HADMÉRNÖK
VÉDELEMINFORMATIKA

18. évfolyam (2023) 4. szám 109–128.
DOI: 10.32567/hm.2023.4.8

Mátyás Ináncsi,[1] Péter Bányász,[2] Máté Dub,[3]
Péter Kugler[4]

Empirical Studies of Russian–Ukrainian War Related Fake News, Part 1[5]

Abstract

The Russian–Ukrainian war, which broke out on February 24, 2022, resulted in several paradigm shifts in cyber warfare. One aspect of these changes is psychological operations. Russia and Ukraine have conducted extensive psychological operation campaigns to fulfil their war objectives, which have since been intense along modified intentions. This series of studies examines the impact of war-related fake news through various empirical research. In the first part of the paper, the authors examine the emergence of psychological operations and related terms in the international academic literature using network analysis methodology. In the second part of the paper, the authors use sentiment and network analysis to investigate the spread of different fake news. In the third study, the authors measure the attitudes toward the perception of the Hungarian Defence Forces from the perspective of the war in the neighbouring country.

Keywords: Russian–Ukrainian war, PSYOPS, cyber warfare, network analysis, sentiment analysis

[1] Ludovika University of Public Service Faculty of Military Science and Officer Training, e-mail: inancsi.matyas@uni-nke.hu
[2] Ludovika University of Public Service Faculty of Public Governance and International Studies Department of Cybersecurity e-mail: banyasz.peter@uni-nke.hu
[3] Ludovika University of Public Service Faculty of Military Science and Officer Training, e-mail: dub.mate@uni-nke.hu
[4] E-mail: kugler.peti@protonmail.com
[5] TKP2021-NKTA-51 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NKTA funding scheme.

Introduction

The Russian–Ukrainian conflict has been dragging on since 2014, and is an unresolved situation affecting our daily lives. Following the Euromaidan protests which began in 2013, and the revolution that led to the ousting of pro-Russian President Viktor Yanukovych in February 2014, pro-Russian unrest broke out in parts of Ukraine.[6]

The two parties finally concluded the Minsk agreements in 2015, however, several disagreements have blocked their full implementation due to both Russia and Ukraine repeatedly violating the treaty, accusing the other. The frozen conflict finally broke out in February 2022, by a military operation launched by Russia on February 24, 2022. This action has surprised the broad public and most experts, even though Ukraine, the NATO, and Russia had conducted large-scale information operations before the war began.[7] The United States, its allies, and Ukraine as a state with increasingly close ties to the United States have regularly accused Russia of preparing a military attack on Ukraine. Meanwhile, Russia has accused – and continues to accuse – Ukraine, using a constantly changing narrative, which is often more and more absurd, to portray itself as a victim of this incident to justify its military aggression.[8] Recurring accusations include that the Nazi Ukrainians (see Figure 1) carried out systematic genocide against the Russian minority, Ukraine is harbouring nuclear weapons to destroy Russia, or that a new type of coronavirus was developed in Ukrainian biological laboratories with U.S. support to build a new world order.

Figure 1: Russian articles about Ukraine that mention Nazism
Source: SMART 2022

[6] The present study does not aim at a detailed description of the war since 2014, but we recommend the studies by József Padányi and János Tomolya, in which they described the events in a complex approach. Padányi–Tomolya 2017a: 63–83. Padányi–Tomolya 2017b: 29–42.

[7] Alekszejeva et al. 2023.

[8] Examples include the history of the Ukrainian bio-labs before the outbreak of the war, and shortly afterwards, or when President Putin and Valery Zorkin together looked at a 400-year-old map on which they claimed there was no Ukraine.

The psychological operations that form part of information operations were significantly intensified on all sides after the start of the war.

The first part of this series of studies aims to define the concepts at the heart of our research, their relative positions, roles, and elements based on military terminology, strategic documents, and the national and international literature.

Methods

In the first half of our study, we reviewed the relevant international and national literature for the following stages of our research. We then searched the Scopus database, looking specifically at how the keywords disinformation, misinformation, or malinformation appear in the relevant international literature.

The results are summarised by year in a chart in the results section. Only a subset of the older scientific papers is recorded in Scopus, so older datasets may, in reality, have more publications than were digitised.

The Scopus system allows the export of up to 20,000 hits at a time, which proved sufficient for the present research. The data were saved in CSV format, and were analysed using VOSviewer version 1.6.19.[9]

Before describing the results of our empirical research, we should consider the relevant concepts.

Hybrid warfare

Although hybrid warfare cannot be considered a directly examined element or part of the narrowed, specific research question, we believe it important to define it in the context of the conceptual outlook. The primary reason for this issue, is that hybrid warfare can be part of information and psychological operations.

In the international literature, there is no consensus on the definition of hybrid warfare, nor on whether it is exclusively attributed to General Valery Vasilievich Gerasimov. Whether he unified the components that already existed and were used, or whether the term "hybrid" as implemented by the West or Gerasimov's original, i.e. the "indirect and asymmetric methods" version, is used in connection with the designation.[10] In this context, the diversity of terminology is illustrated by the fact that the present concept can be referred to as non-linear, next-generation, or fourth-generation warfare or, in some elements, as "grey-zone" activity.[11] However, there is a similarity in terms of the content, i.e., hybrid warfare consists of two main components, military and non-military methods, which contribute to achieving

[9] Comma-separated values is an English abbreviation for a particular separator, usually using a comma or semicolon to separate different values and a row representing a record. For the computer, it is easy to process as a spreadsheet and, because of the lack of formatting, is ergonomic. Its simplicity makes it widely compatible across different operating systems and platforms.

[10] Raychev 2019: 127–151.

[11] Bērziņš 2020: 355–380.

a given objective. In terms of actors, both state and various non-state actors can be identified. General Gerasimov attempts to illustrate with the new rule that non-military means have become more important in achieving political and strategic goals, and often prove more effective than weapons.[12] Regarding non-military means, we can define, among others, political, legal, diplomatic, financial, economic elements, sabotage, social pressure, influence operations, propaganda, and, in the latter case, additional means resulting from cyber capabilities.[13]

Concerning operations in cyberspace, it is important to underline that they can apply to both military (e.g. electronic warfare) and non-military (e.g. psychological operations) components.

NATO defined hybrid threats in its 2014 Wales Summit, specifically in its Closing Declaration, as a set of broad, covert, and overt, military and paramilitary, as well as non-military, procedures and means in the context of a predefined, integrated operational plan.[14]

In 2015, the NATO Parliamentary Assembly's Defence and Security Committee defined hybrid warfare as the use of asymmetric procedures from the attacker's side, whereby non-military means are used to identify and exploit weaknesses and the procedures are tailored to the situation at hand, and then combined with conventional and non-traditional military threats/concrete attacks.[15] In contrast, the EU defines hybrid threats in more detail, as a set of activities that are used by state or non-state actors in a coordinated manner to achieve certain objectives, while not going beyond the officially declared level of warfare. The emphasis is generally on exploiting the vulnerabilities of the target state and creating situations that impede decision-making. Hybrid threat tools also include strong misinformation or disinformation campaigns, whereby attackers use social media platforms to influence the political narrative and to radicalise, recruit and control proxy actors.[16] The social media platforms that are the focus of our research, are defined in the EU terminology and because of their role in information warfare, more specifically in psychological operations, we consider this definition the guiding one.

In summary, hybrid warfare is a coherent and complex system of violent means and threats whereby the attacking party uses a wide range of available assets (military, irregular or non-military) to achieve its objective. In the face of these attacks, it is essential to develop an appropriate defensive methodology, an important element that is to identify the interests, intentions, political objectives and resources of the opposing actor or actors. Knowing the opposing actor's strategy can help refine and improve the effectiveness of defensive solutions and, where appropriate, build consensus or prepare for a possible conflict.[17]

[12] Gerasimov 2013.
[13] Simicskó 2017: 3–16.
[14] NATO 2014.
[15] Kiss 2019: 17–37.
[16] European Commission 2016; Kiss 2019: 17–37.
[17] Van Puyvelde 2015; Kiss–Somodi 2019: 22–28.

The information environment, battlefield and operations

In this section, we discuss the information environment, and more importantly the three dimensions of it. Extending on this, we examine the concept – depending on preferred wording – of information battlefield, information warfare and information operations. We approach this concept from the NATO's definitive perspective.

The information environment

The development of the information environment has accompanied the spread of different ICT tools.[18] The information environment also contributes to the possibility of expanding military operations. The United States of America's Combined Forces Information Operations Doctrine of 2012 (revised in 2014) defines the information environment along the following lines. It is defined as individuals, organisations, and systems which collect, process, and distribute information. According to the document, this environment has three interrelated dimensions that constantly interact with individuals, organisations, and systems. These are the physical, information and cognitive dimensions. The physical dimension includes the leadership and governance systems, key decision-makers and supporting infrastructure that enables individuals and organisations to function effectively. The information dimension defines where and how information is collected, processed, stored, disseminated, and protected. The cognitive dimension includes the people who transmit, receive and act on information, and those who act on it.[19]

Going back to Gerasimov's approach, the forces and methods used are more important to coordinate in the information space than in the physical dimension.[20] Regarding the Hungarian definition of terms, the Hungarian *Encyclopaedia of Military Sciences*[21] does not differentiate from the US JP 3-13 regarding essential elements.[22]

Information battlefield, warfare/operations

In the context of the information battlefield, the Hungarian *Encyclopaedia of Military Sciences* defines it as a multidimensional operational space where information activities for military purposes occur. In accordance with the Hungarian interpretation, the information battlefield and the information environment are correlated since they are all physical and online spaces, places, systems, devices, and human resources where information is acquired or produced, used, protected, and stored. This interpretation

[18] Farkas 2023: 11–30.
[19] Joint Chief of Staff 2014.
[20] Rácz 2014.
[21] Under the Hungarian encyclopaedia of military sciences terminology, we refer to Zoltán Krajnc's *Hadtudományi lexikon*. In order to not to break the flow of the English text, we have translated the name of the document, however, the document has no official English name, and we have used a straightforward direct translation. By this reason, English translations of this document in different publications might differ.
[22] Krajnc 2019.

is also complemented by the technological and cognitive information processes and the struggle to acquire and use information as efficiently as possible.[23]

In the Hungarian terminological interpretation, information operations and warfare appear as separate terms in the Hungarian *Encyclopaedia of Military Sciences.* In this interpretation, information warfare can be divided into two main parts. According to one interpretation, information warfare is a new form of warfare in the classical sense, aiming to attack information systems and use information tools to achieve military objectives as an integral part of warfare. The second interpretation, which is also closer to the scope of our research, is that information warfare can be understood in the context of the information environment described above, and refers to the technical and cognitive information activities of an offensive or defensive nature that take place in this environment.[24] It is important to specify, that information warfare is more a Russian or Chinese definition, while the term information operations is more a NATO term.

In the context of NATO's interpretation of information operations (INFOOPS), the following concepts have been defined:[25]

- Information operations are a set of military activities that provide advice and coordination of military information activities to have the predefined, desired impact on and knowledge of the target group(s), adversaries, and their capabilities and to support the activities of the Alliance
- Information operations are activities aimed at influencing information and information systems. Any actor may conduct them and may include protective measures

The document also discusses in detail the relationship between information and the global security environment, strategic management, non-lethal activities, the relevance of information, the role of the media, and the importance of technology and the internet in information operations. The document identifies as relevant to decision-making, the triad of will to act following strategies, the right assessment of the situation, and the capacity to act appropriately, with the desired impact not being achieved even if one of these criteria is missing.[26]

In this context, the main objective is defined as influencing the capabilities and will of the opponent. It is also an important declaration that information operations can be used in the full range of military operations in support of and for their execution.[27]

NATO defines the following categories as areas of application for information activities:

- information activities that focus on changing, influencing, or reinforcing a particular position/situation
- information activities that focus on preserving and protecting the Alliance's room for manoeuvring in the information environment by protecting data and

[23] Krajnc 2019.
[24] Krajnc 2019.
[25] NATO 2009.
[26] Haig 2011: 12–28.
[27] Czeglédi 2017: 74–87.

information that support the Alliance's decision-makers and decision-making processes
- information activities that focus on countering command and control functions and capabilities by influencing data and information supporting adversaries through command and control, intelligence, surveillance, target detection, and weapons systems information[28]

The document's list of capabilities, tools, and techniques used in (and in support of) information operations is considered to be of particular relevance to our research and includes the following categories:
- psychological operations (PSYOPS)
- presence, posture, and profile (PPP)
- operations security (OPSEC)
- information security (INFOSEC)
- deception (MILDEC)
- electronic warfare (E.W.)
- physical destruction
- key leader engagement (KLE)
- computer-network operations (CNO)
- civil-military cooperation (CIMIC)[29]

The Hungarian military terminology of information operations adopts the NATO interpretation and a separate interpretation of information operations. In addition, it emphasises that three main objectives must be applied to support the commander and the mission at the appropriate level, which are:
- to weaken the enemy target group(s)
- strengthening the commitment of the friendly target group(s)
- gaining the support of uncertain or uncommitted target(s)[30]

In addition, it should be noted that the U.S. Joint Forces Information Operations Doctrine (J.P. 3-13) further defines various cyberspace operations (cyber operations)/ cyberspace capabilities as activities supporting information operations. These include but are not limited to influencing decision-making processes, influencing communications or the cognitive dimension of the target, compromising individuals or encrypted messages, and overall reducing the capabilities of the defending party.[31]

[28] NATO 2009.
[29] Pozderka 2016: 131–141.
[30] Krajnc 2019.
[31] Joint Chief of Staff 2014.

The psychological operations

Psychological operations aim to influence the selected target group in the cognitive dimension.[32]

The following main aspects can be identified concerning the diversification of the objectives of psychological operations:

- influence the thinking, feelings, and behaviour of the opposing side
- strengthen the support of friendly and loyal populations in order to achieve political and military objectives
- gain the support and cooperation of uncommitted or undecided target group(s)
- reduce the impact of the adversary's psychological operations on its resources and on groups to be protected

Above all this, the success of these operations depend on the attacker's ability to precisely define the target group and the content of the message, which is being delivered, and the delivery method must not be compromised.[33]

The conceptual interpretation of psychological operations is defined in the Information Operations Doctrine of the Hungarian Defence Forces along the following lines: PSYOPS is a method of influencing a selected target group's behaviour, attitudes, and opinions to achieve predefined PSYOPS objectives agreed upon by the supervisor. To achieve this, PSYOPS activities are designed to trigger or reinforce the desired behaviour of the target group, which will help to achieve the defined long-term objectives. The target of psychological operations may not only be the population of the enemy country but may also be directed at influencing the population of allied or neutral states, and may even be the population of the country or a group of them.[34]

Regarding NATO, it should be added that PSYOPS plans and activities should be consistent with the strategic guidelines for the activities and objectives set out in the Operation Plan. PSYOPS should also maintain direct control over the specific "content" along with its dissemination and, concerning this, the target group. In addition, effective psychological operations are resource-intensive. These resources include adequate intelligence information, language support, dissemination (graphics, print, broadcast, radio, telephone, television, physical press, voice, etc.) mechanisms, appropriate technological tools, and human factors.[35]

When targeting messages or content, the attacker should select credible topics, which should be developed with a particular focus on the vulnerabilities of the target group. The main objective is to ensure that the message/content is credible, receptive to the target group, and influential. Therefore, the topic to be targeted should be real, credible, and verifiable based on appropriate background information. It should also support the objectives of the own action and the psychological operations and set a course of action for the target group that is reasonable and realistic.[36]

[32] Bányász et al. 2019: 111–133.
[33] Haig 2018.
[34] Bányász et al. 2019: 111–133.
[35] NATO 2009.
[36] Haig–Várhegyi 2005.

Concerning the planning of psychological operations, we can identify three methods according to its classical interpretation:

1. Reflexive control: a strategy intended to influence the decision-making mechanism of the commander of an enemy force. The first step in the method is extensive reconnaissance, followed by penetration of the decision-maker's information systems. Here, disinformation is planted in such a way as to support the attackers in making desired decisions.
2. The concept of a social virus: a society can be infected from within if people in a certain position spread fake news. They can be undercover attackers or so-called opinion leaders who can be recruited to influence opinions even under a "foreign flag". They are usually spread among people who are ideologically manipulable, politically aggrieved, and not objectively informed about current events. Opinion leaders and influencers can be easily identified through networks, allowing the preparation of psychological operations and their detection from a defensive point of view.
3. In order to influence the perception of reality and reduce the psychological stability of a person or a group, not only traditional methods such as leaflets or media platforms can be used, but also special methods and tools. Artificial intelligence research is one of the most important branches of such tools. For example, "deepfake" technology uses machine deep learning to deliver audiovisual content in which another person's face or voice is superimposed on real-time content. Fake news on social media can be easily identified by recognising certain patterns, but such technology makes it difficult for even the most experienced person to spot fake news, and technological advances will further reinforce this trend.[37]

Concerning psychological operations, it is also important to explain further concepts. One of the main concept of psychological operations is the use of propaganda. However, it is important to keep in mind that propaganda is a tool that can be used under different psychological operations. The same rule also applies to fake news, disinformation, misinformation and malinformation.

Propaganda

In popular discourse, psychological operations are often confused with propaganda, but propaganda is, in fact, only a part of psychological operations and, contrary to popular terminology, not a condition for promoting a specific political ideology.[38] For grouping, three categories can be defined:

- White propaganda: It has a known intermediary and usually contains truthful information from a credible source. Its tools often include jokes and caricatures to ridicule and discredit the opponent

[37] Bányász et al. 2019: 111–133.
[38] Miller 2015: 163–188.

- Black propaganda is a form of communication that is not truthful, and is usually disguised in order to deceive the target audience. The cover-up can make it appear as if the source of the propaganda is the government rather than the opponent
- Grey propaganda: The source of the news in this category is unknown, and the primary objective is to demoralise the enemy by spreading fake news that is essentially about the enemy. Such propaganda news is used to reduce morale. Fake news often originates from the "hinterland" and can cover topics such as the destruction of soldiers' families or the infidelity of their wives and sweethearts

Propaganda and its content can be defined as reinforcing an over-emphasised point of view by disseminating true or false information to pursue a specific interest. The aim is, therefore, to persuade the target group with the full presence of bias. Propaganda can be used for political, economic, or military purposes, to demoralise the citizens of other countries, to target so-called "soft targets", to reach large masses of people, or to achieve a desired attitude. Historical examples show that the controlled, conscious dissemination of information is a key tool in propaganda campaigns. Among its elements, we can also identify the encouragement to accept a simple statement without criticism, broad formulations, familiar language, slogans, call words, symbols, illustrations, appeals to desire, and various elements of prestige.[39]

In terms of classification of propaganda, we can distinguish, among others, the following categories:

- using mental influence
- bandwagon technique
- plain folk technique
- fear-mongering
- testimonial/reporting
- false dilemma poser
- slogan-based
- statement-type
- operating with fragments of text[40]

Fake news, disinformation, misinformation and malinformation

The term "fake news" is often referred to in everyday language, but from a scientific perspective, it is important to fragment this concept and define exactly what can be included in this interpretation category. In principle, untrue or false news, fake news should be considered a generic term encompassing several approaches and criteria, requiring new definitions to be added, which may not be directly considered fake

[39] Dobák 2022: 93–124.
[40] Betts 2021.

news. From the point of view of the criteria and in order to define them accurately, two main questions need to be answered:

- Are we concerned with true or false information?
- Is the person disseminating the information aware of the consequences of disseminating the information?

By answering the questions, three categories can be identified:

- If the purpose is the deliberate, misleading, malicious dissemination of false/untrue information, then disinformation can be defined. This category can be divided into the group of fake news.
- If false/untrue information is disseminated so that the disseminator is unaware that the information he/she is disseminating is untrue, without deceptive intent or bad faith, misinformation can be defined as misinformation. This category also falls into the category of misinformation since the information is false, even if the person disseminating it is unaware of it.
- If the information is true/true, but its dissemination is misleading and has the wrong intention, it can be defined as "malinformation". (In Hungarian, this term is often called incorrect or bad information.) Unlike the previous ones, this category cannot be classified as fake news because although the dissemination is intentional and the intention is wrong, the information is true.[41]

Researchers have approached the problem of fake news from various perspectives on different topics. These include but are not limited to how governments and international organisations can regulate fake news, specifically disinformation disseminated online. In these activities, the main argument is to defend against challenges to democracy.[42]

In this context, EU terminology includes two additional terms: disinformation and misinformation. The Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee, and the Committee of the Regions on the Action Plan for Democracy in Europe defines the following related terms:

- Information influence operation: means a concerted effort by domestic or foreign actors to influence a target audience by deceptive means, including suppression of independent sources of information and disinformation
- Foreign interference in information space: a set of coercive and deceptive efforts designed to interfere with and prevent the free formation and expression of the political will of individuals by a foreign state actor or its agents[43]

In summary, fake news, disinformation, misinformation, and malinformation pose a particular risk to our security, and these threats include:

- misleading, uncontrolled information that may be a threat to the security of society

[41] Aïmeur et al. 2023.
[42] Jungherr–Schroeder 2021.
[43] European Commission 2020.

- decreasing social trust in the credibility of the media
- foreign interference in economic, political, and social processes and groups
- threats to clean and transparent democratic political processes, such as manipulation of election campaigns
- facilitating decisions based on false information that negatively affects the security of society and individuals
- acceleration of social conflict, anarchy, and extremism[44]

Disinformation in the Russian–Ukrainian conflict

Nowadays, disinformation activities in the online space can spread in a highly sophisticated way. Based on an already analysed previous case (the 2016 U.S. presidential election), fake news accounted for almost 6% of all news consumption in the period under discussion, but it was highly concentrated: only 1% of users were exposed to 80% of fake news, and 0.1% of users were responsible for sharing 80% of fake news, which is a worrying statistic in the academic world in the context of disinformation campaigns and the defence against them.

In addition, recent events have unfortunately seen disinformation campaigns explicitly threatening human lives.[45]

Regarding Russia, they use the opportunities offered by the various online social media platforms. On these platforms, they have two popular and adequate ways of pushing their narrative: the use of so-called "trolls" and botnets.[46]

By trolls, we mean real users who, either out of conviction or for some quid pro quo, advocate a particular point of view in either their own or opposing communities. By botnet, we mean a so-called "robot network", i.e. a collection of interconnected networks that are centrally controlled. The central controller is the one who controls all these interconnected networks. Suppose an attacker decides to attack an organisation or to carry out any activity on various online platforms that he or she has defined; he or she will need a large amount of resources. In that case, botnets are malicious networks, an army, that allows attackers to penetrate web servers by breaking firewall security, conducting large-scale phishing attacks, delivering malware, among other things, and carrying out (distributed) denial of service (D)DoS attacks, but also use so-called "brute force" to compromise devices, user accounts, including their presence on various online platforms. In this regard, botnets can contribute to the success of various psychological operations and disinformation campaigns by delivering the messages and content they want to target very quickly and efficiently to the target group or different layers of users.[47] These possibilities are, of course, also being used in a meaningful way in the Russian–Ukrainian war. In addition to this, it is important to note that Russia relies heavily – albeit undeclared – on cybercriminal

[44] Dobák 2022: 93–124.
[45] Katz 2020: 659–682.
[46] Alieva et al. 2022.
[47] Chen et al. 2022; Sri Skandha Moorthy – Nathiya 2023: 1405–1413; Elliott 2010: 79–103; Srinivasan–Deepalakshmi 2023.

(APT) groups and non-governmental organisations (NGOs) and actors. In terms of its implementation, based on our current knowledge, the Russian government allows/pays no heed to the activities of these criminal groups on the territory of Russia, while certain "tasks" can be outsourced to these group actors.[48]

Along the previously detailed points, we can identify the same objectives for both Russian and Ukrainian disinformation operations:

- promoting their narrative
- gaining the support of its population and the undecided
- convince international opinion
- demoralising, weakening, and influencing the enemy
- drain the enemy's resources
- influence social processes
- create mistrust, provoke conflicts
- support military, political, and economic objectives

Some of the better-known disinformation campaigns:

- The legend of the ghost of Kyiv
- Denial of the Bucha massacre
- Zelensky's flee to the West
- Poland and Finland marched to the Russian border
- The fake news about refugees
- Faking war events
- Failure to acknowledge the fact of war

Countering disinformation

Countering and defending against disinformation and fake news is in the interest of individuals and the community. For individuals and society, and more broadly for a country or even a federal system, obtaining real, credible information is essential to make the right decisions in a wide range of situations and to enable citizens and decision-makers to make decisions in their own and their community's best interests, free from outside influence.

In the fight against disinformation, it is important to remember the need for fact-checking, source-checking, credibility-checking, critical thinking, and sound reasoning (scientific or from multiple, independent, and reliable sources) to minimise the likelihood of falling victim to campaigns.

There is no doubt that education has a key role in fortifying immunity to pseudo-news. Nevertheless, the methodological limitation is that it can take years to build immunity. In many cases, however, there is no time for this; think of the global pandemic caused by Covid–19 or a war. This is why the state has a key role in the fight against the spreaders of pseudo-news. An important tool for this could be the network-theoretic approach in the second part of our article series.

[48] Galeotti 2017.

Results of the analysis of the scientific literature

In this topic, we look at the scientific trends regarding disinformation, misinformation and malinformation keywords.

Firstly, the term malinformation received 37 results. This amount of results compared to other two keywords were much lower, therefore it was excluded from the analysis. Although, it is worth highlighting that the low results indicate a shallow trend regarding this keyword. We suspect the reason for this is that malinformation has a fundamental element compared to the other two keywords. Malinformation, as the name suggests, involves malice act and proving –which is central in a peer-reviewed article – that element is further demanding, compared to it being called misinformation.

If both keywords were found in the same article, the work was included in both analyses for the latter keyword. From the early 2000s onwards, there was a slow increase for each keyword, which started to increase more intensively from 2013 onwards. For the 2023 data, only publications included up to August were processed.

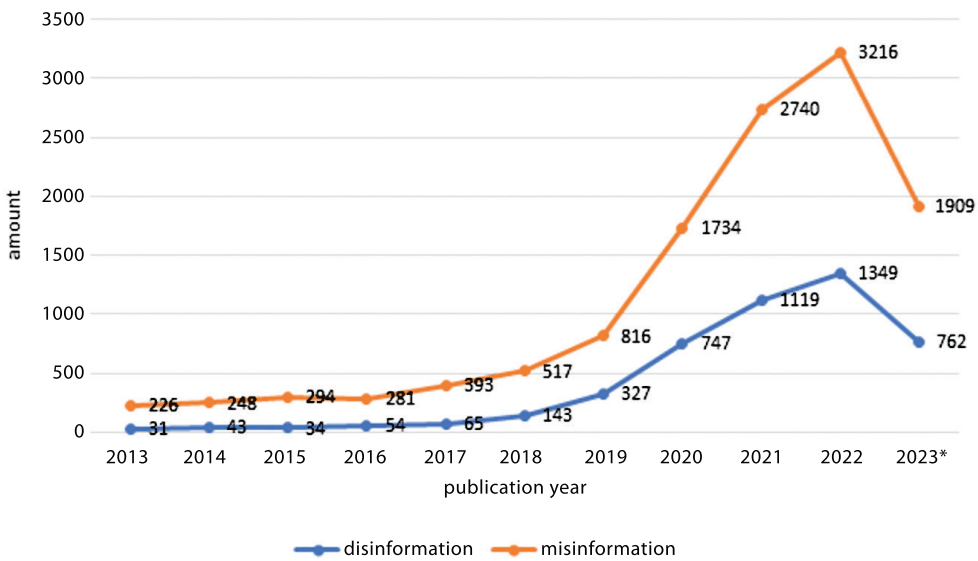

Figure 1: Publication amount comparison by year: disinformation and misinformation 2013–2023
Source: Scopus

Figure 1 shows that the number of publications related to these two terms rose sharply in 2019 and practically quadrupled by 2022. The data suggest that a similar magnitude of publications as in 2022 will be published in 2023. As Figure 1 compares the amount of publications which have the words present, misinformation is more trending. We observe a growth in both words, however misinformation is certainly more popular. From 2019 to 2020 the amount has doubled in both cases. We assume

the reason for this large jump in the trends is connected to the 2020 U.S. Presidential Election, the ongoing Covid–19 crisis, and the Russia–Ukraine conflict. To get a full picture about this assumption, we analysed the top 100 keywords connected to disinformation and misinformation.

Firstly, we highlight the top 100 keywords, and when each keyword started to appear in terms of disinformation is shown in Figure 2. Figure 2 showcases, while disinformation has a major connection to other keywords, it is not clearly in a central position. We can also observe a shift coming from the publishing year. The older articles focus on human aspects, later this transfers to social media and Covid–19. While our initial assumption regarding the Covid–19 connection was right, the U.S. Presidential Election has no connection to the word disinformation in the observed publications.

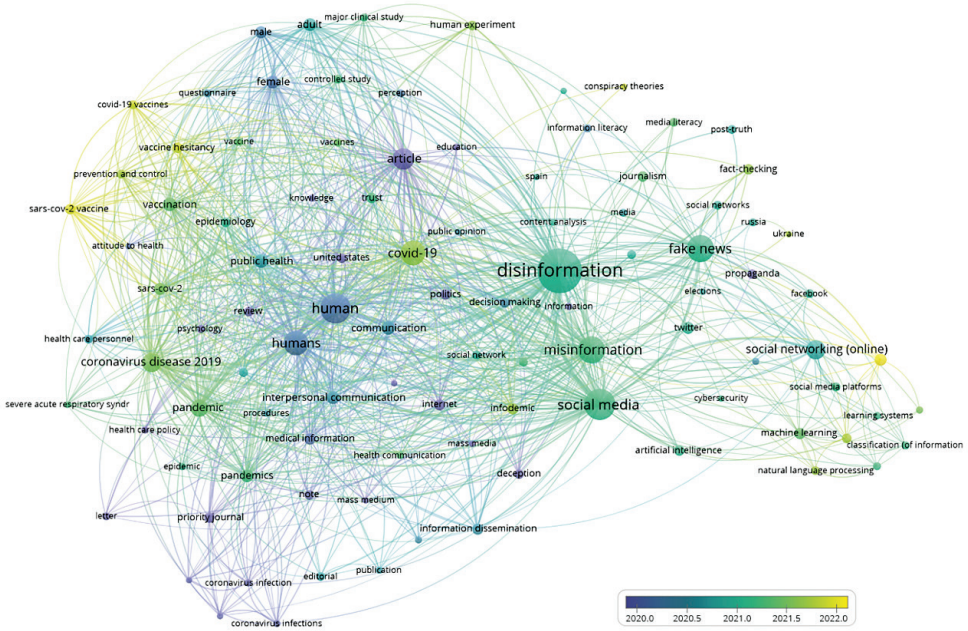

Figure 2: Top 100 keywords in connection with disinformation
Source: Scopus

The only international trend we can witness in Figure 2 is the coronavirus pandemic. The Russia–Ukraine has no presence in the keyword connections, our understanding is that Covid–19 is a way more overwhelming and directly internationally affecting issue. Moreover, for peer-reviewed literature, from the time when the researcher starts working on the article until release more than a year can pass by. For this reason, we assume that the disinformation with Russia–Ukraine related keywords going to be more dominant after 2024.

Figure 3 highlights the top 100 keywords in connection with misinformation. We can already observe compared to Figure 2 that the words are more interconnected.

"Social media" keyword creates a bridge for machine learning, deep learning and fake news topics. This assures an indication that social media plays an important role in these topics. Also looking at the publishing years, we can detect the same shift which we have seen in Figure 2. The older articles showcase mostly human topics, while latest articles focus on Covid–19. Here also the U.S. Presidential Election has no presence in the keyword cloud. The same observation regarding the Russia–Ukraine conflict applies to Figure 3 as well. We assume that due to the research article process topics related to the war going to be more present after 2024.

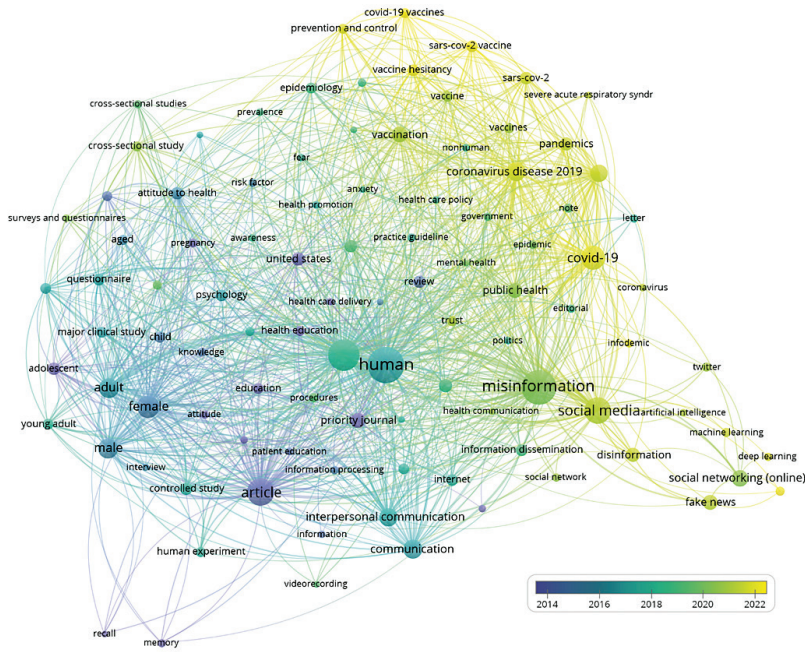

Figure 3: Top 100 keywords in connection with misinformation
Source: Scopus

These three figures give a clear presentation over the current and previous scientific trends. We do observe a delay in topics, which can be connected to the fact that articles take time to create and publish. While Covid–19 as a pandemic started in early 2020, the figures clearly show articles related to this pandemic are mostly from 2022. Based on this observation, we assume that the same will be related to the Russia–Ukraine conflict articles.

It is worth noting and highlighting that the words misinformation, social media, fake news and disinformation are closely bonded. Looking at the shift in time, researchers first approached this question from the individual (human) perspective, but now the focus is on the information itself and platforms, therefore social media, misinformation, disinformation are more dominant in latest articles. We already know that social media plays an important role in the Russia–Ukraine conflict, thus this

trend will very likely to continue. Social media also raises multiple issues regarding fake news, which we open up for discussion in our next chapter.

Discussion

In summary, the operations at the heart of our research (information and psychological operations, disinformation campaigns, dissemination of misinformation and malinformation) represent challenges to the free expression of opinion and political will of the global public, which can be defined as a central, crucial security issue today. In the remainder of our research, we will use sentiment and network analysis to investigate the spread of fake news in war and its impact. As presented in our research, this is not a new issue, but rather an ongoing challenge. If we raise the question of how we tackle fake news, unfortunately there is no clear answer and no clear solution. Creating fake news compared to fact checking information is a relatively cheap and non-time consuming matter. Fake news is often being shared on social media, which further increases the challenge. If traditional media platforms share misleading information, they later can be held responsible for it. There's a clear and established legal process for this, either affected individuals might form a lawsuit towards the media platform, or the government itself can issue a fine. However, if fake news are shared on social by an individual or by a random profile there's a major burden. Firstly resources are required to investigate who is responsible for the fake news. They are also very likely be from a different nation which is lenient in this question. Also governments have no full control over social media platforms, so before any information can be investigated, the platform provider must cooperate. Which is also a burden for governments.

This research is not meant to be deeply analyse how challenging social media is in our modern world, but we feel like in this topic the issue has to be mentioned. Fake news are a constant threat and we see no clear solutions to address them. Moreover, as we have seen from keyword analysis social media is highly connected to fake news. Because it gives a relatively easy option to bad actors to share harmful or misleading information.

As for the information warfare, the spreading of fake news can undermine valuable expensive military operations – especially CIMIC duties in a very cost-effective way. For every military operation, a public support is essential, therefore if we are unable to find a solution to the fake news issue, we anticipate that military operations will be threatened.

References

Aïmeur, Esma et al. (2023): Fake News, Disinformation and Misinformation in Social Media: A Review. *Social Network Analysis and Mining,* 13(30). Online: https://doi.org/10.1007/s13278-023-01028-5

Aleksejeva, Nika et al. (2023): Kremlin Information Operations Before and After Ukraine Invasion. *Atlantic Council,* 22 February, 2023. Online: www.atlantic-

council.org/event/kremlin-information-operations-before-and-after-the-february-2022-invasion

Alieva, I. et al. (2022): How Disinformation Operations against Russian Opposition Leader Alexei Navalny Influence the International Audience on Twitter. *Social Network Analysis and Mining,* 12(1). Online: https://doi.org/10.1007/s13278-022-00908-6

Bányász, Péter et al. (2019): Lélektani műveletek a közösségi médiában. In Auer, Ádám – Joó, Tamás (eds.): *Hálózatok a közszolgálatban.* Budapest: Dialóg Campus, 111–134.

Bērziņš, Jānis (2020): The Theory and Practice of New Generation Warfare: The Case of Ukraine and Syria. *The Journal of Slavic Military Studies,* 33(3), 355–380. Online: https://doi.org/10.1080/13518046.2020.1824109

Betts, Jennifer (2021): Examples of Propaganda Done With Different Tactics. Yourdictionary.com, 19 May, 2021. Online: https://examples.yourdictionary.com/examples-of-propaganda.html

Bundtzen, Sara et al. (2022): Hashtag Pairing Is Being Used on Twitter to Facilitate Soviet Propaganda Tactic 'Whataboutism'. *ISD – Institute for Strategic Dialogue (blog),* 15 March, 2022. Online: www.isdglobal.org/digital_dispatches/hashtag-pairing-is-being-used-on-twitter-to-facilitate-soviet-propaganda-tactic-whataboutism

Chen, Long et al. (2022): Social Network Behavior and Public Opinion Manipulation. *Journal of Information Security and Applications,* 64, 103060. Online: https://doi.org/10.1016/j.jisa.2021.103060

Collins, Ben – Korecki, Natasha (2022): Twitter Bans over 100 Accounts that Pushed #IStandWithPutin. *NBC News,* 4 March, 2022. Online: www.nbcnews.com/tech/internet/twitter-bans-100-accounts-pushed-istandwithputin-rcna18655

Czeglédi, Mihály (2017): Az információs műveletek szerepe a korszerű parancsnoki gondolkodásban. *Honvédségi Szemle,* 145(4), 74–87.

Dobák, Imre (2022): A dezinformáció – napjaink kiemelt kihívása. *Katonai Jogi és Hadijogi Szemle,* 10(1), 93–124.

Elliott, Claire (2010): Botnets: To What Extent Are They a Threat to Information Security? *Information Security Technical Report, Computer Crime – A 2011 Update,* 15(3), 79–103. Online: https://doi.org/10.1016/j.istr.2010.11.003

European Commission (2016): *Joint Communication to the European Parliament and the Council – Joint Framework on countering hybrid threats.* JOIN(2016) 18 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016JC0018

European Commission (2020): *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – A European Strategy for Data.* COM(2020) 66 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066

Farkas, Tibor (2023): A kommunikációs és információs rendszerek értelmezése napjainkban: követelmények és kihívások. In Tóth, András (ed.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika, 11–30.

Galeotti, Mark (2017): Controlling Chaos: How Russia Manages Its Political War in Europe. *ECFR,* 1 September, 2017. Online: https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe

Gerasimov, Valery (2013): The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. *Military-Industrial Kurier,* 27 February, 2013.

Grinberg, Nir et al. (2019): Fake News on Twitter during the 2016 U.S. Presidential Election. *Science,* 363(6425), 374–378. Online: https://doi.org/10.1126/science.aau2706

Haig, Zsolt (2011): Az információs hadviselés kialakulása, katonai értelmezése. *Hadtudomány,* 21(1–2), 12–28.

Haig, Zsolt (2018): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus.

Haig, Zsolt – Várhegyi, István (2005): *Hadviselés az információs hadszíntéren.* Budapest: Zrínyi.

Joint Chief of Staff (2014): *Joint Publication 3-13: Information Operations.* 20 November, 2014.

Jungherr, Andreas – Schroeder, Ralph (2021): Disinformation and the Structural Transformations of the Public Arena: Addressing the Actual Challenges to Democracy. *Social Media + Society,* 7(1). Online: https://doi.org/10.1177/2056305121988928

Katz, Eian (2020): Liar's War: Protecting Civilians from Disinformation during Armed Conflict. *International Review of the Red Cross,* 102(914), 659–682. Online: https://doi.org/10.1017/S1816383121000473

Kiss, Álmos Péter (2019): A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147(4), 17–37.

Kiss, Álmos Péter – Somodi, Zoltán (2019): A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. *Honvédségi Szemle,* 147(6), 22–28. Online: https://doi.org/10.35926/HSZ.2019.6.2

Krajnc, Zoltán ed. (2019): *Hadtudományi lexikon: Új kötet.* Budapest: Dialóg Campus. Online: https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/14688/790_hadtudomanyi_lexikon_2019.pdf?sequence=1&isAllowed=y

Magyar Honvédség (2014): *Ált/57 Információs Műveletek Doktrina.*

Miller, David (2015): Sociology, Propaganda, and Psychological Operations. In Dawson, Matt et al. (eds.): *Stretching the Sociological Imagination: Essays in Honour of John Eldridge.* London: Palgrave Macmillan, 163–188. Online: https://doi.org/10.1057/9781137493644_9

NATO (2009): *NATO AJP-3.10 – Allied Joint Doctrine for Information Operations.* Online: https://info.publicintelligence.net/NATO-IO.pdf

NATO (2014): *Wales Summit Declaration issued by NATO Heads of State and Government participating in the meeting of the North Atlantic Council in Wales.* 5 September, 2014. Online: www.nato.int/cps/en/natohq/official_texts_112964.htm

Nemeth, William J. (2002): *Future War and Chechnya: A Case for Hybrid Warfare.* Naval Postgraduate School, Monterey. Online: https://core.ac.uk/download/pdf/36699567.pdf

Padányi, József – Tomolya, János (2017): Háború és béke Ukrajnában, avagy keleten a helyzet változatlan 1. rész. *Hadtudomány,* 27(1–2), 63–83. Online: https://doi.org/10.17047/HADTUD.2017.27.1-2.63

Padányi, József – Tomolya, János (2017): Háború és béke Ukrajnában, avagy keleten a helyzet változatlan 2. rész. *Hadtudomány,* 27(3–4), 29–42. Online: https://doi.org/10.17047/HADTUD.2017.27.3-4.29

Porkoláb, Imre (2015): Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? *Hadtudomány,* 25(3–4), 36–48. Online: https://doi.org/10.17047/HADTUD.2015.25.3-4.36

Pozderka, Zoltán (2016): Az információs műveletek helye és szerepe a műveletervezésben. *Hadtudomány,* 26(Special ed.), 131–141. Online: https://doi.org/10.17047/HADTUD.2016.26.K.131

Rácz, András (2014): *Oroszország hibrid háborúja Ukrajnában*. KKI-Tanulmányok 2014/1. Online: http://docplayer.hu/6612943-Oroszorszag-hibrid-haboruja-ukrajnaban.html

Raychev, Yavor (2019): Roots of the Concept of Hybrid War in Russian Political and Military Thought. *Balkan Social Science Review,* 13(13), 127–151.

Simicskó, István (2017): A hibrid hadviselés előzményei és aktualitásai. *Hadtudomány,* 27(3–4), 3–16. Online: https://doi.org/10.17047/HADTUD.2017.27.3-4.3

Smart, Charlie (2022): How the Russian Media Spread False Claims About Ukrainian Nazis. *The New York Times,* 2 July, 2022. Online: www.nytimes.com/interactive/2022/07/02/world/europe/ukraine-nazis-russia-media.html

Sri Skandha Moorthy, R. – Nathiya, N. (2023): Botnet Detection Using Artificial Intelligence. *Procedia Computer Science, International Conference on Machine Learning and Data Engineering,* 218, 1405–1413. Online: https://doi.org/10.1016/j.procs.2023.01.119

Srinivasan, Sathiyandrakumar – Deepalakshmi, P. (2023): Enhancing the Security in Cyber-World by Detecting the Botnets Using Ensemble Classification Based Machine Learning. *Measurement: Sensors,* 25, 100624. Online: https://doi.org/10.1016/j.measen.2022.100624

UNHCR [s. a.]: *Situation Ukraine – Refugee Situation.* Online: https://data2.unhcr.org/en/situations/ukraine

Van Puyvelde, Damien (2015): Hybrid war – does it even exist? *NATO Review,* 7 May, 2015. Online: www.nato.int/docu/review/articles/2015/05/07/hybrid-war-does-it-even-exist/index.html

Legal sources

Government Decree 1163/2020 (21.IV.) on the National Security Strategy of Hungary. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001

Government Decree 1393/2021 (24.VI.) on the National Military Strategy of Hungary. Online: https://honvedelem.hu/hirek/nemzeti-katonai-strategia.html