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