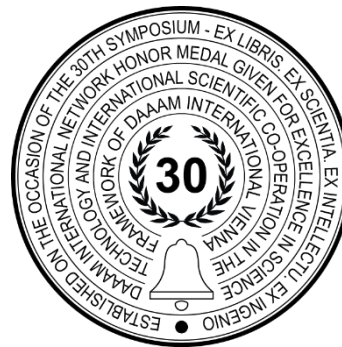


INFORMATION WARFARE, MEDIA AND CIVILIANS

Miroslav Tomsu, Martin Dzermansky, Nikola Cajkova & Pavel Wanecki



This Publication has to be referred as: Tomsu, M[iroslav]; Dzermansky, M[artin]; Cajkova, N[ikola] & Wanecki, P[avel] (2023). Information Warfare, Media and Civilians, Proceedings of the 34th DAAAM International Symposium, pp.0371-0378, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-41-9, ISSN 1726-9679, Vienna, Austria

DOI: 10.2507/34th.daaam.proceedings.051

Abstract

The progress in information and communication technologies in the transmission and sharing of data has fundamentally affected the armed forces, not only in terms of the development of information systems, control, and fire control systems but also in the conduct of war. The topic of the article is information warfare. The aim is to explain the meaning and concept of information warfare and to analyse the purpose of information warfare and its development in future security operations. The article first deals with the mutual relationship between information and military science and their concept of information. It continues with the characteristics of individual forms of information warfare, including the ways of conducting them. It explains the possible consequences of its action from information point of view. The benefit is considering the further possible development of some forms of information warfare and predicting probable implications in the event of their use.

Keywords: Information warfare; information operations; psychological operations; electronic warfare; intelligence operation.

1. Introduction

Contemporary society is increasingly approaching the ideas of the information society, and the main features are the predominance of work with information, interactivity, integration, and globalisation tendencies. From a technological point of view, an information society is a society with a high level of use of information and communication technologies based on computer technology and associated digitisation. However, the growing need for communication, sharing, and exchanging information characterises civilian and military institutions. The increasing dependence of military technology on electronic means that work with an unimaginable amount of information and the growing importance of the information itself has made information a lucrative target of combat action but, at the same time, a valuable weapon [1].

These changes are directly revolutionary from the point of view of information and from the point of view of conducting war. Unsurprisingly, there is more and more talk about the so-called information war nowadays. It has a lot to do with information science. The common subject of interest of information science and information warfare, which can be characterised in the broadest sense as „the joint deployment of available combat capabilities to influence, invalidate, dominate and disrupt enemy command capabilities, including automated means of decision-making; and at the same time to ensure the protection of all these own resources from the enemy [2], is indeed information.

In their studies, some authors mention the term information war in connection with a military conflict [3] [4] or the manifestation of the events of the last few years, [5] [6] but some authors also deal with it in the context of a socio-philosophical analysis of the processes associated with the formation of information culture among young people. [7] This article deals with information warfare in a military and general context with an emphasis on the role of the media and its impact on the civilian population.

2. Information environment

Information is a multifaceted term that every person encounters almost daily. It is a universal phenomenon, tightly connected not only with the daily life of man and society but also with living and non-living nature. From his point of view, its four basic meanings (are a psychophysiological phenomenon, numerical measure of disorganisation removal, potential information - sign-recorded and circulating data in technical devices, and expression of diversity in the objects and processes of nature). In the most general sense, information is information about the natural environment, its state, and the processes taking place [1].

2.1. Information from the perspective of information and military science

Information science primarily understands information as a message, communicable knowledge necessary for the recipient, or data that facilitates a choice between alternative decision-making options. [2] Vickery refers to information as knowledge or a type of knowledge. At the same time, he specifies command as what people know or think they know. In that case, new or modified knowledge is added or assimilated into the individual's „knowledge structure“ [8].

In this context, Britz even believes that Vickery understands information from a social perspective as a process between the source (information) and the user (information). Information is, therefore, not only a part or product of a process but the process itself (from the creation of information to its use). This is, of course, one of the approaches to the concept of „information“. User access can also be mentioned, which in the broadest sense means that information is what reduces the amount or degree of uncertainty. From the point of view of the content approach, what is communicated between people can be informed. According to Norbert Wiener's cybernetic concept, information is the content of what is exchanged with the external world when we adapt to it and act upon it with our adaptation. As Britz further states, ideological, knowledge, or anti-definitional approaches exist. Proponents of the latter oppose attempts to define the term information because it is said to have no practical meaning for information science [9].

2.2. Movement of information within military intelligence services

From the point of view of information, the military intelligence service can be considered an information institution within the armed forces. As with civilian information institutions, the information goes not only to the intelligence service – the intelligence service collects information and distributes it after processing and evaluation. The information provided is essential for the decision-making activities of the state [10].

The intelligence cycle is called the movement or chain of successive and interconnected activities during which information is obtained, processed, evaluated, and passed on to users. It comprises four phases: management, collection, processing, and dissemination, and it has a similar course to the classic information process. The names used for each step may vary, but these are synonymous terms. Even phase five is distinguished in American military regulations, such as the Doctrine for Intelligence Support of Joint Operations [11].

3. Information and military science

The difference in understanding information neither pits the two scientific fields against each other. On the contrary, they intermingle. Concerning its focus, military science, among other things, focuses on the military information environment, which is part of the global information environment and intertwines with the civilian sector. The military information environment is defined as an environment that is part of the worldwide information environment and is made up of information systems, friendly and hostile organisations, military and non-military, that support or significantly affect a specific military operation [12].

Military science is generally defined as „a system of knowledge about the nature and laws of war, the military preparation of the state and the armed forces for war, and the methods of conducting it.“ [13]. The primary subject of her research is armed struggle. In the broadest sense, information science can be defined as the science of information (physical, biological, cultural). „In a narrower sense, it is a science of an interdisciplinary nature dealing with the regularities of the processes of creation, processing, measurement, coding, storage, transformation, distribution and reception of information in society.“ [14]. The Explanatory Dictionary of Czech Terminology in Information Science and Librarianship further states that its goal is to secure and rationalise social information and communication processes. It is, therefore, clear that information science is not an isolated science but affects, among other things, the fields of technical sciences and information technologies (especially computer and communication technology), psychology, philosophy, etc. Military science also affects technical sciences, and, of course, information and communication technologies, philosophy, and psychology are also part of conducting war and commanding troops.

3.1. Information and the changing nature of wars

The introduction and use of modern weapons and the growing importance of electronics and computer technology have changed the character of war. Today, one of the most potent weapons is information. A completely new concept was born - information war (Information War - IW). Based on the generalisation of historical experience and experience from contemporary wars and armed conflicts, it is clear that the importance of information will continue to grow. It has always been, is, and will continue to be important in the future as well, the rule that whoever has information also has power and superiority. On the other hand, effectively using this information needs to be improved [15].

3.2. Information warfare

Information warfare is one of the means of hybrid warfare. We can define it as an activity aimed at gaining an advantage or superiority over an opponent in the management and use of communication and information channels or technology." Through the means of information, it takes place continuously from peacetime to wartime and then also during wartime. Previously, it was used only as a means of support. For example, in World War 1, leaflets were distributed among soldiers with calls to leave the resistance.

The main advantage of information warfare is a significant ratio of damage to the opponent compared to the percentage of costs incurred. Information warfare can be divided into offensive or defensive, depending on whether we protect information or try to influence it. This concept is often confused by the public with the term cyber war, which, according to the terminological dictionaries of the Ministry of the Interior, means: "The use of computers and the Internet to wage war in cyberspace. A set of large-scale, often politically or strategically motivated, related and mutually induced organised cyber-attacks and counter-attacks." Information warfare affects cyber warfare, but it also deals with other forms of action that intertwine with each other: command and control, intelligence operation, electronic warfare, psychological warfare, economic information war, diplomatic war, and, last but not least, a hacker war [16].

Christopher Bellamy of the Royal Military College of Science from Great Britain used an exciting definition in his analysis. According to him, the term information war could be a suitable designation for cyber warfare, provided that information is used to destroy, damage, or use the information of the adversary, information systems, and computer networks of the adversary. It also describes attacks against the mindset of commanders (influencing decision-making) - i.e., psychological warfare, deception, and mind-twisting. In this context, information war could be called a new term - psycho-cybernetic war, „psyberwar.“ In addition to these two areas, information warfare overlaps with warfare against command-and-control systems, electronic warfare, and information is crucial in deploying precision-guided munitions [17].

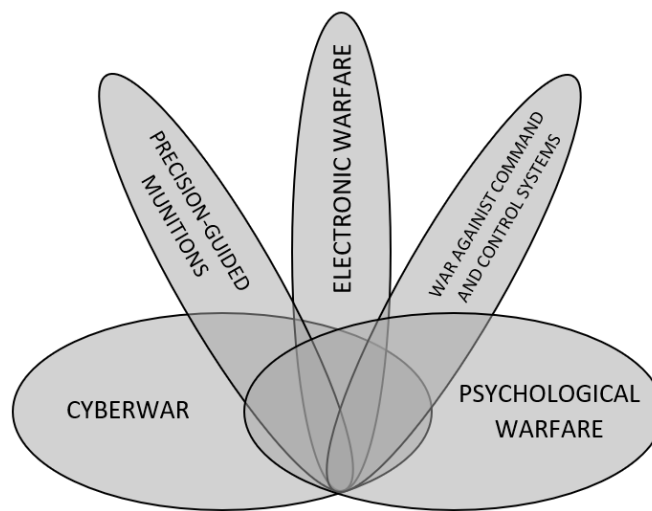


Fig. 1. Definition of the newly introduced term "psyberwar". [17]

4. Forms of information warfare

In recent years, in connection with the tactics of the great powers to abandon the complex techniques of conducting battles (about possible losses in the ranks of soldiers or the civilian population), the emphasis has shifted to the so-called soft forms of war. "This is why there has been a massive development of individual forms of conducting information warfare." Information warfare can be conducted by lethal or non-lethal means, brute force, or non-lethal means. It can also be divided into offensive or defensive - depending on whether the goal is to protect information or to act on it. However, such a division is crude, corresponding only to the primary division of combat activity into defence and attack [18].

Information warfare has yet to exist as a separate technique. It is made up of several forms that intertwine and complement each other. Currently, one can distinguish at least seven forms of information warfare:

4.1. Command-and-control warfare

Disarming a commander has been one of the goals for gaining dominance on the battlefield for centuries. However, the actual realisation of this plan has always been more difficult. However, the shift occurred at the moment of the creation of command centres. These are easily identifiable by basic features such as visible communication, computing equipment (associated with electromagnetic radiation), movements of printed documents and logistical material, and, most importantly, by atypical activities that are entirely different from the regular exercise of other units [18].

The purpose of the action is to destroy or disrupt the means of command and neutralise the control. This will interrupt the flow of information from the command structures to the executive element. These combat units will thus lose an overview of the overall situation. They will need to have, among other things, information on where to intervene, when to intervene, or how to intervene [19].

4.2. Intelligence-based warfare

The intelligence form of action in information warfare is discussed if intelligence is directly included in the combat activity - for example, in the process of selecting and allocating "targeting" targets or in determining whether the given means hit the target and the desired "Battle Damage Assessment" effect was met – and not only as an input to the command-and-control process. Therefore, including intelligence in combat is to obtain information to create a permanent and comprehensive picture of the battlefield. In addition, reporting also has the task of protecting data, i.e., preventing the enemy from failing to obtain information and form a complete picture of the battlefield, including the adversary's capabilities [19].

4.3. Electronic warfare

Electronic warfare is defined as „an activity focused on the use of the electromagnetic spectrum, which includes the search, interception, and identification of electromagnetic emissions, the use of electromagnetic energy, including directional radiation, to limit or prevent its use by the adversary against its means and ensuring their effective use“ [20].

4.4. Psychological warfare

Psychological operations are defined as „planned psychological activity in peace and war directed at an adversary, own or neutral persons to influence attitudes and behaviour, which affects the achievement of political and military objectives. They include psychological activity at the strategic level, psychological consolidation, and psychological activity on the battlefield“ [20].

But, according to Nastoupil, psychological warfare aims to influence the enemy's will without using weapons. From an information point of view, it is a planned and systematic distribution of information to various target groups. It must be carried out in a precisely defined period so that the announcement affects their awareness.

Psychological operations and propaganda are very close to each other. The boundary between the two activities needs to be clarified; some authors say these activities overlap. In general, peacetime psychological operations are based on presenting accurate information, or at least the truth as it is perceived. Propaganda, on the other hand, is perceived, according to the Oxford Guide to Military History authors, as the spread of lies (misleading information), and the target group is often one's population [21].

4.5. Economic information warfare

The economic information war was created by combining economic war and information war. Currently, two forms of it are distinguished: information blockade and information imperialism [22].

4.6. Hacker warfare

Information warfare is often simplistically considered a hacking war. In reality, however, the hacker war is one information war. Attacks are directed at specific systems (their structure and content) using technological shortcomings or "holes" in security measures. [36] The techniques or methods of hacker warfare vary according to the location from which the attacker launches the attack, the process of execution, and the expected extent of the damage. All of the hacker warfare techniques presented hereafter represent attacks against civilian targets. Attacks on civilian and, theoretically, military targets have common characteristics in a hacker war [22].

4.7. Cyberwarfare

Cyber warfare is considered a particular area of information warfare; it includes information terrorism, semantic attacks (intertwined with hacker warfare), simulated warfare, and Gibson warfare [22]. It is assumed that some of these forms will affect advanced military systems. Computer technology differs from other military assets because it is an integral part of all other assets used in modern armies; from this perspective, it is the critical component that many modern armies depend on, and potential enemies are well aware of this dependency. Cyber warfare has not yet been used against military assets, but it is increasingly being discussed, and its forms interest military experts [18].

5. Information warfare and civilians

In his famous 1921 essay on the importance of a free press, the long-time editor of the British Guardian, C. P. Scott, declared that comment is free, but facts are sacred. In quality independent journalism, it is good practice to verify facts from at least two independent sources and to separate clear facts from impressions and interpretations. Nevertheless, these principles cease to be the rule.

According to publicist and security analyst Jan Schneider, "An essential feature of current media events is the emphasis on creating a first impression. It is quickly passed off as a safe mainstream so as not to raise disturbing doubts or even questions of conscience. Political decisions are then built on this chimerical basis, which - put into practice - unfortunately already have irreversible material consequences. And all this happens even though the second impression, a closer examination of the original information, can show its shakiness, baselessness, or even falsity." [19]. On the other hand, some news sources still maintain a high ethical standard and rely on the truth of the facts they present to the public.

5.1. Making decisions based on desire and succumbing to fear

We don't necessarily have to lie if we want to distort reality to influence the recipient's thinking in a certain way. Yet, we have many tools to manipulate information to our advantage. One of the essential tools is the so-called agenda setting. Agenda-setting theory assumes that the emphasis and importance given to a specific issue by the media affects how the audience perceives and accepts the case.

The media have mechanisms that can determine what the audience is thinking about and which issues they perceive most important. The authors of this concept, Maxwell McCombs and Donald Shaw, concluded that the media set the public's agenda - they construct their reality and tell the people what to think about, what to notice, and what to consider necessary. Manipulation techniques in dealing with information that we can encounter in the media can be divided into several basic types:

- manipulation using purposeful selection of presented information (overwhelming with meaningless information, deliberate highlighting or ignoring of specific topics),
- sorting manipulation (this is the sorting of messages in a particular order when some messages are deliberately pushed aside and the main space is left for favoured messages - in the case of print, this is, for example, the front page),
- manipulation of emotions,
- manipulation of the selection of commentators (statements of witnesses or bystanders, which can have a significant influence on the overall tone of the report),
- manipulation of the context of communicated information (information taken out of context can have an opposite tone),
- manipulation by communicating incomprehensible messages,
- manipulation by editing – shortening and taking the statement out of context. [20]

6. Defence against information warfare

Psychology, as a scientific field, also has a dark side. Without realising it, we often become objects of psychological operations, the aim of which is to influence our attitudes, our opinions and our decisions. Psychological warfare methods are used in political, economic and hot conflicts. In a global society, it is a battle for territory and resources and for whom the world public will consider good and bad guys. It isn't easy to be utterly immune to psychological operations. However, as civilians in information warfare, we can defend ourselves with common sense, critical thinking, and knowledge of the manipulation techniques used against us. [21]. In addition to the criminalisation of the dissemination of hateful or alarmist messages, the main methods of defence against propaganda and information warfare are, in particular, the cultivation of the media and civil society and the responsible approach of the state.

6.1. Freedom and independence of the media

In the case of the media, it is about ensuring that the press is especially free and independent from the political sphere and that the market is rich and open to the whole spectrum of media. However, these media should have publicly declared and enforced standards of journalistic ethics and a transparent ownership structure.

There should be significant and independent public service media in the media market, sufficiently funded to follow current trends and compete with others. Although the media scene should be watched by a respected and impartial regulator that can effectively impose significant sanctions for breaking the rules - the media should be left with enough autonomy to set and enforce the laws through their journalistic organisations. The press should be assigned a credible disinformation rating. All media should be dedicated to uncovering misinformation or fake news and correcting it, as well as conducting impartial fact-checking when reporting the opinions and positions of actors in public affairs. Journalists and other media workers should be carefully and regularly trained on propaganda, disinformation and how to counter it.

6.2. Society Education

Expanding media and internet literacy through various educational programs is the most important among all citizens. Citizens should have the opportunity to participate with their opinions in a freely ongoing public debate and to get to know other nations and cultures, for example, through various international programs. Non-governmental organisations dealing with human rights and media freedom and quality should be created and supported in civil society to forge media control independent of the state and the journalistic form. States should allow such international non-governmental organisations to operate on their territory. For example, coercive actions should also come from the occasional company to dissuade advertisers from advertising in media that spread hateful materials or misinformation.

6.3. Steps taken by governments to prevent the spread of information warfare

In addition to implementing the measures mentioned above, governments should refrain from owning or exerting influence on the media and, of course, propaganda and spreading disinformation by any means. They should start dealing with the power of foreign propaganda and misinformation on their citizens; they should measure it and respond to it flexibly and effectively. From a position of authority, the state apparatus should also devote itself to refuting at least the most severe misinformation and fake news, and politicians should then speak out against propaganda and hateful opinions. At the same time, the government should also lead by example in improving its strategic communication – it should better explain the measures introduced and be generally transparent and open.

7. Weaknesses of information warfare

Weaknesses of information warfare: the meaning and importance of information generally will remain the same in the short term. However, the availability of information, the speed of its transmission and transmission, and its accuracy (accuracy of data obtained from advanced sensors) will increase. Dependence on advanced information technologies also has its weak side. Modern technology applies practically only to the ability to receive, share and disseminate information. There is an information war here, the weapons and targets of which are information and information technology. If properly conducted, it can interrupt the flow of information, shut down the communication of information systems, and even affect a person's decision-making process, the morale and mood of the population.

The intensity and amount of disinformation is increasing. Suppose most people agree that the official news is lying or that emotional contributions are deliberately made visible and amplified. In that case, this can lead to further problems. The constant impact of disinformation can lead to the fact that the population will claim that the constitutionally guaranteed freedom of speech is also that they, politicians, or the news media can knowingly publish false information or lie. Some see misinformation as part of the constitutionally guaranteed freedom of speech. The influence of disinformation can make the population feel that information warfare is just an excuse for Western governments to restrict freedom of speech and inconvenient media. [22]. Of course, information warfare is not limited to the population. It is fully applicable even in competition in a commercial environment. This area can also become a possible topic for further study and research.

8. Significance and development of information warfare in the early future

Information warfare plays a significant role in security operations as an integral part of them. It can be assumed that its position will be irreplaceable in the future as well; it will not lose its importance; on the contrary, it will increase. The speed of computing is growing dramatically while the size of computers is decreasing. In a study from the late 1990s, NASA's nanotechnology team states that soon, computers that will be millions of times more potent than the current ones can be made. [23]

Developed countries will thus dominate technologically on the battlefield, but paradoxically, their dependence on complex technologies will be a vulnerable point. One can, therefore, agree with Dunlevy's statement that "dependence on advanced technologies can be considered a potential Achilles' heel". [24]. No matter who is fighting on the battlefield, no matter what the image of the battlefield is (undersea depths, outer space, urban areas, mountainous terrain, virtual space of computer networks, etc.), future conflicts will be governed by the general principles of warfare, just like the current ones. Of these, the most important is that defence alone cannot be relied upon, for a "defensive war," as Welch points out, cannot lead to victory. [25]. How the information war will develop and what forms of information war will be used for this is a matter of imagination and consideration.

9. Conclusion

The progress in information and communication technologies in the transmission and sharing of data has fundamentally affected the armed forces in terms of the development of information systems, control and fire control systems, and the conduct of war. The meaning and importance of information in the military, in the general sense, will not change shortly. However, the accessibility of information, the speed of its transmission and transmission, and its accuracy (accuracy of data obtained from advanced sensors) will increase. Currently, when comparing the capacities of the armed forces and estimating the probable outcome of their confrontation, the factor of physical strength and speed (manoeuvrability) is considered in particular. In the future, it will probably be replaced by awareness - in the sense of situational preparedness, i.e., the ability to quickly deploy forces and resources to defend one's units or to strike at the enemy.

Dependence on advanced information technologies also has its weak side. Modern technology is practically only valid with the ability to receive, share, and spread information. This is where the information war occurs, the weapons and targets of which are information and information technology. If properly conducted, it can interrupt the flow of information, turn off weapons and information systems communications, and even affect the decision-making process of commanders, the units' morale, and the population's mood. Of course, information warfare is not limited to the military sector. It can also be fully applied in competition in a commercial environment. This area can also become a possible topic for further studies.

10. Acknowledgments

This article was supported by grant project IGA/FAI/2023/002, „Protection of the population, soft targets and the information environment”, solved in 2023-2024.

11. References

- [1] Cejpek, J. (2005). Information, communication and thinking: an introduction to information science, Nakladatelství Karolinum, ISBN 80-246-1037-X, Prague
- [2] Ressler, M. (2006). Information science and librarianship: an explanatory dictionary of Czech terminology in the field of information science and librarianship, VSCHT Prague, ISBN 80-7080-599-4, Prague
- [3] Li, Q., Liu, Q., Liu, S., Di, X., Chen, S., & Zhang, H. (2023). Influence of social bots in information warfare: A case study on @UAWeapons Twitter account in the context of Russia–Ukraine conflict. *Communication and the Public*, Vol. 8, No 2, pp. 54–80, DOI: 10.1177/20570473231166157
- [4] Putkalets, L. A., & Vyshnevska, G. B. (2023). Regional mass media in the context of Russia's information and psychological war against Ukraine, In *FUNCTIONING OF THE UKRAINIAN MEDIA DURING MARTIAL LAW IN UKRAINE*, pp. 93-107, DOI: 10.30525/978-9934-26-270-8-6.
- [5] Aro, J. (2016). The Cyberspace War: Propaganda and Trolling as Warfare Tools, *European View*, Vol. 15, No. 1, pp 121-132, ISSN 1781-6858, DOI: 10.1007/s12290-016-0395-5
- [6] Deepa, K. (2006). Media, War, and Propaganda: Strategies of Information Management During the 2003 Iraq War, *Communication and Critical/Cultural Studies*, Vol. 3, No. 1, pp. 48-69, DOI: 10.1080/14791420500505650
- [7] Mamasoliyevich, N. K. (2023). INFORMATION CULTURE: A NEW APPROACH. *World Bulletin of Social Sciences*, Vol. 19, pp. 129-134. Available: <https://scholarexpress.net/index.php/wbss/article/view/2228>
- [8] Vickery, B. (2011). Information science – part 1, Available: <http://www.lucis.me.uk/infosci1.htm>
- [9] Britz, J. (2006). A critical analysis of information poverty from a social justice perspective, Ph.D. Dissertation, University of Pretoria, Pretoria, South Africa
- [10] Bucharova, L. (2006). Information sources in the field of state security, Diploma thesis, Faculty of Arts, Charles University, Prague, Czech Republic
- [11] Doctrine for Intelligence Support to Joint Operations, (2000). Chiefs of Staff, Washington, Available: http://www.bits.de/NRANEU/others/jp-doctrine/jp2_0.pdf.
- [12] Information Operations, (1996). Headquarters, Department of The Army, Washington, Available: <http://www.iwar.org.uk/iwar/resources/usarmyio/fm100-6.pdf>.
- [13] Svoboda, O., et al. (1984). Concise Dictionary of the Military, Our army, Prague
- [14] Ressler, M. (2006). Information science and librarianship: an explanatory dictionary of Czech terminology in the field of information science and librarianship, VSCHT Prague, ISBN 80-7080-599-4, Prague
- [15] Piątkowski, K. (2003). *Wojna w mediach, Nowa Technika Wojskowa*, ISBN: 978-83-7395-246-1
- [16] Kubesa, M. (2013). "Military Deception in the Information Age", *Military perspectives*, Vol. 22, pp. 160-164, DOI: 10.3849/2336-2995.22.2013.01.160-164
- [17] Ch. Bellamy, Ch. (2001). "What is Information Warfare?" In: *Managing the Revolution in Military Affairs*, R. Matthews, J. Treddenick, (Ed.), pp. 234-252, Palgrave, ISBN 0333781899, Basingstoke
- [18] Hodicky, J. (2007). "The Information Age in the Military," In *The Information age, information society and military*, pp. 76-102, MO CR-AVIS, ISBN 978-80-7278-379-3, Prague
- [19] Schneider, J. (2016). *Words do not fall into a void*, ISBN 978-80-7376-468-5, Olympia, Velke Prilepy

- [20] McCombs, M. E. & Shaw D., L. (2023). “The Agenda-Setting Function of Mass Media”, *The Public Opinion Quarterly*, Vol. 36, No. 2, pp. 176–187. JSTOR <http://www.jstor.org/stable/2747787>.
- [21] Lucas, E. & Pomeranzev, L. (2016). “Winning the Information War – Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe: A Report by CEPA’s Information Warfare Project in Partnership with the Legatum Institute”, Center for European Policy Analysis, Available: https://cepa.ecms.pl/files/?id_plik=2715
- [22] Tomsu, M. (2022). *Reliable Information Sources in the Age of Propaganda*, Proceedings of the 33rd DAAAM International Symposium, pp. 437-443, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-36-5, ISSN 1726-9679, Vienna, Austria DOI: 10.2507/33rd.daaam.proceedings.061
- [23] Globus, A.; Bailey, D.; Han, J.; Jaffe, R.; Levit, C.; Merkle, R. & Srivastava, D. (1998). NASA applications of molecular nanotechnology, *The Journal of the British Interplanetary Society*, Vol. 51, pp. 145-152. Available: <http://www.nas.nasa.gov/News/Techreports/1997/PDF/nas-97-029.pdf>
- [24] Dunlevy, C.; Shimeall, T. & Williams P. (2001). *Countering Cyber War*, NATO Review, Director of Information and Press NATO, Vol. 49, pp. 16-19, Brussel
- [25] Welch, D.; Buchheit, N. & Ruocco, A. (1999). *Strike Back: Offensive Actions in Information Warfare*, New Security Paradigms Workshop, pp. 47-52, Caledon Hills, Ontario, Canada Available: <http://delivery.acm.org/10.1145/340000/335192/p47-welch.pdf?key1=335192&key2=9541386811&coll=&dl=&CFID=15151515&CFTOKEN=618461>