTMAN, L. 2020. *Mezinárodní dezinformace: černá propaganda, aktivní opatření a tajné akce*. Praha : Mladá fronta, 2020. 360 s. ISBN 978-80-204-0843-6.

BURNS, M. 1999. Information Warfare: What and How? In *Carnegie Mellon's School of Computer Science*, 1999. [online] [cit. 31-08-2023]. Dostupné na internete: <https://www.cs.cmu.edu/~burnsm/InfoWarfare.html>.

CCD COE. 2023. About NATO CCD COE. In *NATO Cooperative Cyber Defence Centre of Excellence*, 2023. [online] [cit. 02-09-2023]. Dostupné na internete: <https://ccdcoe.org/about-us/>.

CLAUSEWITZ, C. 2008. *O vojne*. Praha : Academia, 2008. 749 s. ISBN 978-80-2001-598-3.

DANYK, Y. – MALIARCHUK, T. – BRIGGS, C. 2017. Hybrid War: High-tech, Information and Cyber Conflicts. In *Connections*, 2017, roč. 16, č. 2, s. 5-24. ISSN 1812-1098.

DARNTON, G. 2006. Information Warfare and the Laws of War. In Halpin, E. et al. (eds.): Cyberwar, Netwar and the Revolution in Military Affairs. London : Palgrave Macmillan, 2006, s. 139-153. ISBN 978-0-230-62583-9.

DEBUNK. 2023. Debunking disinformation together! In *Debunk.eu*, 2023. [online] [cit. 01-09-2023]. Dostupné na internete: <https://debunk.eu>.

EEAS. 2019. Rapid Alert System. In European Union External Action Service, 2019. [online] [cit. 02-09-2023]. Dostupné na internete: <https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf>.

EEAS. 2021.Questions and Answers about the East StratCom Task Force. In *European Union External Action Service*, 2021. [online] [cit. 02-09-2023]. Dostupné na internete: <https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en>.

EU. 2018. A Europe that Protects: Countering Hybrid Threats. In *European External Action Service*, 2018. [online] [cit. 30-08-2023] Dostupné na: <https://www.dsn.gob.es/sites/dsn/files/hybrid_threats_en_final.pdf>.

European Commission. 2018. Action Plan against Disinformation. In *Eur-Lex*, 2018. [online] [cit. 01-09-2023] Dostupné na internete: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018JC0036>.

EUvsDisinfo. 2023. About. In *EUvsDisinfo*, 2023. [online] [cit. 02-09-2023]. Dostupné na internete: <https://euvsdisinfo.eu/about/>.

FREELON, D. – WELLS, C. 2020. Disinformation as Political Communication. In *Political Communication, 2020, roč.* 37, č. 2, s. 145-156. ISSN 1091-7675.

GREEN, K. 2020. Does War Ever Change? A Clausewitzian Critique of Hybrid Warfare. In *E-International Relations*, 2020. [online] [cit. 29-08-2023]. Dostupné na internete: <https://www.e-ir.info/2020/09/28/does-war-ever-change-a-clausewitzian-critique-of-hybrid-warfare/>.

HAJDÚKOVÁ, T. – ŠIŠULÁK, S. 2022. Abuse of modern means of communication to manipulate public opinion. In *INTED 2022: 16th International Technology, Education and Development Conference – Conference Proceedings*. Barcelona : IATED, 2022, s. 1992-2000. ISBN 978-84-09-37758-9.

HALPIN, E. – TREVORROW, P. –WEBB, D. – WRIGHT, S. 2006. Cyberwar, Netwar and the Revolution in Military Affairs. London : Palgrave McMillan, 2006. 253 s. ISBN 978-0-230-62583-9.

HCSS. 2022. Hybrid Threats. In *The Hague Centre for Strategic Studies*, 2022. [online] [cit. 30-08-2023] Dostupné na: <https://hcss.nl/research/hybrid-threats/>.

HOFFMAN, F. G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. [online] [cit. 27-08-2023]. Dostupné na internete: <https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf>.

HOFFMAN, F. G. 2009. Hybrid Warfare and Challenges. In *Joint Force Quarterly*, 2009, roč. 52, č. 1, s. 34-39. ISSN 1070-0692. [online] [cit. 27-08-2023]. Dostupné na internete: <smallwarsjournal.com/documents/jfqhoffman.pdf>.

HOFREITER, L. – ZVAKOVÁ, Z. 2019. *Teória bezpečnosti*. Krakow : European Association for Security, 2019. 258 p. ISBN 978-83-61645-35-1.

Hybrid CoE. 2023. Hybrid threats as a concept. In *The European Centre of Excellence for Countering Hybrid Threats*, 2023. [online] [cit. 30-08-2023] Dostupné na internete: <https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/>.

IVANČÍK, R. 2021. Informačná vojna – jeden z multidisciplinárnych fenoménov súčasnej ľudskej spoločnosti spoločnosti. In *Politické vedy*, roč. 24, č. 1, s. 135-152. ISSN 1335-2741.

IVANČÍK, R. Teoretické východiská skúmania problematiky hybridnej vojny – vojny 21. storočia. In *Medzinárodné vzťahy*, 2016, roč. 14, č. 2, s. 130-156. ISSN 1339 – 2751.

JOWETT, G. J. – O'DONNELL, V. 2012. *Propaganda & Persuasion*. Thousand Oaks : SAGE Publications, 2012. 432 s. ISBN 978-1-41297-782-1.

JURČÁK, V. – JURČÁK, J. – SASARÁK, J. 2016. Hybridné hrozby – výzva pre Európsku úniu. In *Medzinárodné vzťahy – aktuálne otázky svetovej ekonomiky a politiky*. Bratislava: Vydavateľstvo Ekonóm, 2016, s. 542-550. ISBN 978-80-225-4365-1.

JURČÁK, V. – TURAC, J. 2018. Hybridné vojny – výzva pre NATO. In *Bezpečnostné fórum 2018 – zborník vedeckých prác z medzinárodnej vedeckej konferencie*. Banská Bystrica : Interpolis, 2018. s. 177-184. ISBN 978-80-972673-5-3.

KANIČÁROVÁ, K. 2021. Propaganda. In InfoSecurity.sk, 2021. [online] [cit. 31-08-2023]. Dostupné na internete: <https://infosecurity.sk/dezinfo/propaganda-disinfo-basics/>.

KELEMEN, M. 2015. Teória bezpečnosti: vybrané problémy ochrany osôb, majetku a ďalších chránených záujmov v sektoroch bezpečnosti. Košice : Vysoká škola bezpečnostného manažérstva, 2015. 99 p. ISBN 978-80-8928-299-9.

Krátky slovník hybridných hrozieb. 2021. Propaganda. In *Národný bezpečnostný úrad*, 2021. [online] [cit. 01-09-2023] Dostupné na internete: <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/kratky-slovnik-hybridnych-hrozieb/index.html>

KŘÍŽ, Z. – SCHEVCUK, Z. – ŠTEVKOV, P. *Hybridní válka jako fenomén v bezpečnostním prostředí Evropy*. Ostrava : Jagelo 2000, 2015. 16 s. ISBN 978-80-904850-2-0.

KUBEŠA, M. 2013. Vojenské klamání v informačním věku. In *Vojenské rozhledy*, 2013, roč. 22, č. 1, s. 160-164. ISSN 2336-299. <https://www.vojenskerozhledy.cz/kategorie-clanku/teorie-a-doktriny/vojenske-klamani-v-informacnim-veku>.

KUCHTOVÁ, J. 2023. Bezpečnosť na sociálnych sieťach. In *Bezpečnosť elektronickej komunikácie – zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou*. Bratislava : Akadémia Policajného zboru v Bratislave, 2022, s. 237-247. ISBN 978-80-8054-968-8.

LIBICKI, M. C. 1995. What is information warfare? In *Center for Advanced Concepts and Technology, Institute fo National Startegic Studies, National defense university*, 2020. [online] [cit. 31-08-2023]. Dostupné na internete: <https://apps.dtic.mil/sti/pdfs/ADA367662.pdf>.

MANKO, O. – MIKHIEIEV, Y. 2018. Defining the Concept of 'Hybrid Warfare' Based on Analysis of Russian Agression against Ukraine. In *Information & Security: An International Journal,* 2018, roč. 41, s. 11-20. ISSN 0861-5160.

McKAY, S. – TANOVE, C. 2021. Disinformation as a Threat to Deliberative Democracy. In *Political Research Quarterly*, 2021, roč. 74, č. 3, s. 703-717. [online] [cit. 02-09-2023]. Dostupné na internete: <https://doi.org/10.1177/1065912920938143>.

NATO. 2020. Media - (Dis)Information - Security. In NATO, 2020. [online] [cit. 31-08-2023]. Dostupné na internete: <https://www.nato.int/nato_static_fl2014/assets/

NATO. 2020. NATO's approach to countering disinformation. In *North Atlantic Treaty Organisation*, 2020. [online] [cit. 01-09-2023] Dostupné na internete: <https://www.nato.int/cps/en/natohq/177273.htm>.

NATO. 2023. NATO's response to hybrid threats. In *North Atlantic Treaty Organisation*, 2023. [online] [cit. 30-08-2023] Dostupné na: <https://www.nato.int/cps/en/natohq/topics_156338.htm>.

NCDSA. 2023. National Centre For Defence & Security Awareness - Company Information. In *6sense*, 2023. [online] [cit. 01-09-2023]. Dostupné na internete: <https://6sense.com/company/national-centre-for-defence-security-awareness/605db32710fce904a7429036>.

PAUL, C. – MATTHEWS, M. 2016. The Russian ‚Firehose of Falsehood´ Propaganda Model: Why It Might Work and Options to Counter It. In RAND Corporation, 2016. [online] [cit. 01-09-2023]. Dostupné na internete: <https://www.rand.org/pubs/perspectives/PE198.html>.

PIWOWARSKI, J. 2017. *Nauki o bezpieczeństwie. Zagadnienia elementarne*. Krakow : European Association for Security, 2017. 218 p. ISBN 978-83-64035-55-5.

QUALTER, T. H. 2020. *Propaganda and Psychological Warfare*. New Jersey : Burtyrki Books, 2020. 265 s. ISBN 978-1-8397-4304-7.

REICHBORN-KJENNERUD, E. – CULLEN, P. 2016. What is Hybrid Warfare? In *Norwegian Institute of International Affairs*, 2016. [online] [cit. 28-08-2023]. Dostupné na internete: <https://www.jstor.org/stable/resrep07978>.

ROGOŻA, J. – DUBAS, A. 2008. Russian Propaganda War: Media as a Long and Short-Range Weapon. In *CES Commentary*, 2008, č. 9, s. 1-5. [online] [cit. 01-09-2023]. Dostupné na internete: <https://www.files.ethz.ch/isn/91705/commentary_09.pdf>.

ROSEN, K. R. 2023. Estonia's answer to Russian disinformation. In *Coda Media*. [online] [cit. 01-09-2023]. Dostupné na internete: <https://www.codastory.com/newsletters/ estonia-public-media-russian-disinformation/>.

ŘEHKA, K. 2017. *Informační válka*. Praha : Academia, 2017. 224 s. ISBN 978-80-200-2770-2.

SHU et al. 2020.Combating Disinformation in a Social Media Age. In *Cornell University*, 2020. [online] [cit. 01-09-2023]. Dostupné na internete: <https://arxiv.org/abs/2007.07388>.

SNYDER, T. 2018. *The Road to Unfreedom - Russia, Europe, America*. New York : Random House, 2018. 368 s. ISBN 978-1-473-55620-1.

Sociologická encyklopedie. 2017. Dezinformace. In Sociologický ústav Akadémie vied Českej republiky, 2017. [online] [cit. 01-09-2023] Dostupné na internete: <https://encyklopedie.soc.cas.cz/w/Dezinformace>.

SPROULE, J. M. 1997. *Propaganda and Democracy: The American Experience of Media and Mass Persuasion*. Cambridge : Cambridge University Press, 1997. 332 s. ISBN 978-0-52147-022-3.

STOKER, D. – WHITESIDE, C. 2020. Blurred Lines: Gray-Zone Conflict and Hybrid War—Two Failures of American Strategic Thinking. In *Naval War College Review*, 2020, roč. 73, č. 1, s. 1-37. [online] [cit. 29-08-2023]. Dostupné na internete: <https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=8092&context=nwc-review>.

StratCom COE. 2023. About NATO StratCom COE. In NATO Strategic Communications Centre of Excellence, 2023. [online] [cit. 02-09-2023]. Dostupné na internete: <https://stratcomcoe.org/about_us/about-nato-stratcom-coe/5>.

TÁBORSKÝ, J. 2019. *V síti dezinformací. Proč věříme alternativním faktům*. Praha : Grada Publishing, 2020. 224 s. ISBN 978-8-02712-014-7.

TOMÁŠEK, R. 2022. O hybridných hrozbách a hybridnej vojne. In *Národná a medzinárodná bezpečnosť 2022 – zborník vedeckých prác z 13. medzinárodnej vedeckej konferencie*. Liptovský Mikuláš : Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2022, s. 319-328. ISBN 978-80-8040-631-8.

TRIFUNOVIC, D. – KAZANSKÝ.R. – NEČAS. P. 2021. Conceptualization of Terrorism as a Modern Form of Political Violence. In *Politické vedy*, 2021, roč. 24, č. 2, s. 108-124. ISSN 1335 – 2741.

WARDLE, C. – DERAKHSHAN, H. 2017. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. In *Council of Europe*, 2017. [online] [cit. 01-09-2023] Dostupné na internete: <https://firstdraftnews.com/wp-content/uploads/2017/10/Information_Disorder_FirstDraft-CoE_2018.pdf?x56713>.

Col. GS (ret.) Assoc. Prof. Dipl. Eng. Radoslav IVANČÍK, PhD. et PhD., MBA, MSc.
Akadémia Policajného zboru
Sklabinská 1, 835 17 Bratislava
tel.: 09610 57490
e-mail: radoslav.ivancik@akademiapz.sk

DOI: https://doi.org/10.52651/vr.a.2023.3.59-73
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2023, Number 3, Page 59-73

OPPORTUNITIES AND DIRECTIONS FOR THE EVOLUTION OF COMMAND AND CONTROL SYSTEMS IN THE CONTEXT OF MULTI-DOMAIN OPERATIONS

Andras TOTH, Tibor FARKAS

ARTICLE HISTORY

Submitted: *05. 10. 2023*
Accepted: *06. 12. 2023*
Published: *31. 12. 2023*

ABSTRACT

The military conflicts of recent times have highlighted the need for modern military operations to focus on multi-domain operations, which requires a transformation of the command and control system, by creating mobile and flexible headquarters that can provide relevant information at any time, even during redeployments and redeployments. Cloud computing can be used to integrate data collection tools, ensuring fast and accurate analysis of large amounts of incoming data. A private 5G network can provide a secure, high-speed and reliable communication environment for cloud-based command and control systems. This network will enable real-time information transfer, facilitate rapid decision-making processes and enable the deployment of autonomous vehicles and drones. The authors have also explored capabilities that support the deployment of autonomous vehicles and drones, enabling commanders to conduct intelligence and surveillance more effectively. By leveraging technology and advanced communications systems, commanders can lead their teams in a dynamic environment while providing a high level of situational awareness. This integration of information and mobility allows commanders to react quickly and decisively, ultimately increasing their effectiveness on the battlefield.

KEYWORDS

command and control, multi-domain operations, command posts, 5G, cloud computing.

INTRODUCTION

The Russian-Ukrainian conflict seems to be overturning many military principles that were once considered fundamental and that the armies of the present day are typically designed to uphold. There has been no preparation for symmetrical warfare in recent decades, with the emphasis shifting to peacekeeping operations, where asymmetric traits are typical. Accordingly, the conceptual and practical implementation of command and control (C2) has moved in a direction that does not meet the requirements of conventional multidimensional operations. The abbreviation "C2" stands for both the conceptual side of command and

control, the command, control, cooperation, and coordination scheme. However, it can also be applied to the physical components that provide the interconnection. NATO's Allied Joint Doctrine (AJP-01) emphasizes that command and control are related concepts, generally used together but not synonymously. The military leader, the commander at all levels, is an expert in decision-making, motivating, and directing to accomplish a given task. His or her main task is personal leadership and decision-making while sharing accountability and command and control with his or her tribe (NATO, 2022).

This divergence of emphasis has led to a lack of preparedness for symmetrical warfare, with potentially devastating consequences. To address this problem, it is important to re-evaluate current C2 strategies and make them more relevant to the needs of traditional multi-domain operations. This could include the incorporation of new technologies and tactics, as well as improved communication and coordination between different military disciplines. In addition, a new emphasis on training and preparation for symmetric warfare, including scenarios involving both conventional and asymmetric threats, is needed. By taking these steps we can better ensure that our soldiers are prepared for any type of conflict that may arise in the future.

This was recognized by three senior US Army leaders (Lt. Gen. Milford "Beags" Beagle, Brig. Gen. Jason C. Slider, Lt. Col. Matthew R. Arrol) who examined the lethality and transparency of the modern battlefield through the example of the Battle of Chornobayevka during the Russian-Ukrainian conflict, using the coordinated application of multi-domain effects on the warfare function. The article highlights the need for a rethinking of command and control in this new era of warfare. Faced with the immediate threat, armies must transform their command and control systems to incorporate the principles of multi-domain operations (MDO). To fight and win in large-scale combat operations in the modern theatre, the Army's command posts must become more resilient, agile and responsive without sacrificing effectiveness. Otherwise, command posts become places where commanders go to die (Beagle et. al., 2023).

1 MULTI-DOMAIN OPERATIONS

Under the concept of multi-domain operations (MDO), in the future, multiple operations will be conducted simultaneously on the battlefield, including space, information, and cyber operations, in addition to traditional air, land, and naval military operations. In the event of a major power conflict, this will be the most likely form of warfare in the coming decades.

The future of military operations will be complex and multifaceted. With the emergence of space, information, and cyber operations, navigating the battlefield will become an even more challenging environment alongside traditional air, land, and naval military operations. Combat in this new form of warfare will require a high degree of

coordination and cooperation between the different branches of the military, as well as other government agencies and private sector partners.

Collecting and analyzing large amounts of data in real time will be critical to success in the field. In addition, advanced technologies such as artificial intelligence, autonomous systems, and robotics will play an increasingly important role in future military operations. Looking ahead to the coming decades, it is clear that those who adapt quickly to this changing environment will be best placed to engage in any great power conflict successfully. To this end, military organizations must prioritize developing and implementing cutting-edge technologies that enable real-time data collection and analysis. Significant investment in research and development and a willingness to embrace emerging technologies such as artificial intelligence, autonomous systems, and robotics, as mentioned above, will be required. In addition to technological developments, military leaders will also need to prioritize the training and education of personnel to ensure they have the skills to operate new systems effectively.

Ultimately, success on the battlefield depends on the ability of the military to adapt quickly to changing circumstances and leverage technology to gain a strategic advantage over adversaries. Those who can do so will be well placed to engage successfully in future conflicts with the great powers. In addition, military leaders need to establish clear communication channels and protocols to ensure effective coordination between different units and branches. Doing so will enable them to respond quickly and decisively to any threats or challenges during combat operations.

By investing in technology and personnel development, military organizations can increase their preparedness and effectiveness against evolving security threats. In addition, training programs focusing on leadership development and cross-functional collaboration can help to develop a culture of innovation and adaptability in the military. At the same time, it is particularly important in today's rapidly changing global security environment, where new threats and challenges are emerging at an unprecedented pace. By adopting these strategies, military leaders can ensure that their organizations remain resilient and resilient in the face of adversity. Ultimately, this will help them fulfil their mission of protecting their countries and promoting peace and stability worldwide (Perkins, 2017).

MDO integration combines autonomous platforms with intelligent command and control systems to achieve tasks and goals. However, current C2 systems struggle to manage the operational tempo between autonomy, people, and battlefield dynamics. Internet of Battlefield Things (IoBTs) such as unmanned aerial, ground, maritime, and space vehicles (UxVs) create benefits and problems for C2 systems. The ubiquity, dispersion, complexity, stochasticity, and heterogeneity of IoBTs will require a change in the way C3I (Command, Control, Communications, and Intelligence) decision-making and support systems acquire situational awareness, structure operational problems, assess courses of action, and provide feedback on execution. The collective intelligence nature of IoBTs can create battlefield

dynamics that only IoBT itself can address. MDO and cross-domain capabilities will increase the complexity of situational awareness and challenge the nature of warfare. How, for example, does a commander decide between autonomous combat and long-range artillery or cyber-attacks? How do they integrate data from integrated forces to create a unified picture of what is happening?

The nature of the effects - whether initiated by the IoBT or by the commander's decision - creates new dynamics that require new battlefield concepts that combine human command with machine control. Disrupting enemy decision-making has always been a goal in combat, but automated C2 tools and IoBT technologies can rapidly assemble, adapt and reassemble the force structure and implications to achieve military objectives. The MDO battlefield also requires new concepts of operations that take full advantage of the potential of artificially intelligent and autonomous systems (Russell et. al., 2019).

The advent of MDO and the integration of advanced technologies will undoubtedly transform the nature of warfare. Combining human command and control with machine control can improve military decision-making, enabling more effective targeting and mission execution. Furthermore, artificially intelligent and autonomous systems will enable new operations concepts that can exploit these technologies' potential. However, it is important to consider the ethical implications of such warfare developments and ensure that they are used responsibly. As we move towards a more technologically advanced battlefield, we must maintain a balance between human decision-making and machine control to ensure optimal outcomes for both military objectives and humanitarian concerns.

2 REQUIREMENTS FOR THE OPTIMIZATION OF COMMAND AND CONTROL SYSTEMS

Optimizing command posts requires reducing the reliance on the physical dimension (assets), increasing the use of the information dimension (data), and maximizing the ability to interact with the human dimension (commanders). This approach involves leveraging technology and data analytics to streamline operations and improve decision-making processes. Resources can be allocated more efficiently by reducing the need for physical assets such as vehicles and equipment. In addition, using data can provide valuable insights into trends and patterns that can inform strategic planning.

Finally, by enhancing communication and collaboration between commanders, the overall effectiveness of command posts can be significantly improved. This perspective requires a shift towards adopting new technologies and operational methods, but ultimately can greatly improve military operations. In today's rapidly evolving military environment, commanders must look for new ways to optimize their operations. One key strategy is to leverage data analytics to gain valuable insights into the causes of changes in their environment (trends, patterns). As a result, they can make more informed decisions about resource allocation and streamline their processes for maximum effectiveness. Another

important factor is communication and collaboration between command posts. By promoting a culture of openness and teamwork, headquarters can work together more effectively and achieve greater success on the battlefield. While these changes may require a shift in mindset, the potential benefits are significant. With the right approach, new technologies and operational methods can help military organizations achieve their goals more effectively than ever before.

Developing an effective and survivable command post in large-scale operations requires focusing on four key principles. The first principle is to ensure the command post is mobile and can be rapidly deployed to different locations as required. This allows commanders to respond quickly to changing conditions on the battlefield. In a conflict, mobility is essential, whether tactical or strategic. Its importance comes from how it relates to the creation of opportunities and how it gives the actor multiple strategies for thinking, fighting, moving, and planning. Moreover, immobility makes the actor a convenient target. Both physical and mental immobility are possible. Because cognitive immobility limits the actor's alternatives, his future behavior becomes predictable, making him more vulnerable to intentional harm.

The second principle focuses on integrating advanced technologies to improve data collection, analysis, and dissemination. This will enable commanders to make informed decisions based on real-time information and gain a tactical advantage over the enemy. Armies can integrate these technologies into systems comprising subsystems that communicate with each other to maintain balance. Sustainment, the physical manifestation of the system's equilibrium, is essential for its proper functioning, and the actor must aggressively target and defend it. Mapping the adversary's system helps to identify barriers and bottlenecks that lead to exhaustion and depletion. In large-scale combat operations, actors must operate to fend off sophisticated attacks against their sustainment network.

The third principle is to establish a clear line of communication between all members of the command, including those in the field. This guarantees that everyone can access critical information and work together seamlessly towards a common goal. Information is a crucial element of military operations, and the effectiveness of operations often depends crucially on the flow of information. Another serious problem can be information manipulation, including delays, misinformation, and delayed or distorted data, which can cause instability and misrepresentation. Protecting the integrity of information is key in warfare, and actors must contribute to properly functioning the system while remaining vigilant about their information (Fox, 2021).

Finally, it is essential to focus on human factors such as leadership, training, and morale. By investing in these areas, commanders can maximize their ability to interact with their teams and make informed decisions under pressure. In addition to the abovementioned principles, other factors must be considered for success in combat. One such factor is the importance of intelligence and analysis. By gathering and analyzing

intelligence information, commanders can better understand the enemy's capabilities and intentions and thus plan and execute operations more effectively. It is also important to consider the impact of terrain on operations. Understanding the impact of terrain on movement and communications can help commanders plan and execute operations more effectively. Finally, it is important to maintain flexibility in planning and execution. On the battlefield, the ability to adapt to changing conditions can mean the difference between success and failure. Suppose commanders consider these factors in addition to the command principles outlined above. In that case, they can increase their chances of victory over the enemy.

Recognizing the challenges of the current environment, the cross-cutting operation stresses that command posts must follow the principles of agility, alignment, resiliency, and depth as an element of the command system. Examining these four principles will help define what it means to develop an acceptable, reliable, and comprehensive command post that is effective and survivable in a large-scale military operation against a strong adversary.

2.1 Agility

The command posts are currently facing an endless cycle of installation, decommissioning, relocation, and redeployment to maintain operational efficiency and effectiveness. Reducing the number of tents and mounting systems on vehicles can improve mobility. However, it does not eliminate the need for constant set-up and configuration. To address this problem, militaries are exploring new approaches to designing and deploying command posts, such as modular, prefabricated structures that can be quickly assembled and disassembled.

These structures can be customized to meet specific mission requirements and are easily transported by air or ground. By using these innovative solutions, forces can improve the ability to rapidly deploy command posts in any environment, increasing operational readiness and effectiveness on the battlefield. Using modular and prefabricated structures also brings many other benefits to headquarters. For example, these structures are often more cost-effective than conventional command posts because they can be produced in large quantities and require less time and human resources to assemble. In addition, modular structures can be easily adapted to changing mission requirements or operational environments, providing greater flexibility and agility for military forces.

Furthermore, these structures can be equipped with advanced technologies such as satellite communication systems, secure data networks, and real-time situational awareness tools to increase the efficiency of command and control operations. Overall, using modular and prefabricated structures for command posts represents a promising new approach to military operations that can greatly enhance operational readiness and effectiveness on the battlefield.

2.2 Alignment

Current systems and on-site servers cannot adequately support effective C2 processes nor maintain a steady flow of relevant data to make the best decisions. This requires moving to the cloud and improving data servers and data federation concepts. A data grid is a decentralized data architecture that combines creating, managing, and sharing data within and between domains. The data fabric automates data integration, reducing dependencies on individual platforms or data stores.

The move to the information dimension requires new methodologies and competencies to achieve efficient operations. Integrating sensors, weapon systems, and decision-makers through machine learning and artificial intelligence can improve efficiency and enable faster decision-making and more effective response to dynamic situations. Cloud computing and distributed systems can further enhance the scalability and flexibility of information infrastructure, ensuring that teams stay at the leading edge and achieve optimal efficiency.

Military organizations can also benefit from deploying emerging communications technologies, such as 5G networks, providing high-speed connectivity and low latency for real-time data transmission. In addition, using unmanned aerial vehicles (UAVs) and autonomous ground vehicles (AGVs) can reduce the risk to human personnel in hazardous situations while providing enhanced situational awareness and intelligence capabilities. Furthermore, integrating Augmented Reality (AR) and Virtual Reality (VR) technologies can provide an immersive training experience for military personnel, allowing them to simulate different scenarios and develop their decision-making skills.

Altogether, using advanced technologies can greatly improve the operational capabilities of military organizations, enabling them to achieve their objectives with greater efficiency and effectiveness. Adaptation to new technologies is key for military organizations to maintain their competitive advantage in modern warfare. By investing in cutting-edge technologies such as artificial intelligence (AI) and Internet of Things (IoT), military personnel can gain real-time insights into the battlefield, enabling them to make informed decisions quickly and efficiently. Moreover, integrating these technologies can also lead to the developing of autonomous systems that can perform tasks with minimal human intervention.

This reduces the risk of casualties and allows military personnel to focus on more strategic tasks. In addition, drones and other unmanned vehicles can provide valuable intelligence and reconnaissance capabilities, allowing military organizations to gather critical information without risking their personnel. Advanced communications systems can also greatly improve coordination and cooperation between different units, allowing them to work seamlessly towards a common goal. Overall, embracing emerging technologies is essential for military organizations to achieve alignment and ensure that the established command posts contribute to maintaining the dominance gained on the battlefield.

2.3 Resiliency

Resilience in the military is another key benefit of using emerging technologies. Adapting and responding quickly to changing situations enables military organizations to withstand unexpected challenges and threats better. This resiliency can lead to more successful missions and effectiveness in achieving strategic objectives. In addition, new technologies can enhance the safety of military personnel by providing advanced surveillance and communication systems.

Moreover, it can reduce the risk of casualties and improve situational awareness, allowing for more informed decision-making on the battlefield. In addition, these technologies can also improve the efficiency and speed of operations, enabling faster reaction times and better coordination between units. However, it is important to balance the use of technology with appropriate training and preparation to ensure that military personnel have the necessary skills to use these tools effectively in combat situations. Another important aspect of military technology is cyber security. As military operations become increasingly reliant on digital networks and communications systems, they become more vulnerable to cyber-attacks by hostile actors.

Therefore, this highlights the need for robust cybersecurity measures to protect sensitive information and prevent unauthorized access to critical systems. Cyber resilience is also key, allowing military units to recover quickly from cyber-attacks and continue operations without major disruptions. Therefore, investing in cyber security and resilience is as important as investing in advanced military technology. As technology continues to evolve, so does the risk of cyber-attacks. Military units are particularly vulnerable to these attacks, which can compromise sensitive information and critical systems. To combat this threat, robust cybersecurity measures are needed to prevent unauthorized access and protect against hostile actors. By prioritizing these measures, military units can ensure they are well prepared to face the evolving threat of cyber-attacks and protect their critical assets from damage.

Command posts and communications networks are particularly vulnerable to cyber-attacks compromising sensitive information confidentiality, integrity, and availability. Therefore, military units must implement robust cybersecurity protocols and conduct regular training and exercises to enhance their cyber defense capabilities. As modern warfare increasingly relies on technology, the complexity and frequency of cyber threats are expected to increase, making cybersecurity a key priority for military leaders worldwide.

2.4 Depth

The depth of military operations extends operations in time, space, or cognitive sense. Multi-domain operations allow teams to maximize effectiveness in the human, physical, and information dimensions. By leveraging deeper planning and thinking, teams

can achieve better situational awareness, decision-making, coordination, and rapid adaptation. This approach also increases efficiency and effectiveness by sharing information and resources. As a result, forces can adapt quickly to changing circumstances and achieve their goals more quickly and accurately.

Ultimately, MDOs are critical to maintaining strategic advantage on the battlefield and ensuring mission success. In addition to their importance in warfare, MDOs significantly impact national security and global stability. By harnessing the power of technology and information, military forces can better understand their adversaries and respond more effectively to emerging threats. They also enable greater cooperation between different forces and with allied nations and other partners. This cooperation is essential to build trust and promote peace in an increasingly complex and interconnected world. Ultimately, the success of MDOs depends on the ability of military leaders to integrate different capabilities and technologies into a coherent strategy that supports overall mission objectives. However, with careful planning and execution, these operations can help ensure the safety and security of people worldwide.

The depth of military operations requires a comprehensive understanding of the operational environment and the ability to adapt to changing circumstances. It also requires effective communication and cooperation with civilian agencies, international partners, and local communities to achieve common goals and minimize potential negative impacts. In addition, military operations must be conducted in accordance with international law and human rights norms to preserve legitimacy and avoid undermining the values they seek to protect. In addition, a clear exit strategy and post-conflict reconstruction plan are essential to ensure long-term stability and prevent a relapse into conflict.

2.5 Data-centric command posts

Data-centric command posts are replacing network-centric ones and relying on the help of data processing, security, and operations specialists. Such an approach allows commanders to adapt and tailor command and control systems based on specific operational requirements and managerial preferences. The as-a-service (aaS) model outsources maintenance and enables rapid adoption of new technologies and mobility. Military units can leverage cloud services to improve operational capabilities, gain global access to critical information and applications, reduce costs, and collaborate more effectively. As technology advances, the aaS model is expected to become more prevalent in military operations, enabling militaries to stay ahead of emerging threats and maintain their information superiority on the battlefield. As technology evolves, the aaS model will likely become even more important for military organizations that want to maintain their competitive edge in an increasingly complex and dynamic global environment.

The adoption of the aaS model will bring significant benefits to modern warfare. With its cost-effective and on-demand approach, militaries can access state-of-the-art technologies and expertise without investing in expensive infrastructure or training programs. This can reduce the burden on military budgets and improve the speed and efficiency of operations. The aaS model also allows for greater cooperation and interoperability between the different branches of the military and with international partners. This will facilitate joint missions and enhanced information sharing, essential for successful outcomes in today's complex security environment. Looking ahead, it is clear that the aaS model will play a critical role in shaping the future of military operations. As a result, data-centric command posts are becoming increasingly important, enabling military leaders to make informed decisions in real-time based on the vast amounts of data available.

Cloud computing could also revolutionize the way military organizations operate. By leveraging cloud services, militaries can enhance their operational capabilities and gain global access to critical information and applications. With cloud computing, military forces can streamline operations, reduce costs and stay at the forefront of new technologies and mobility. As a result, militaries can adapt quickly to changing circumstances and use resources more efficiently, ultimately leading to better mission outcomes. Cloud computing also enables military organizations to improve their collaboration and information-sharing capabilities. By storing data and applications in the cloud, different units and branches can easily access and exchange information in real-time, leading to faster decision-making and better coordination. Cloud services also provide enhanced cybersecurity measures to protect sensitive military data from unauthorized access or cyber threats.

The military's use of cloud computing also enables efficient resource allocation. Military organizations can scale up or down computing resources and optimize their operations and resource utilization. Such flexibility also allows for easier integration of new technologies and systems, enabling rapid innovation and modernization. Cloud computing also facilitates data analysis and intelligence, providing military personnel with actionable insights and predictive capabilities.

Moreover, it enables proactive decision-making and strategic planning, ultimately enhancing the overall effectiveness of the mission. Additionally, the cloud offers improved disaster recovery capabilities, ensuring that critical data and applications are backed up and accessible even during unexpected disruptions or attacks. Cloud computing revolutionizes military operations by providing a secure, collaborative, cost-effective, and technologically advanced platform for information management and decision support.

3 INFOCOMMUNICATION SOLUTIONS

5G networks are a key communications solution to support the above capabilities, providing faster and more reliable connectivity for military personnel and information gathering and sharing assets in the field. This allows them to share critical information and

coordinate their operations more effectively, ultimately leading to better results on the battlefield. In addition, deploying 5G networks can also facilitate using emerging technologies, such as artificial intelligence and autonomous systems, to improve real-time situational awareness and decision-making capabilities.

A 5G standalone private network is a wireless communications network specifically designed for an organization or group, with full configuration, security, and management. Autonomous private networks use 5G technology to provide high-speed, low-latency connectivity for mission-critical communications applications and IoT devices. They can also provide wireless connectivity in remote industrial facilities, mining operations, and military bases where public networks are unavailable or unreliable.

Deploying 5G autonomous private networks to equipment supporting command and control in military operations requires careful planning and consideration. This includes conducting a feasibility study, defining the network architecture, selecting the appropriate spectrum, deploying and configuring the network infrastructure, and conducting a network architecture study. In addition, it is essential to ensure the security and resilience of the network as it will handle sensitive and classified information.

Regular network maintenance and monitoring will also be necessary to address any problems or vulnerabilities that may arise. Regular monitoring and evaluation of network performance can identify potential problems and ensure the network meets its objectives. Security measures, such as data encryption and access control, can be used to protect the network from potential threats. Regular testing and monitoring are needed to guarantee optimal performance and to detect potential problems. Once devices are installed, the network must be tested, optimized, maintained, and updated.

Network maintenance should be planned to meet the changing needs of, for example, military operations, ensuring that the network can handle the increasing amount of data generated by the deployed devices and remain secure against potential threats. For assets supporting military command and control, deploying a 5G autonomous private network has both potential advantages and disadvantages. Benefits include increased security, reliability, resilience, high-speed connectivity, reduced latency, and dependability. Organizations can tailor the network to their needs, including creating dedicated coverage areas, managing device connections, and optimizing bandwidth for different purposes. However, prospective drawbacks include the need for specialized equipment and infrastructure. In deciding whether to deploy a standalone 5G private network for command and control support devices in a military environment, it is essential to weigh the potential benefits and potential drawbacks, such as limited coverage, interference, implementation complexity, high deployment costs, inadequate network coverage, and regulatory concerns. 5G networks use higher frequencies, making them more susceptible to interference from other electrical equipment in many regions that have not yet been deployed (Tóth, 2022).

These developments will enable allied forces to stay at the forefront of the constantly evolving theatre of war and maintain their competitive edge. Military private 5G networks can also improve communication and coordination between different units and forces, enabling seamless integration and interoperability. Furthermore, the high bandwidth and low latency of 5G networks can support the transmission of large amounts of data, enabling faster and more accurate intelligence and analysis. This can greatly enhance the effectiveness of military operations and provide commanders with timely and actionable information.

Additionally, private 5G networks offer enhanced security measures, ensuring that sensitive military communications and data remain protected against potential cyber threats. The advanced encryption protocols and robust authentication mechanisms of 5G networks provide a secure and reliable communications infrastructure for military operations. Furthermore, private 5G networks enable faster and more efficient data transfer, allowing military personnel to share critical information and make informed decisions in real-time. This improved connectivity can ensure interoperability, significantly improving situational awareness and coordination between different units and ultimately improving the overall effectiveness of military missions.

For 5G, it is important to stress the performance and efficiency requirements of 5G mobile communication systems. Key performance indicators include user experience ratio, link density, latency, spectrum efficiency, and system energy efficiency. For military applications, priority, latency, reliability, user rate, mobility, connection density, security classification, and energy efficiency are defined as eight categories, as shown in Table 1.

Table 1 Key performance indicator system for 5G military applications

Key Performance Indicator	Feature	Value
Priority	The priority of the 5G network scheduling resources can be determined according to the priority assigned by the military mission priority, which can be dynamically adjusted in real-time according to the mission flow or the battlefield environment.	High: Real-time military tasks in the battlefield Middle: Cooperative training exercises Low: Logistical asset support tasks
Latency	It refers specifically to end-to-end delay, i.e., the time it takes for a terminal to send data to another endpoint to receive data while executing military tasks. The remote control service of an unmanned combat platform has higher requirements.	The 5G end-to-end delay should be less than 1 ms.
Reliability	It can provide reliable services for specific military missions under defined conditions and functions. It determines the reliability of	Weapon systems: 99.999% Command and control systems: 99.9%

	the network in the execution of military missions.	Service support systems: 99%
User rate	This is the guaranteed user speed under the actual load on the system. The user includes the fighter and the personnel support equipment and the radar and other sensors, missiles, and different weapon platforms.	The top speed of 5G can be up to 20 Gbit/s in the right conditions.
Mobility	It describes the maximum mobile speed supported under the given Quality of Service (QoS) and seamless transmission conditions. The target is high-speed moving objects such as aircraft, ships, and land combat vehicles. 5G focuses on overcoming Doppler shift and frequency switching.	High: >200 km/h Medium: 20-200 km/h Low: <20 km/h
Connection density	It represents the total number of online terminals supported per unit area. Online means that the terminal communicates with a given QoS level, especially in combat or military material support scenarios where several sensors are distributed and interconnected.	High: >1000 km2 Medium: 100-1000 km2 Low: <100 km2
Security classification	It refers to the level of security of the military services. They are logically separated according to their security level.	High: Secret Medium: Restricted Low: Unclassified
Energy efficiency	It represents the amount of data that can be sent and received per unit of energy used on the network and terminal equipment sides. This is primarily for the needs of the IoT, such as weapon sensors, surveillance systems and unmanned vehicles.	High: Weapon control systems Medium: Surveillance assets Low: Remote control

Source: Liao, Ou, 2020

CONCLUSION

The Russian-Ukrainian conflict has highlighted that today's military operations are based on a completely different basis than those of the past decades. The focus is on multi-domain operations, and the entire command and control structure must be adapted accordingly. A fundamental step in this process is the transformation of the headquarters system, which will support commanders in meeting the challenges they face with these new capabilities. This will require the creation of command posts that are sufficiently mobile and flexible to adapt to a rapidly changing operational environment.

Accordingly, they must be equipped with capabilities that can provide relevant information at any time, even during rapid redeployments and relocations. An excellent solution is to use cloud computing to integrate all data collection tools to provide commanders with the necessary information. The computing power of the cloud can contribute to a fast and accurate analysis of large amounts of incoming data so that the information available is always the most reliable. A communications solution for this

environment could be a private 5G network providing a robust, high-speed, reliable, and secure communications environment for cloud-based command and control systems.

This private 5G network would provide seamless connectivity between data collection devices and the cloud, enabling real-time information transfer. In addition, introducing advanced encryption protocols and authentication mechanisms would guarantee the security of sensitive data. Leveraging the power of 5G technology, commanders would have access to a highly responsive and low-latency network, facilitating rapid decision-making processes. This would significantly increase the effectiveness of military operations, as commanders could receive and analyze real-time data from multiple sources simultaneously. Thanks to the low latency provided by 5G, they could quickly assess the situation on the ground and make timely and informed decisions. Furthermore, this private 5G network would also support the deployment of autonomous vehicles and drones, allowing commanders to conduct intelligence and surveillance more efficiently. Seamless connectivity between the data collection devices and the cloud would ensure secure, uninterrupted, and undelayed transmission of information.

They all contribute to commanders having access to all information in the right place, at the right time, and in the right format, which means that they do not necessarily have to lead their troops from a fixed command post but can do so from their command vehicle, for example, ensuring a high degree of mobility and flexibility. This flexibility is key in modern warfare, where the battlefield constantly changes, and commanders must adapt quickly. Access to real-time information enables them to make informed decisions on the ground, adjusting their strategy and tactics as necessary. In addition, the ability to drive from command vehicles allows commanders to be closer to the action, giving them a better understanding of the situation on the ground. This proximity also allows faster communication and coordination with their teams, increasing operational effectiveness. In addition, having all information available in the right format ensures that commanders can easily analyze and interpret data, identifying patterns and trends that are key to success. By leveraging technology and advanced communications systems, commanders can effectively lead their teams in a dynamic environment while maintaining high situational awareness. This integration of information and mobility enables commanders to react quickly and decisively, ultimately increasing their effectiveness on the battlefield.

ACKNOWLEDGMENT

Project no. TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development, and Innovation Fund, financed under the TKP2021-NVA funding scheme, financed under the TKP2021-NVA funding scheme.

This research is supported by the National Media and Infocommunications Authority of Hungary.

REFERENCES

BEAGLE, M. – SLIDER, J. C. – ARROL, M. R. The Graveyard of Command Posts. *Military Review*. May-June 2023, p. 10-24.

FOX, A. C. On the Principles of War: Reorganizing Thought and Practice for Large-Scale Combat Operations. *Land Warfare Paper* 138 / June 2021, p. 1-18.

LIAO J. – OU, X. 5G Military Application Scenarios and Private Network Architectures. *2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications(AEECA)*. 2020, p. 726-732. DOI: https://doi.org/10.1109/AEECA49918.2020.9213507

NATO's Allied Joint Doctrine (AJP-01), Source: https://www.gov.uk/government/publications/ajp-01-d-allied-joint-doctrine

PERKINS, D. G. Multi-Domain Battle the Advent of Twenty-First Century War. *Military Review*. November-December 2017, p. 8-13.

RUSSELL, S. – ABDELZAHER, T. – SURI, N. Multi-Domain Effects and the Internet of Battlefield Things. *MILCOM 2019 - 2019 IEEE Military Communications Conference (MILCOM)*. Norfolk, VA, USA, 2019, p. 724-730.

TÓTH, A. The Use of 5G in Military Cloud of Things Solutions. *AARMS* Vol. 21, No. 3, 2022, p. 5–20.

Andras TOTH, PhD
1101 Budapest, Hungaria krt. 9-11. Hungary
toth.hir.andras@uni-nke.hu

Tibor FARKAS, PhD
1101 Budapest, Hungaria krt. 9-11. Hungary
farkas.tibor@uni-nke.hu

DOI: https://doi.org/10.52651/vr.a.2023.3.74-80
VOJENSKÉ REFLEXIE
ISSN: 1336-9202 (online)
2023, Number 3, Page 74-80

HUMAN SECURITY TODAY FROM THE JAPANESE PERSPECTIVE

Petra MARTAUS

ARTICLE HISTORY

Submitted: *30. 10. 2023*

Accepted: *06. 12. 2023*

Published: *31. 12. 2023*

ABSTRACT

The COVID-19 pandemic and at the same time, the largest number of violent conflicts since 1946 are causing record-high numbers of people to be forcibly displaced from their homes. That includes the Israeli-Hamas conflict and war on Ukraine, which is not only causing immense human suffering but is also playing a role in precipitating a global food, energy, and financial crisis. As a result, the world now faces its worst cost-of-living crisis in a generation. This paper sets out the human security today from the perspective of japanese foreign policy.

KEYWORDS

Japan, human security, military expenditure

INTRODUCTION

According to UNDP´s Human security special report, just before the COVID-19 pandemic hit, as the world reached unprecedented development levels, six of every seven people around the world felt insecure. And this feeling of insecurity was not only high—it had been growing in most countries with data, including a surge in some countries with the highest HDI values. Indeed, as many development indicators were moving up, people's sense of security was coming down. This is also related to Japan´s recent announcement about increasing military spending.

The human security approach has long been championed by Japan as a backbone of its foreign policy and in its engagement with UNDP globally. For decades, Japan has been putting the human security concept into practice across the world. The concept of Human Security is deeply imbedded in Japan's own development history. Japan has focused on building its Human Security through investments in education, health, rule of law, and disaster risk reduction. These efforts, together with its economic growth, are now attributed to the country's development success. But will increase of military spending affect country´s development activities around the world?

1 ORIGINS OF HUMAN SECURITY

Human security has been understood very differently through all the years since its introduction in Human Development Report 1994, prepared by the United Nations Development Programme. Human Development Report introduced the concept of human security as a novel way of thinking about security along seven interrelated areas — economic security, food security, health security, environmental security, personal security, community security, and political security. We can see, how all of these seven pillars of human security are mutually interlinked, how all human needs are closely connected. Poverty and inequality are undoubtedly a cause of violence and crime.

The origin of the concept was tied to a specific moment in our history: the Cold War was over and there was hope for a new period of international relations guided by meaningful multilateralism. Human rights issues came to the fore. Originating out of the human development discourse, human security was considered as being rooted in the "freedom from fear" and the "freedom from want".

As report argues "The concept of security," has for too long been interpreted narrowly: as security of territory from external aggression, or as protection of national interests in foreign policy or as global security from the threat of nuclear holocaust.... Forgotten were the legitimate concerns of ordinary people who sought security in their daily lives." This opinion was one of the reasons, why human security has also been subjected to sustained critique. Roland Paris critics suggested that human security is so vague that it verges on meaninglessness—and consequently offers little practical guidance to academics and who might be interested in applying the concept, or to policymakers. Almost 30 years later, international relations have aligned themselves around new concerns and are being driven by different forces. According to Buzan and Hansen human security has contributed to 'deepening' (from the state to the individual) and 'widening' (from state and military security to economic, environmental, etc.) the concept of security from the Cold War focus on military defence of the state to include a much broader and comprehensive set of concerns. Human security is still often framed more as an aspirational agenda persistently debated in academic and policy-making circles, with its future impact open to speculation. But it has nevertheless left its imprints on policy, practice, and research.

Discussions about human security undermining state security (and vice versa) are still widespread. No doubt, instinct to prioritise state security may seem natural during such crises as Russia´s invasion to Ukraine or Israeli-Hamas war. However, doing so at the expense of human security, according to Anna Brach, may negatively impact prospects for peace and efforts to build security. This, however, doesn´t mean the human security approach rejects the role of the state as a provider of security for its own people[1], but rather the approach argues that states are providers of security for individuals in ideal conditions, with recognition that sometimes states endanger human security. Furthermore, the approach as a challenge to state-centric approach changes the sovereignty of the state from absolute sovereignty to conditional sovereignty.

The concept of human security will obviously be part of the wider discussion on security in the near future. It continues to play an important role within the UN, EU and

[1] On the contrary, it has opened practical possibilities of human security – the notion that governemnts and international institutions take responsibility for wellbeing of its individuals and communities in which they live.

NATO, despite the fact that the operationalization of the concept still strongly reflects the interests of the states. Anyway, academics and policymakers in relation to human security can be currently placed into three categories:

i) those, for whom human security appears to be an attractive idea, but lacks analytical rigour,
ii) those, who accept concept of human security, but insist on limiting it with a narrowly conceived definition (focused on factors causing violence),
iii) those, for whom a broad definition of the concept of the human security is an essential tool for understanding current crises in context of human rights and development issues.

Even though the professional public still did not agree on the defenitive meaning of the concept of human security and the extent to which the concept can be applied, everyone agrees on relevance and validity of the concept—despite the criticism.

2 NARROW VS. BROAD UNDERSTANDING OF HUMAN SECURITY

Surrounding discussions of the 1994 report, as mentioned above, have led others to judge the concept of human security to be too all-encompassing for practical purposes, the report idealistic, and its recommendations naïve. While some of the harsher criticisms bear further discussion, it is fair to argue that the conceptual distinction between human development and human security was not sufficiently clear, as the dimensions do seem to embrace the entirety of the human development agenda unnecessarily. If human security is to be a feasible agenda it must be narrower. In this connection state and international developments in human security showed states and international organizations have focused on narrow definitions of human security that prioritize the category of personal security.

Today we can see growing interest in human security especially within NATO and some national militaries, notably the UK. For both UK and NATO, according Mary Kaldor, human security is understood as un umbrella concept that encompasses Building Integrity (anti-corruption), Protection of Civilians, Cultural Property Protection, Children and Armed Conflict, Conflict-related Sexual and Gender-based Violence, Human Trafficking and Women, Peace and Security.

Next state which for a time championed the human security concept, is Canada, also focusing on physical threats as the core indicator of threats to human security. This approach reflected a narrowing of human security to just ‘freedom from fear’, focusing on crisis prevention or conflict management. It left aside the dimensions of the human security concept that emphasised immediate but non-violent threats to people. Norway likewise focuses on the freedom from fear aspects of human security, The Armed Forces have a special role to play in creating security, and are required to pursue an integrated approach to human security in operations at all levels, as Norway´s National Action Plan: Women, peace and security (2023-2030) sets forth.

According to United Nations, human security is a multidimensional analytical framework that can assist the United Nations system to assess, develop and implement integrated responses to a broad range of issues that are complex and require the

combined inputs of the United Nations system, in partnership with Governments, non-governmental entities and communities.

3 HUMAN SECURITY IN JAPAN´S FOREIGN POLICY

Canada and Japan were the first countries to include this concept in their foreign policy. Japan maintains the broadest definition of human security, which "comprehensively covers all the menaces that threaten human survival, daily life and dignity… and strengthens efforts to confront these threats." A year after the UNDP issued its report, in a speech in the United Nations, Prime Minister Murayama Tomiichi endorsed human security as an important idea for the UN. Murayama's endorsement made Japan one of the first countries to offer its support to the human security idea.

Japan was searching for an international role commensurate with its considerable economic power and the Japanese government had began to take measures to strengthen Japan's international contribution. In 1994, Murayama had been elevated to prime minister from the post of chairman of the Japan Socialist Party (JSP), and his support for human security can be seen as rather natural, given the fact that the human security concept is non-military in nature and fitted like a glove to his party's highprofile pacifist stance.

Nevertheless, as some mentioned, it was Keizo Obuchi in 1998, which put a cornerstone of the commitment to human security in Japanese foreign policy. He mentioned health and employment as "human security" concerns and showed an intention to enhance cooperation in this area further by putting priority on social development in Japan's Official Development Assistance (ODA) policy. Related to the promotion of human security, Obuchi announced that the Japanese government would establish the "Human Security Fund" under the United Nations. Establishment of this fund was initially purported to provide flexible and timely financial support for international organizations eager to implement projects in Asia. The rest of the world was not included in the scope of the fund, but when the Human Security Fund was established, the fund became available to projects implemented in any part of the world. In a speech in Tokyo on December 2, 1998, Obuchi said:

"An unavoidable fact is that Asia's remarkable economic development in recent years also created social strains. The current economic crisis has aggravated those strains, threatening the daily lives of many people. Taking this fact fully into consideration, I believe that we must deal with these difficulties with due consideration for the socially vulnerable segments of population, in the light of 'Human Security,' and that we must seek new strategies for economic development which attach importance to human security with a view to enhancing the long term development of our region." (AKIYAMA, 258-259)

Japan posed a different case as the country seeks to broaden the scope of human security. From the Japanese government's point of view, human security encompasses not just the security from the threat of aggression in wars, but also the fundamental needs of citizens. The Japanese government takes a more comprehensive view of the UNDP's definition of human security as it believes human security should be safeguarded even during the absence of conflict. Thus, for Japan, human security comprehensively covers all the measures that threaten human survival, daily life, and human dignity, such as

environmental degradation, human rights violation, transnational organized crime, illicit drugs, refugees, poverty, anti-personnel landmines, and infectious diseases. Consequently, Japan stands out differently from Western countries like Norway and Canada, which have concentrated solely on issues of arms control while overlooking the security of human life during peace time. Both ideas of "freedom from want" – as initiated by Japan and UNDP and "freedom from fear" as affirmed by Canada and Norway – mutually constitute the understanding of the concept. It doesn´t mean that Japan prioritizes "freedom from fear" over the "freedom from want", but holds them as dual objectives of human security.

In 2000, the Ministry of Foreign Affairs added a grassroots human security program to its grant aid portfolio within Human Security Trust Fund. All the issues identified in the human security agenda, moreover, are amenable to action through existing ODA programs. Governmental agency that delivers the bulk of ODA for the government of Japan is called The Japan International Cooperation (JICA). This aid is distributed through embassies abroad mostly for small-scale social development projects. JICA is the agency committed to the links between human security, peace-building, and development. This shift is visible in JICA's development activities regarding transition situations between conflict and peace in fragile states or conflict-affected countries like, for example, Afghanistan, Iraq or Cambodia.

According to some, human security was a *„godsend for Japanese aid policy makers, because it provided a way to make a contribution to the maintenance of international security without having to engage in the politically delicate tasks of constitutional reinterpretation or commitment to increased military spending"*. (Potter, 50)

As Edstrom mentioned, the japanese poliucy makers downgraded human security from a key foreign policy pillar to simply a basic principle of ODA after the intervention in Afghanistan and Iraq. After 2001, human security continued to inform japanese development assistance but aid also began to be used as a tool of counter-terrorism, an issue that straddles the demarcation between hard and soft security. Have these changes in Japan's approach to development assistance affected aid allocations?

3.1 Human security and military expenditure

According to new data on global military spending published by the Stockholm International Peace Research Institute (SIPRI), world military spending is increasing, with new historical levels year by year. Japan last year announced that it plans to increase defense spending over the next five years as it faces an increasingly assertive China and an unpredictable North Korea.. (Carnegie endowment for international peace, february 2023) It intends to raise defense spending to 2 percent of GDP by 2027. This will give the country the third-largest defense budget in the world. Japan's new national security strategy explains how it will take primary responsibility for its own defense within five years and assume a far more active role in Indo-Pacific security. So the question is, will aid (or human security gaps) allocations be affected by increased military expenditure?

In response, authors of the document „The human security case for rebalancing military expenditure" argued that *„savings from military expenditure reductions could make an important contribution to the rising need to meet challenges such as extreme*

poverty and climate change, but threats and risks to human security cannot be met by reallocating funds from military spending alone. However, the goal of that paper was not showing that reductions in military expenditure can help improve all dimensions of security, but attempt to initiate discussions on opportunities for further, wide-reaching reductions of global military expenditure in the future and rebalancing security spending." (Brzoska – Omitoogun – Skons, 29)

CONCLUSION

The reasons why governments put forward to justify the levels of their military expenditure are often based on concern about military threats to their states and peoples. This can also be applied to Japan case. Yet a large and increasing number of the threats facing people and states across the world are not military in nature. Extreme poverty, persisting hunger, natural disasters, political and criminal violence, the consequences of armed conflict, climate change and other environmental changes cannot be addressed by military means. These are still threats to security of people but also that of states, communities and societies.

Undoubtly, Japan still needs to be considered as a significant and key actor in international politics due to its role as a leading provider of overseas foreign aid. The standard of human security implies a reconsideration of spending on the military in view of the demands of non-military risks and threats. But concerns, that are based on a traditional understanding of security that focuses on the protection of territory and the state order, must be taken seriously, too. So in my opinion, following recent events, it is necessary for Japan to link the objective of effective spending military expenditure to border security assessments. Only then it will be possible to find a balance between the resources spent on military and human security.

REFERENCES

AKIYAMA, N. (2004). Human Security at the Crossroad: Human Security in the Japanese Foreign Policy Context, in Hideaki Shinoda and Ho-Won Jeong, eds., Conflict and Human Security: A Search for New Approaches of Peace-building, IPSHU English Research Report Series No. 19 (Hiroshima: Hiroshima University, Institute for Peace Science).

BOSOLD, D. – WERTHES, S. (2005). Human Security in Practice: Canadian and Japanese Experiences (IPG I).

BRZOSKA, M. – OMITOOGUN, W. – SKONS, E. (2022). The Human Security Case for Rebalancing Military Expenditure. Stockholm International Peace Research Institute.

BUZAN, B. – HANSEN, L. (2009), The Evolution of International Security Studies (Cambridge: Cambridge University Press).

EDSTROM, B. (2011). Japan and Human Security: The Derailing of a Foreign Policy Vision. Institute for Security and Development Policy. ISBN: 978-91-86635-07-7. pp. 7-8.

HAMA, H. (2017). State Security, Societal Security, and Human Security. Jadavpur Journal of International Relations. 21. DOI: 10.1177/0973598417706591.

HUMAN SECURITY HANDBOOK. Jan. 2016. See [https://www.un.org/humansecurity/wp-content/uploads/2018/05/HS-Handook_rev-2015.pdf]

KALDOR, M. – RANGELOV, I. (2023). Human security in future military operations. In: Routledge Hadbook of the future of Warfare. Taylor and Francis Inc., ISBN: 9781032288901. pp. 41-51.

KALDOR, M. (2023). Paradox of human security. See [https://www.gcsp.ch/publications/paradox-human-security] accessed September 21, 2023

Norway´s National Action Plan: Women, peace and security (2023-2030). See [https://www.regjeringen.no/contentassets/a2aec6a0bf874885a1f78eb5d9674339/en-gb/pdfs/women-peace-and-security.pdf]

ROLAND, P. (2001) Human Security: Paradigm Shift or Hot Air?, International Security, 26(2): 87-102.

United Nations Development Programme. 2022. 2022 Special Report on Human Security. New York.

United Nations Development Programme. Human Development Report 1994 (Oxford University Press 1994), p. 24-25.

Petra Martaus

Ministry of Defence of the Slovak republic

0960 303 141

petra.martaus@mod.gov.sk

Information for authors:

Submission deadline

- for papers to be published in **issue 1** in Slovak / Czech language **30th April**
- for papers to be published in **issue 2** in Slovak / Czech language **30th October**
- for papers to be published in **issue 3** in English language **30th October**

Template - **http://vr.aos.sk/index.php/en/for-authors-vr.html**

VOJENSKÉ REFLEXIE

AOS

VOJENSKÉ REFLEXIE

Military science journal

Publisher:

Akadémia ozbrojených síl
generála Milana Rastislava Štefánika
Demänová 393
031 01 Liptovský Mikuláš

Electronical journal published on internet with free access
http://vr.aos.sk/index.php/sk/

Published twice a year in Slovak/Czech and once a year in English

Number of pages: 81

Published:

December 2023, Volume XVIII, Issue 3/2023
Photocover: Peter POLDRUHÁK
Cover: Dušan SALAK

ISSN 1336-9202 DOI https://doi.org/10.52651/vr.j.2023.3

DOAJ

ERIHPLUS
EUROPEAN REFERENCE INDEX FOR THE HUMANITIES AND SOCIAL SCIENCES

AKADÉMIA OZBROJENÝCH SÍL
GENERÁLA MILANA RASTISLAVA ŠTEFÁNIKA