ISSN: 2450-6869

eISSN: 2719-6763

No. 20, 2024

DEFENCE SCIENCE REVIEW

http://www.journalssystem.com/pno/

DOI: 10.37055/pno/200300

Countering Disinformation Concept for building social resilience in times of cognitive warfare

Original article

Received: 2024-06-17

Revised: 2024-11-22

Accepted: 2025-01-19

Final review: 2024-12-17

Peer review: 2024-05-27

Double blind

Keywords:

disinformation, social resilience, cognitive warfare

Tomasz Gergelewicz [1], A-D

ORCID 0000-0002-9145-5099

A – Research concept and design, B – Collection and/or assembly of data, C – Data analysis and interpretation, D – Writing the article, E – Critical revision of the article, F – Final approval of article

[1] Ministry of Defence, Poland

Abstract

Objectives: The aim of this article is to answer the following question: Are there any particular areas that shall be taken into consideration when discussing the problem of cognitive warfare. The author presents the Countering Disinformation Concept, which indicated particular areas that may serve as a potential direction for building and developing social resilience in times of cognitive warfare.

Methods: The author analyzed researches that prove a low social awareness of disinformation and point the possible sources of false content. The author revised professional literature to examine what is the current state of practical solutions in the researched field. The conclusion from the analysis was a basis for proposing the Countering Disinformation Concept. The author uses also a case study of Russian hostile informative influence as evidence for destructive actions of global actors and possible harmful influence of information.

Results: The result of the conducted research led to the conclusion that there is a lack of holistic, practical solutions in the field of building social resilience against disinformation. The proposed Countering Disinformation Concept is a comprehensive approach that shall be considered to build social resilience against hostile information operations in times of cognitive warfare.

Conclusions: Societies are not aware of hostile information influence that some actors strive to have. The awareness of disinformation processes is low as well as the level of practical solutions implemented in the information sphere. There is a serious need to build and develop social resilience against disinformation especially in the times of cognitive warfare spread by hostile global players.

Corresponding author: Tomasz Gergelewicz, Phd, Ministry of Defence, Poland, e-mail: t.gergelewicz@wp.pl.

Introduction

Information war is not a new phenomenon but nowadays is provided with modern tools, which have changed together with the information environment. The main tool in this war is the hostile process of disinformation that purposely misleads a target audience to influence cognition and push to particular behaviour. The aim of disinformation is to influence cognitive dimension within the information sphere; thus, the aspect of recognizing the world and reality tightly associated with emotions, morale and ethical values, and as a hostile tool plays a vital role in the hybrid warfare. The information sphere itself being a natural playground for the humanity is more and more nested by cruel destroyable factors, which gradually influence the persons singularly and nations holistically. It may be characterized as "the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on information. The information environment is a heterogeneous global environment where humans and automated systems observe, orient, decide, and act on data, information, and knowledge" (DOD Strategy, 2016).

The span of threats derived from the information sphere is important for the national security, mostly because of its holistic dimension, which includes dangers not only for units but also for nations as a whole. The Polish National Security Strategy indicates: "In the context of digital revolution a distinctive role of cyberspace and infosphere has to be considered. It is also a field to disinformation and information manipulation, which demands effective actions in the scope of strategic communication" (Strategia Bezpieczeństwa Narodowego, 2020). The demand for actions is a strong voice highlighting the real nature of the threats and the appearance of new dimension for battles. Considering the above, there shall be high priority granted to defence against infoaggression directed towards society, as it strikes social perception in order to control the way of thinking and to provoke particular behaviour in favor of the aggressor's lines of operations.

Nowadays, there is a lack of comprehensive and holistic approach towards disinformation. Practical solutions do not follow theoretical backgrounds and there are no dedicated institutions to conduct the task of combating disinformation. The aim of this article is to answer the following question: Are there any particular areas that shall be taken into consideration when discussing solutions for the problem of cognitive warfare and its influence on societies. Thus, the author presents the Countering Disinformation Concept, in which specific areas are characterized and may serve as a potential direction for building and developing social resilience in times of cognitive warfare. The author enumerates three areas that shall be taken into consideration both by governmental and non-governmental actors to create comprehensive protective umbrella over society in order to keep it resilient against hostile cognitive actions.

The subject of disinformation and cognitive warfare has also been addressed by Roy Godson (Godson, 2000), Yuryi Danyk (Danyk, 2023), the Central European Digital Media Observatory (CEDMO, 2024), Institut Public de Sondage d'Opinion Secteur (IPSOS, 2024), Digitalpoland (2024), Bernard Claverie and François du Cluzel (Claverie, Cluzel, 2022), Zara Abrams (Abrams, 2021), Florian Winterrlin and Tiim Schatto-Eckrodt (Winterrlin, Schatto-Eckrodt, 2023).

The author analyzed researches that prove a low social awareness of disinformation threats and point the possible sources of false content. The subject natter literature was reviewed to examine what is the current state of practical solutions in the researched field. The conclusion from the analysis was a basis for proposing the Countering Disinformation Concept, which constitute directions towards building social resilience against hostile information activities. The author uses also a case study of Russian hostile informative influence as evidence for destructive actions of global actors and possible harmful influence of information.

1. Cognition as the battlefield

If by any chance someone can influence the cognitive aspect of world-perception, it may lead to abnormal understanding of reality. Thus, the cognition itself is a vital target for hostile activities and a dimension of warfare, as it enables adversaries to take control over multiple associations fundament for world recognition. To understand the place of "cognition", it has to be distinguished from other dimensions of the information environment:

1. Physical - composed of the command and control systems, and supporting infrastructures that enable individuals and organizations to conduct operations.
2. Informational - where information is collected, processed, stored, disseminated, displayed and protected.
3. Cognitive - encompasses the mind of the decision maker and the target audience. This is the dimension in which people think, perceive, visualize, and decide (USMCU, 2022).

The cognitive dimension includes, among others: cultural beliefs, norms, motivation, emotions, vulnerabilities, identity, ideology, perception, will, awareness, attitude, understanding, opinions, experience, knowledge, assumptions and behavior. Defining these factors in a given environment is crucial for understanding, by which means adversaries influence minds of the target audience. From the very beginning of a crisis to the transfer into a war, cognitive dimension is a vital sphere both to attack and to defend. The mental strength of fighting sides, their understanding of goals, and a will to survive constitute a shadow power of cognition. It is underlined that cognitive dimension may be a platform for hostile operations and these operations "can be tools of expansion or even specific colonization through transformations of outlook, values, and interests of targeted groups. They occur through deep knowledge of the mental space of certain target groups and societies, and an understanding of how social and mental vulnerabilities." (Danyk, 2023).

Regarding the cognitive dimension as the battlefield, there appears a phenomenon of cognitive warfare. As underlined by NATO: "Cognitive Warfare integrates cyber, information, psychological, and social engineering capabilities. These activities, conducted in synchronization with other instruments of power, can affect attitudes and behaviour by influencing, protecting, or disrupting individual and group cognition to gain advantage over an adversary" (Cognitive warfare, 2023). Societies are the target in a "run-for-mind" race and extensive assets of influence are employed from both sides: adversaries - to take control; and the state - to sustain immunity to hostile info-activities. As the US Department of Defence

highlights: “Opponents try to use the information environment, including information technology and social media. Actions can range from trying to plant malware in weapons, to spreading disinformation on social media” (U.S. Government Accountability Office, 2022). The aim of the cognitive warfare was also characterized by Laurie Fenstermacher as a new domain of the battlefield including attacks of the wide scale impact on the entire population (Fenstermacher, Uzcha, 2023). Furthermore, the total output the cognitive warfare is supposed to have on the target was swiftly explained at the NATO Scientific Meeting in 2021: “Cognitive Warfare is the most advanced form of human mental manipulation, to date, permitting influence over individual or collective behavior, with the goal of obtaining a tactical or strategic advantage. In this domain of action, the human brain becomes the battlefield. The pursued objective is to influence not only what the targets think, but also the way they think and, ultimately, the way they act.” (Claverie, Cluzel, 2022). Tzu-Chieh Hung and Tzu-Wei Hung underline the specificity of the cognitive warfare as a highly important tool of influence: “Cognitive warfare also resembles influence warfare in its effects. Therefore, although all of them—cyberwarfare, information warfare, cognitive warfare, and hybrid warfare—contain the element of influence operations and may impact human cognition, only cognitive warfare is specifically dedicated to brain control by incorporating weaponized neuroscience into various practices.” (Tzu-Chieh Hung, Tzu-Wei Hung, 2022).

Cognitive warfare carried out heavily in the information environment includes an information war, which is characterized, among others, as: “The operations conducted to gain info-advantage over an opponent. It is achieved by controlling own infosphere, securing an access to own information, and at the same time gaining and using information from the opponent, destroying his info-systems and disturbing the flow of information.” (Media – (Dis)Information-Security, 2005). It is also explained as: “The manipulation of information trusted by a target without the target’s awareness so that the target will make decisions against their interest but in the interest of the one conducting information warfare.” (ECPS, 2024). To highlight the importance of information sphere, it may be stated that military conflicts in the nearest future still will be conducted in a very kinetic manner, though the cyberspace will start prevailing. Thus, it is crucial to notice that the centre of gravity is being pushed towards the virtual dimension. Yet, the Russian aggression towards Ukraine since 2014 has been a proof for the rising importance of infowarfare, the meaning of the news-battlefront, so the cognitive aspects of influencing target audience.

2. Disinformation as a primary tool in cognitive warfare

Cognitive warfare is executed by the use of different tools, and one of the most influential is disinformation. It has to be explained that the author enumerates three elements of disinformation, labeling them as MFN:

1. Manipulation with facts,
2. Fake news’ creation,
3. Noise in the information sphere (implementation of information noise and media hype). Manipulation with facts is a purposed use of factual information but presenting it in a way that it does not reflect the actual state of affairs. It may be partial

information, or cut out of the context in favor of the author's line of narratives. Creation of fake news means thinking up information that does not go along with reality, and this includes lies. There is also a phenomena of information noise and media hype. These have to be taken into consideration as a powerful tool because of their blurred nature. Media hype is characterized by Peter Vasterman as, "media-generated, all-embracing news wave, triggered by one particular event and strengthened by a self-perpetuating process within the media's news production." (Miotk, 2021). In order to flatten and disperse the core message by making information noise, an infoaggressor introduces:

- ✓ overflow of meaningless data in the context of the subject matter, so mixing facts with manipulated information;
- ✓ another, additional threads of discussion in order to redirect attention from the leading topic, so implementing other directions in order to make audience unaware of the topic of the real importance.

There is also a worth-noticing characteristics for disinformation, which concerns provoking particular reaction of the target audience regardless costs it may take (Kupiecki, Bryjka, Chłoń, 2022).

3. Russia in disinformative practices

Russia appears to be a troublemaker in the European community. Its authoritarian posture and aggressive actions pose a threat to Western countries and democratic values. The cognitive warfare that Russia conducts towards the West, including the war in Ukraine, is carried out also by the wide use of MFN[1]. The disinformative activities of pro-Russian channels of information are not mostly aimed at influencing the message of the mainstream media, but it strikes by sneaking backdoor using minor media corridors. Thus, it maintains the ability to influence selected layers of society, as these backdoor activities support broader disinformation streams carried out with the use of other media tools. The main strings of disinformation are aimed at polarizing nations and undermining Western governments as well as democratic values. Russia sustains its influential capabilities in Lithuania, Latvia and Estonia on certain representatives, who may be used as the trigger for serious broad-scale operation, e.g. a destabilization of the political situation (Marek, 2020). Ionita Craisor-Constantin enumerates some events as the examples of hostile Russian activities: "Kosovo crisis and the military support provided by Moscow to Belgrade, and also the recent spate of bomb threats and cyber-attacks in North Macedonia and Serbia (…) and the change in the Russian-Serbian psychological disinformation strategy in the Western Balkans" (Craisor-Constantin, 2023). She highlights also that such Kremlin's actions have also been reported in other parts of the globe, e.g. New Zealand, the USA, Canada and Germany, and that these activities are a sign of a hybrid war against NATO Members and Partners. It has to be also remembered that Russian hostile informative actions are organized and planned with the great level of details including the deep knowledge of the target and careful choice of the forces and assets used to disinform. As highlighted by experts in the "Fakehunter" project: 'In the case of

[1] Manipulation, fake news, noise in the information sphere.

Russian disinformation, we can talk about a "dedicated product". The messages resulting from propaganda are the result of thorough analysis." (PAP). Anna Taranenko highlights the cognitive dimension of disinformation regarding the recent European war of Russia against Ukraine, "Disinformation is also an important component of the cognitive dimension of the ongoing Russo-Ukrainian war. Ever since the start of the Russian aggression (…) scholars state that Russia has also been waging an information war against Ukraine and the Western bloc countries." (Taranenko, 2024). The cognitive warfare conducted by Moscow is both hard-straightforward and soft-subtle in order to reach the vast part of societies along the world, including Russians themselves. Moscow engaging in many open and hidden conflicts provides itself an opportunity to practice disinformation; thus, it is a great challenge for the West to stay resilient to Kremlin's cognitive warfare.

4. Social awareness of MFN

Areas that should be taken into account while combating infothreats are dispersed and not clearly defined. What is more, when it comes to details there are few practical solutions to be considered. One of the main challenges in building social resilience is an unawareness of society being a target of hostile narratives and of the ongoing infowar. National Research Institute (NASK) published research, which shows that more than half of Polish Internet users have encountered manipulation or disinformation, and 35% of Poles encountered fake news online once a week or more. At the same time, as much as 19% explicitly state, they do not check the credibility of online information or its sources (NASK, 2019). The report of the Pen America states: "More than 90% had made one or more changes in their journalistic practice as a result of disinformation, including 66% who said they are spending more time actively debunking disinformation and 59% who reported intentional efforts to be transparent about decisions, methods, and sources." (PEN America, 2021). Research conducted by the Internet Branch Employers Association Poland shows that, "according to respondents, disinformation is mostly spread by common Internet users – 62%. 39% of respondents claim that Internet services are responsible for this state of events and 27% state that these are professionally trained people from abroad." (Wrzosek, 2019). Research provided by the Central European Digital Media Observatory shows the awareness of particular countries of the information war associated with the Russian aggression against Ukraine. 41% of respondents in the Czech Republic and 41% in Hungary agreed that the information war is only an excuse for denying freedom of speech. Citizens of the Czech Republic (39%) and Hungary (32%) states their motherland is an arena for the Russian information war. In Slovakia, more people than in the Czech Republic believe that Russia is waging an information war against the West. However, in Poland, over half of the population (55%) believes that Russia is conducting an information war against Western countries (CEDMO, 2024). Research run by IPSOS shows that "Americans are most likely to think social media platforms, elected officials, and TV and cable news are responsible for creating "fake news," (…). One in four Americans say social media platforms (25%) are most responsible for the creation of "fake news" or disinformation, while 19% say politicians and elected officials and 17% say TV and cable news networks." (IPSOS, 2024). It is worth mentioning that society manifest low level of trust to media and opinion leaders that are blamed for being the source of disinformation. Brandy Zadrozny underlines that the spread of disinformation impacts

crucial areas of social interest like politics or health: “It <disinformation> can also provide false evidence for claims with conclusions that threaten democracy or national health, when people are persuaded to take up arms against Congress, for example, or decline vaccination.” (Zadrozny, 2024). Regarding the source for false content, well discussed research has been provided by Florian Winterrlin, who claims that “alternative media use was the main direct predictor for sharing disinformation. People who use alternative media reported higher intentions to share disinformation.” (Winterrlin, Schatto-Eckrodt, 2023). In 2024 there was report issued by the foundation Digitalpoland on technology in-service to the society. It discusses a comprehensive research conducted among Polish citizens regarding among others, the influence of technology on their security in the infosphere. Authors of the report indicate that an average Pole is unprepared for identification and signaling hostile cyberactivities, which influence the way of perceiving the reality. The list of factors that contribute to susceptibility to information threats, includes: carelessness of people (59%), inadequate protection of systems and devices (48%) and lack of knowledge or training (46%). Moreover, 62% of respondents stated that the media in Poland are subordinated to political goals, and 60% there is a lack of access to reliable information (Digitalpoland-Technology, 2024). In another report of the Digitalpoland, authors present the result of research on disinformation. 84% of Poles declared that they had encountered false information and according to 82% the scale of false information has increased over the last decade (Digitalpoland-Dezinformacja, 2024). All of the above mentioned factors are a cornerstone for creating effective hostile influence operations with a deep cognitive impact.

Vulnerability to MFN increases in direct proportion to the lack of awareness of threats and the disability to deal with them. Thus. there is an explicit need to build social resilience against disinformation, especially in the light of a vast unawareness among societies and the lack of skills to unveil disinformative attacks. Societies in general are not aware of being attacked with hostile information inputs and they do not know how to deal with infothreats. At the same time the main sources of information may occur to be the main sources of false content.

5. Countering Disinformation Concept

It shall be noticed that the subject of countering disinformation has been raised also at the level of EU institutions. Signatories commit to put more efforts in order to better equip societies to identify disinformation, enable them to navigate sources in an informed way and facilitate their access to tools appropriate for information assessment with the assistance of fact-checking institutions that flag potential disinformation (The Strengthened Code of Practice, 2022). On the forum of the European Union there is a strong call to fight disinformative content: “The fight against disinformation is a joint effort involving all European institutions. The EU is working in close cooperation with online platforms to encourage them to promote authoritative sources, demote content that is fact-checked as false or misleading.” (European Commission, 2022). As highlighted, “Fact-checking initiatives attempt to identify and correct false or misleading information, propagated either by political and economic elites or through peer-to-peer interactions on social media (Studdart, 2021). One of the fundaments described by the Canadian government is debunking false information

content with the goal: ‘to make sure accurate information prevails by providing facts to counteract false information’ (Canadian Government).

Due to ongoing cognitive warfare, the low level of social understanding of information threats, and the need of developing resilient society, the author proposes particular areas, which ought to be considered as vital in building social resilience against disinformation:

- successful communication;
- combating disinformation;
- antidisinformative education.

Particular pillars for the countering disinformation concept stands for:

1. Successful Communication is a must-be to have a real impact on society. If there is no possibility to reach people with the truthful and credible information or people simply do not trust the channels of communication, there is no chance to make them aware of threats and to make them resilient to these threats. As it is often highlighted: “Every medium may and should counter the spreads of disinformation, efficient debunking false information, and also simply deliver high-quality information in which the recipients may lay their trust.” (Nougayrede, 2019). Credible information channels and the appropriately chosen tools shall be the venue for the facts’ delivery and the gain of the social trust. The recipient of information is not able to assess every piece of info in the “true-false” category, not having enough knowledge in every field. Thus, info-recipient must trust the channels of information transfer and the institutions responsible for the protection of the infosphere. Only socially trusted sources will be able to support society with credible information, element vital especially in the time of crisis and war. Media communication may have a distinctive influence on social cognition also in war time. An influence over an opponent’s perception is a milestone in gaining an advantage. It is not only the forward edge of the battle area that is a war ground, but currently it is a whole-of-society and whole-of-ground that is supposed to be captured. In such a hostile environment media play a key role: “(…) calling and coordinating a crowd of people was partly dependent on people publishing on the Internet (…). Thus, there was an informal structure which disseminated information and could to some extent influence the behavior of the crowd: journalists and bloggers, who initiated the outbreak of protests with the published content.” (Górnikiewicz, Szczurek, 2018).

   The solution may the introduction of legal regulations that would limit and finally penalize MFN. The key would not be to strict the array of media activities but to limit a lack of professionalism, clickbait chase, the creation of information bubbles and hostile information influence. Such regulations shall stress the need for sources checking and the necessity to provide information without MFN. As highlighted by António Guterres: ‘Countering disinformation requires lasting investment in building societal resilience and media and information literacy’ (Guterres).

2. Antidisinformative Education in this context means building a whole-of-society awareness of infothreats and pointing the need of critical thinking when coming across any information. Critical thinking is of the highest importance because once

embedded into mind of the target audience, later may be a self-developed shield in the infowar. It stands for an objective assessment of the infosphere and it is "the source of laws introducing order (rationality) to reality." (Bakuła, 2013). It may be also defined as: "an ability to question; to acknowledge and test previously held assumptions; to recognize ambiguity; to examine, interpret, evaluate, reason, and reflect; to make informed judgments and decisions; and to clarify, articulate, and justify positions' (Louisville University). Social-widespread of awareness is crucial for building watchful approach towards infothreats. As stressed by Roy Godson, awareness of deceptive operations is one of the most important factors to stay immune to the cognitive manipulation: "(…) accurate and consistent explanation that adversaries are interested in shaping public and media opinion to serve their own interests can sensitize individuals to the possibility that they are being manipulated. Awareness of how past, current, and possibly future D&D <Denial and Deception> has targeted the media and other nongovernmental sectors will help minimize effectiveness of strategic foreign deception efforts (Godson, 2000). Courses, trainings, conferences, meetings, social initiatives, etc. are one of the educational tools that the state must use to enhance the awareness and strengthen social resilience. The state is obliged to educate in such a way that a society acquire the ability to recognize, oppose and fight harmful information on its own; and that is why education is a crucial area for building a holistic resilient approach against disinformation. It may be added that social campaigns may be an effective tool as a straightforward, direct message supported by an image. These should be comprehensive and understandable projects carried out to anchor the message in social awareness. As an educational factor there may be, for example "fakeresilience rules" proposed to the audience. The rules might be:

- remember that what you read does not have to be true;
- if you have any doubts, check information in many different sources;
- do not share unconfirmed information or else you also became responsible for false content.

It has to be remembered that antidisinformative education may be socially accepted and employed only from credible sources and delivered by reliable channels of communication. The example of a real educational initiative may be the project called: "Education with the Army" run by the Polish Ministry of National Defence. Soldiers from military units teach the youngest the basic rules concerning security and safety, including, among others, topics associated with resilience against disinformation[2] (Polska Zbrojna, 2024).

3. Combating Disinformation is another pillar for countering hostile info operations. It means direct reaction to particular element of MFN. It may be possibly conducted in two manners: either by the reactive debunking or proactive communication:

[2] The project included over 3500 schools from all over the country. The author of this article developed the training programme for this project and run the methodological classes for soldiers-instructors.

- reactive debunking stands for unveiling MFN by revealing facts and it is mostly carried out by fact-checking institutions, when doubted information is checked in order to confirm if it is true or to debunk it as false (for e.g. checking it in multiple sources or consulting with experts).
- proactive communication in this context stands for delivering the audience facts in advance, so prior the disinformation would nest itself in the social cognition. It creates a "no-gaps infosphere", in which hostile narratives cannot be embedded because society is fact-aware; thus, much less susceptible to fakes. Thus, when the infoaggressor wish to manipulate or deceive, the population has been already well informed and thanks to that, resilient against disinformation.

6. Caveats and obstacles

Even though there is an urgent need to deal with disinformation and a lot of forces as well as cutting edge technologies have been applied to counter information threats; still there are factors, which undermine these efforts and pose a challenge. Mostly these are human-driven reasons derived from cognitive caveats. Hence, it is challenging to successfully reach the target audience with the "correct version of information", because it is difficult to change once embedded "reality" in the human's understanding. As the American Psychology Association (APA) highlights: "When we hear new information, we often think about what it may mean (…). If we later hear a correction, it doesn't invalidate our thoughts - and it's our own thoughts that can maintain a bias, even when we accept that the original information was false." (Abrams, 2021). What is more, advanced technology also does not solve the problem of MFN, as it can be used for both, the truth or fake content creation. As raised by Dipto Barman: "With the rapid advancement of artificial intelligence and the growing prominence of large language models (LLMs) such as ChatGPT, new avenues for the dissemination of disinformation are emerging (…). Utilizing these advanced models, malicious actors can automate and scale up disinformation effectively (…). The advent of LLMs poses an additional concern as they can be harnessed to significantly amplify the velocity, variety, and volume of disinformation." (Barman, 2024). Moreover, as emphasized by Kai Shu: "People are reluctant to believe the results of AI-powered disinformation detection tools as these techniques are often like a black-box and lack of transparency." (Shu, 2022).

Conclusion

The aim of cognitive warfare the infohostility is to influence the way of perceiving the reality by a target society. The more polarization among societies, the less educated people are, and the little critical thinking is engaged in absorbing knowledge from the infosphere, the easier nations are influenced and pushed into particular actions. In order to stay reality-conscious, as well as, to develop aware and healthy social multidimensional relations, societies have to be equipped with tools to defend and shall be supported by the state in the war against info-threats. The Countering Disinformation Concept stands for a holistic defensive approach towards the hostile influence operations, hostile narratives, and disinformation process, which includes MFN and are employed to drill minds of societies in

order to twist the way of thinking and push to actions in favor of an infoaggressor. The three pillars in the Concept: successful communication, antidisinformative education and combating disinformation are vital elements of creating and strengthening social resilience against hostile information operations in times of cognitive warfare.

References

Abrams, Z. (2021), 'Controlling the spread of misinformation', Monitor on Psychology, vol. 52, no. 2, pp. 44, Available at: https://www.apa.org/monitor/2021/03/controlling-misinformation [Accessed: 11.08.2023].

Bakuła, S. (2013), 'Problem poznania w krytyce czystego rozumu Kanta jako teoretyczna propozycja dla współczesnych dyskusji nad poznaniem', Filozofia i Nauka. Studia Filozoficzne i Interdyscyplinarne, t. 1, pp. 257-263.

Barman, D., Guo, Z. Conlan, O. (2024), 'The Dark Side of Language Models: Exploring the Potential of LLMs in Multimedia Disinformation Generation and Dissemination, Machine Learning with Applications, vol. 16, Available at: https://www.sciencedirect.com/science/article/pii/S2666827024000215 [Accessed: 17.07.2024].

Claverie, B., Cluzel, F. (2022), '"Cognitive Warfare": The Advent of the Concept of "Cognitics" in the Field of Warfare'. Available at: https://www.researchgate.net/publication/359991886_Cognitive_Warfare_The_Advent_of_the_Concept_of_Cognitics_in_the_Field_of_Warfare [Accessed: 21.06.2024].

Craisor-Constantin, I. (2023), 'Conventional and hybrid actions in the Russia's invasion of Ukraine', pp. 9, Available at: https://securityanddefence.pl/pdf-168870-93689?filename=Conventional%20and%20Hybrid.pdf [Accessed: 10.09.2023].

Danyk, Y., Briggs, C. (2023), 'Modern Cognitive Operations and Hybrid Warfare." Journal of Strategic Security 16, no. 1 (2023): 35-50. Available at: https://digitalcommons.usf.edu/jss/vol16/iss1/3 [Accessed: 12.06.2024].

Fenstermacher, L., Uzcha, D. (2023), 'New perspectives on cognitive warfare', Proceedings of the SPIE, vol.12547, pp.16, Available at: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12547/125470I/New-perspectives-on-cognitive-warfare/10.1117/12.2666777 [Accessed: 11.05.2024].

Godson, R. (2000), 'Strategic Denial and Deception' in International Journal of Intelligence and Counter Intelligence, vol. 13, no. 4, pp. 424-437, Available at: https://core.ac.uk/download/pdf/36735473.pdf [Accessed: 18.04.2024].

Górnikiewicz, M., Szczurek, T., 'Social Media Wars The R-evolution Has Just Begun', Available at:https://www.researchgate.net/profile/Marcin-Gornikiewicz/publication/328306146_Arabic_Spring_Chapter_3_31_Social_Media_Wars_The_R-

evolution_Has_Just_Begun/links/ 5bc59c81299bf17a1c55912c/Arabic-Spring-Chapter-3-31-Social-Media-Wars-The-R-evolution-Has-Just-Begun.pdf [Accessed: 22.11.2024].

Guterres, A., 'United Nations – Countering Disinformation, Available at: https://www.un.org/en/countering-disinformation [Accessed: 23.06.2024].

Hung, Tzu-Ch., Hung, Tzu-W. (2022), 'How China's Cognitive Warfare Works: A Frontline Perspective of Taiwan's Anti-Disinformation Wars', Journal of Global Security Studies, vol. 7, Issue 4, Available at: https://academic.oup.com/jogss/article/7/4/ogac016/6647447? login=false [Accessed: 25.06.2024].

Miotk, A.D. (2021), 'I Tak W Koło Macieju, czyli jak powstaje szum medialny', Studia Humanistyczne AGH, 20/21, pp. 47-48.

Nougayrede, N. (2019), 'Stop dezinformacji – przewodnik dla dziennikarzy i redakcji', Available at: https://panoptykon.org/stop-dezinformacji-przewodnik [Accessed: 15.07.2023].

Kai Shu (2022), 'Combating disinformation on social media: A computational perspective.

Kupiecki, R., Bryjka, F., Chłoń, T. (2022), 'Dezinformacja międzynarodowa: pojęcie, rozpoznanie, przeciwdziałanie', Scholar, Available at: https://www.researchgate.net/publication/360631169_R_Kupiecki_F_Bryjka_T_Chlon_Dezinformacja_miedzynarodowa_pojecie_rozpoznanie_przeciwdzialanie_Wydawnictwo_Naukowe_Scholar_Warszawa_2022.pdf, [Accessed: 22.11.2024].

Marek, M. (2021), 'Polska nadal zagrożeniem dla Rosji – przekaz propagandowy dedykowany ludności państw bałtyckich', Available at: https://infowarfare.pl/2021/10/13/polska-nadal-zagrozeniem-dla-rosji-przekaz-propagandowy [Accessed: 10.08.2023].

Studdart, A. (2021), 'Building Civil Society Capacity To Mitigate And Counter Disinformation', Available at: https://counteringdisinformation.org/node/2690 [Accessed: 13.10.2023].

Taranenko, A. (2024), 'Ensuring information security: Countering Russian disinformation in Ukrainian speeches at the United Nations'. Social Sciences & Humanities Open, vol. 10, 100987, Available at: https://www.sciencedirect.com/science/article/pii/S2590291124001840 [Accessed: 01.07.2024].

Winterrlin, F., Schatto-Eckrodt, T. (2023), '"It's us against them up there": Spreading online disinformation as populist collective action', Computers in Human Behavior, vol. 146, 107784, Available at: https://www.sciencedirect.com/science/article/pii/S0747563223001358 [Accessed: 10.07.2024].

Wrzosek, M. (2019), 'Zjawisko dezinformacji w dobie rewolucji cyfrowej', Warszawa, pp. 32 (eds). Available at:

https://cyberprofilaktyka.pl/badania/Raport_CP_Dezinformacja_ONLINE.pdf [Accessed: 2.07.2023].

Zadrozny, B. (2024), 'Disinformation poses an unprecedented threat in 2024 — and the U.S. is less ready than ever, Available at: https://www.nbcnews.com/tech/misinformation/disinformation-unprecedented-threat-2024-election-rcna134290 [Accessed: 9.03.2024].

Other sources:

Canadian Government, 'Countering Disinformation: A Guidebook for Public Servants', Available at: https://www.canada.ca/en/democratic-institutions/services/protecting-democratic-institutions/countering-disinformation-guidebook-public-servants.html#toc26 [Accessed: 12.07.2024].

Bench Council Transactions on Benchmarks, Standards and Evaluations', vol. 2, Issue 1, Available at: https://www.sciencedirect.com/science/article/pii/S2772485922000229?fr=RR-2&ref=pdf_download&rr=8adc0a5eda67c3c7 [Accessed: 6.02.2024].

CEDMO (2024), Available at: https://cedmohub.eu/four-out-of-ten-czechs-and-hungarians-41-think-that-the-information-war-is-just-an-excuse-for-western-governments-to-restrict-freedom-of-speech-in-slovakia-more-than-a-third-35-and-in-poland-a-q/ [Accessed: 03.07.2024].

Cognitive Warfare (2023), 'Strengthening and Defending the Mind', Available at: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind [Accessed: 3.07.2023].

Digitalpoland-Dezinformacja (2024), Available at: https://digitalpoland.org/publikacje/pobierz?id=70f40c4e-3fe1-4abd-9a32-02a26c324f18 [Accessed: 22.11.2024].

Digitalpoland-Technology (2024), Available at: https://digitalpoland.org/en/publications/download?id=151bae71-dc52-474c-a64f-181a49d6ab8d [Accessed: 22.11.2024].

DoD Strategy for Operations in the Information Environment (2016), p. 3, Available at: http://www.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf [Accessed: 23.07.2023].

ECPS – European Center for Populism Studies, 'Glossary: Information Warfare', Available at: https://www.populismstudies.org/Vocabulary/information-warfare/ [Accessed: 20.05.2024].

European Commission (2022), 'Fighting Disinformation', Available at: https://commission.europa.eu/strategy-and-policy/coronavirus-response/fighting-disinformation_en [Accessed: 2.09.2023].

IPSOS (2024), ‘Americans blame social media, elected officials, TV and cable news for “fake news”‘,Available at: https://www.ipsos.com/en-us/americans-blame-social-media-elected-officials-tv-and-cable-news-fake-news [Accessed: 28.02.2024].

Media – (Dis)Information-Security, Available at: www.nato.int, Media – (Dis)Information – Security, 2005-deepportal4-information-warfare.pdf [Accessed: 10.07.2023].

NASK (2019), ‘Bezpieczne wybory’, Available at: https://www.nask.pl/pl/aktualnosci/2249,Badania-NASK-ponad-polowa-polskich-internautow-styka-sie-z-manipulacja-i-dezinfo.html [Accessed: 06.08.2023].

PAP, ‘Gra na konflikt – główne narracje rosyjskiej dezinformacji’, Available at: https://fake-hunter.pap.pl/node/19 [Accessed: 05.06.2023].

PEN America (2021), ‘The Impact of Disinformation on Journalism: Online Survey of Journalists’, Available at: https://pen.org/wp-content/uploads/2022/04/PEN-America-Complete-Survey-Results_Hard-News.pdf [Accessed: 20.07.2023].

Polska Zbrojna (2024), “Program „Edukacja z wojskiem” wystartował”, Available at: https://polska-zbrojna.pl/home/articleshow/41661?t=Program-Edukacja-z-wojskiem-wystartowal [Accessed: 12.05.2024].

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (2020), pp. 8. Available at: https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf [Accessed: 10.07.2023].

The Strengthened Code of Practice on Disinformation (2022), pp. 21-22. Available at: https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation [Accessed: 11.08.2023].

University of Louisville, Available at: https://louisville.edu/ideastoaction/about/criticalthinking /what [Accessed: 21.06.2024].

US Marine Corps University. Available at: https://www.usmcu.edu/CRSS/Support/Cognitive-Dimension-Training [Accessed: 15.09.2023].

U.S. Government Accountability Office (2022), ‘Information Environment: Opportunities and Threats to DOD's National Security Mission’, Available at: https://www.gao.gov/products/gao-22-104714 [Accessed: 23.06.2024].